

9.3

IBM MQ Odkaz na konfiguraci

IBM

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí [“Poznámky” na stránce 259](#).

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

Když odešlete informace na adresu IBM, udělujete IBM nevýhradní právo používat nebo distribuovat informace libovolným způsobem, který považuje za odpovídající, aniž by vám tím vznikl jakýkoliv závazek.

© **Copyright International Business Machines Corporation 2007, 2024.**

Obsah

Odkaz na konfiguraci.....	5
Příklad: Nastavení komunikace mezi platformami pro IBM MQ.....	5
Jak používat příklady komunikace mezi platformami.....	7
Příklad: nastavení komunikace mezi platformami IBM MQ na systému AIX.....	9
Příklad: nastavení komunikace mezi platformami IBM MQ na systému IBM i.....	15
Příklad: nastavení komunikace mezi platformami IBM MQ na systému Linux.....	32
Příklad: nastavení komunikace mezi platformami IBM MQ na systému Windows.....	38
Příklad: nastavení komunikace mezi platformami IBM MQ na systému z/OS.....	44
Příklad: Nastavení IBM MQ komunikace mezi platformami na systému z/OS pomocí QSGs.....	49
Příklad: Nastavení IBM MQ mezisložkové komunikace pro řazení do front v rámci skupiny na systému z/OS.....	57
IBM MQ oprávnění systému souborů použitá pro /var/mqm.....	64
IBM MQ oprávnění k souboru v /opt/mqm s setuid pro mqm.....	68
IBM MQ oprávnění systému souborů na Windows.....	70
Omezení pojmenování pro fronty.....	71
Omezení pojmenování pro jiné objekty.....	73
Rozlišení názvu fronty.....	74
Co je rozlišení názvu fronty?.....	76
Jak se rozlišují atributy cílového objektu pro aliasy, vzdálené fronty a fronty klastru?.....	76
Systémové a výchozí objekty.....	77
SYSTEM.BASE.TOPIC.....	82
Informace o sekci konfiguračních souborů.....	83
Sekce konfiguračního souboru pro distribuované fronty.....	85
Atributy kanálu.....	86
Atributy kanálu pro klíčová slova MQSC (A-B).....	91
Atributy kanálu pro klíčová slova MQSC (C).....	94
Atributy kanálu pro klíčová slova MQSC (D-L).....	101
Atributy kanálu pro klíčová slova MQSC (M).....	108
Atributy kanálu pro klíčová slova MQSC (N-R).....	113
Atributy kanálu pro klíčová slova MQSC (S).....	117
Atributy kanálu pro klíčová slova MQSC (T-Z).....	122
Příkazy a atributy klastru IBM MQ.....	124
Atributy klastru dostupné v příkazech definice kanálu.....	125
Atributy klastru dostupné v příkazech definice fronty.....	128
Atributy klastru dostupné v příkazech definice správce front.....	130
DISPLAY CLUSQMgr.....	131
Aktualizovat klastr.....	133
RESET CLUSTER: Vynucené odebrání správce front z klastru.....	134
SUSPEND QMgr, RESUME QMgr a klastry.....	136
Vyrovnávání pracovní zátěže v klastrech.....	136
Asynchronní chování příkazů CLUSTER v systému z/OS.....	145
Programy kanálů.....	145
Úlohy interkomunikace na systému IBM i.....	146
Stavy kanálů na systému IBM i.....	146
Příklad: Plánování kanálu zpráv v systému AIX, Linux, and Windows.....	147
Nastavení příkladu kanálu zpráv pro AIX, Linux, and Windows.....	148
Spuštění a rozbalení příkladu pro AIX, Linux, and Windows.....	150
Příklad: Plánování kanálu zpráv v systému IBM i.....	150
Nastavení agenta kanálu zpráv v systému IBM i.....	152
Spuštění a rozbalení příkladu pro IBM i.....	154
Příklad: Plánování kanálu zpráv v systému z/OS.....	155
Nastavení agenta kanálu zpráv v systému z/OS.....	156

Spuštění a rozbalení příkladu pro z/OS.....	158
Příklad: Plánování kanálu zpráv pro z/OS pomocí skupin sdílení front.....	159
Nastavení definic skupin sdílení front a správce front QM3 , který není ve skupině sdílení front...	161
Příklad spuštění skupiny sdílení front pro z/OS.....	162
Použití aliasu k odkazování na knihovnu produktu MQ.....	163
Managed File Transfer odkaz na konfiguraci.....	163
Použití proměnných prostředí ve vlastnostech MFT.....	163
Soubor MFT installation.properties.....	165
Soubor MFT agent.properties.....	169
Soubor MFT coordination.properties.....	191
Soubor MFT command.properties.....	195
Soubor MFT logger.properties.....	199
Výstup vytvořený funkcí LogTransfer.....	209
Java systémové vlastnosti pro MFT.....	212
SHA-2 CipherSpecs a CipherSuites pro MFT.....	213
Konfigurační soubory modulu protokolování souborů MFT.....	213
Knihovna SCSQFCMD.....	221
SYSTEM.FTE.....	222
MFT Nastavení fronty agenta.....	223
MFT systémové fronty a téma systému.....	225
Konvence pojmenování objektů MFT.....	226
Stavové zprávy agenta MFT.....	227
IBM MQ Internet Pass-Thru odkaz na konfiguraci.....	228
Souhrn vlastností MQIPT.....	229
MQIPT globálních vlastností.....	235
MQIPT Vlastnosti trasy.....	239
mqiptAdmin vlastnosti.....	258
Poznámky.....	259
Informace o programovacím rozhraní.....	260
Ochranné známky.....	260


Odkaz na konfiguraci

Informace o odkazech v této sekci vám pomohou s konfigurací produktu IBM MQ.

Informace o odkazu na konfiguraci jsou uvedeny v následujících dílčích tématech:

Související úlohy

[Konfigurace](#)


 [Konfigurace produktu z/OS](#)

Příklad: Nastavení komunikace mezi platformami pro IBM MQ

Tento příklad ukazuje, jak vytvořit funkční síť IBM MQ konfigurací odesílacího a přijímacího kanálu IBM MQ, aby byl umožněn obousměrný tok zpráv mezi platformami přes všechny podporované protokoly.










Než začnete

Příklady konfigurace předpokládají, že pro konkrétní platformy jsou zavedeny konkrétní síťové infrastruktury:

-  Produkt z/OS komunikuje pomocí síťového řadiče 3745 (nebo ekvivalentu)

Předpokládá se také, že pro SNA jsou všechny požadované definice v VTAM a NCP (network control program) zavedeny a aktivovány pro platformy připojené k LAN, aby komunikovaly přes WAN (wide area network). Podobně se u protokolu TCP předpokládá, že funkce serveru názvů je k dispozici buď pomocí serveru názvů domény, nebo pomocí lokálně zadržených tabulek (například souboru hostitele).

Ukázkové konfigurace pokrývají následující síťové softwarové produkty:

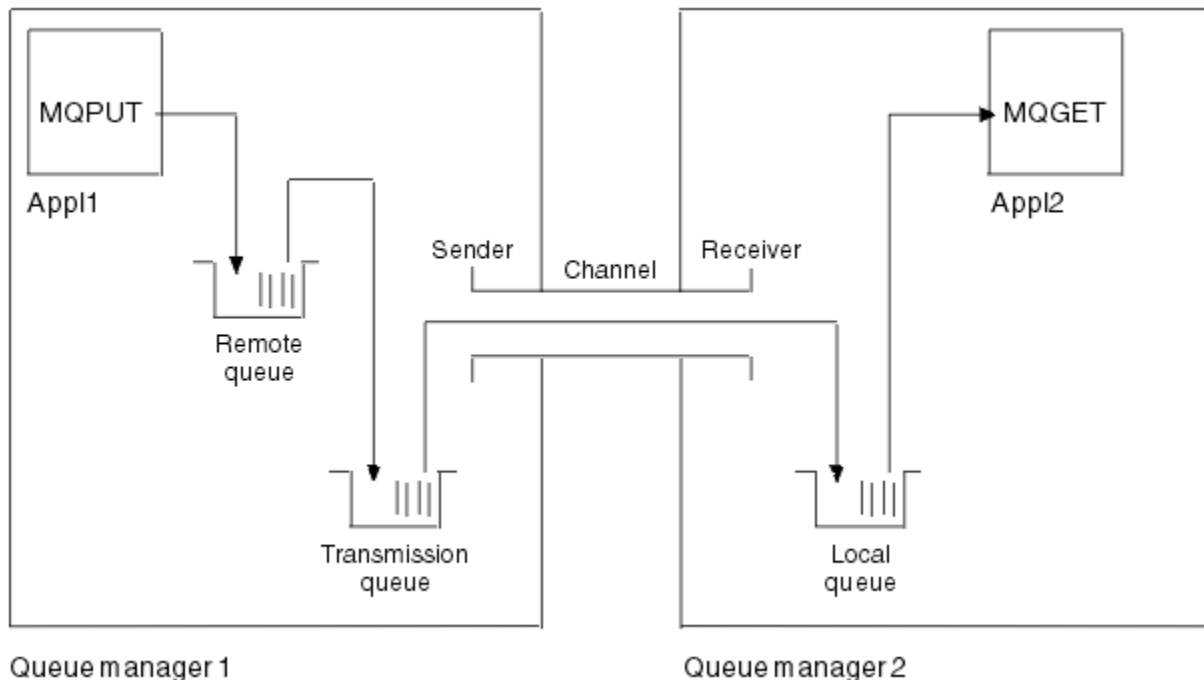
- SNA
 -  IBM Personal Communications pro Windows
 -  IBM Komunikační server pro AIX
 -  IBM i
 - OS/390
- TCP
 -  Microsoft Windows
 -  AIX
 -  IBM i
 -  TCP pro z/OS
-  NetBIOS
-  SPX

Další informace o podporovaných komunikačních protokolech a softwaru viz [Systémové požadavky pro IBM MQ](#).

Informace o této úloze

Tento příklad používá odesílací a přijímací kanály. Chcete-li použít jiné typy kanálů než příjemce odesílatele, použijte volbu [DEFINE CHANNEL](#) (define a new channel).

Obrázek 1 na stránce 6 je koncepční reprezentace jednoho kanálu a objektů IBM MQ, které jsou k němu přidruženy.



Obrázek 1. Kanál IBM MQ, který má být nastaven v ukázkové konfiguraci

Tento příklad je jednoduchý, určený k zavedení pouze základních prvků sítě IBM MQ. Neukazuje použití spouštěče, který je popsán v části [Spouštěcí kanály](#).

Objekty v této síti jsou:

- Vzdálená fronta
- Přenosová fronta
- Lokální fronta
- Kanál odesílatele
- Přijímací kanál

Appl1 a Appl2 jsou oba aplikační programy; Appl1 vkládá zprávy a Appl2 je přijímá.

Appl1 vkládá zprávy do vzdálené fronty. Definice této vzdálené fronty určuje název cílového správce front, lokální frontu v tomto správci front a přenosovou frontu v tomto lokálním správci front.

Když správce front obdrží od Appl1 požadavek na vložení zprávy do vzdálené fronty, určí z definice fronty, že je cíl vzdálený. Proto vloží zprávu spolu s přenosovým záhlavím přímo do přenosové fronty uvedené v definici. Zpráva zůstává v přenosové frontě, dokud nebude kanál k dispozici, což se může stát okamžitě.

Kanál odesílatele má ve své definici odkaz na jednu a pouze jednu přenosovou frontu. Když je kanál spuštěn a jindy během normálního provozu, podívá se na tuto přenosovou frontu a odešle všechny zprávy na ní do cílového systému. Zpráva obsahuje podrobnosti záhlaví přenosu cílové fronty a správce front.

Příklady komunikace podrobně popisují vytvoření každého z výše uvedených objektů pro různé kombinace platforem.

Ve správci cílové fronty jsou vyžadovány definice pro lokální frontu a stranu příjemce kanálu. Tyto objekty fungují nezávisle na sobě, a tak mohou být vytvořeny v libovolném pořadí.

V lokálním správci front jsou vyžadovány definice pro vzdálenou frontu, přenosovou frontu a odesílací stranu kanálu. Vzhledem k tomu, že definice vzdálené fronty i definice kanálu odkazují na název přenosové fronty, doporučuje se nejprve vytvořit přenosovou frontu.

Postup

1. Přečtěte si informace v části [“Jak používat příklady komunikace mezi platformami”](#) na stránce 7.
2. Při vytváření síťového připojení a definování kanálů postupujte podle pokynů pro příslušnou platformu nebo platformy.
 - a) **AIX**
Viz téma [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému AIX”](#) na stránce 9
 - b) **IBM i**
Viz téma [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému IBM i”](#) na stránce 15
 - c) **Linux**
Viz téma [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému Linux”](#) na stránce 32
 - d) **Windows**
Viz téma [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému Windows”](#) na stránce 38
 - e) **z/OS**
Viz téma [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému z/OS”](#) na stránce 44
 - f) **z/OS**
Viz téma [“Příklad: Nastavení IBM MQ komunikace mezi platformami na systému z/OS pomocí QSGs”](#) na stránce 49
 - g) **z/OS**
Viz téma [“Příklad: Nastavení IBM MQ mezisložkové komunikace pro řazení do front v rámci skupiny na systému z/OS”](#) na stránce 57

Související úlohy

[Konfigurace distribuovaných front](#)

[Nastavení komunikace s ostatními správci front v systému z/OS](#)

Jak používat příklady komunikace mezi platformami

Ukázkové konfigurace pro nastavení komunikace mezi platformami pro produkt IBM MQ popisují úlohy prováděné na jedné platformě pro nastavení komunikace s jinou platformou. V příkladech jsou popsány úlohy pro vytvoření pracovního kanálu pro tuto platformu.

Pokud je to možné, je záměrem učinit tyto informace co nejobecnější. Chcete-li tedy připojit libovolné dva správce front na různých platformách, je třeba odkazovat pouze na příslušné dvě sekce. Jakékoli odchylky nebo zvláštní případy jsou jako takové zvýrazněny. Můžete také připojit dva správce front spuštěné na stejné platformě (na různých počítačích nebo na stejném počítači). V tomto případě lze všechny informace odvodit z jedné sekce.

ALW V systému AIX, Linux, and Windows musíte před tím, než začnete postupovat podle pokynů pro vaši platformu, nastavit různé proměnné prostředí. Provedte to zadáním jednoho z následujících příkazů:

- **Linux** **AIX** V systému AIX and Linux:

```
MQ_INSTALLATION_PATH/bin/setmqenv
```

kde `MQ_INSTALLATION_PATH` odkazuje na umístění, kde je nainstalován produkt IBM MQ . Tento příkaz nastaví proměnné prostředí pro shell, ve kterém momentálně pracujete. Pokud otevřete jiný shell, musíte zadat příkaz znovu.

- **Windows** V systému Windows:

```
MQ_INSTALLATION_PATH/bin/setmqenv
```

kde `MQ_INSTALLATION_PATH` odkazuje na umístění, kde je nainstalován produkt IBM MQ .

Existují příklady, ve kterých můžete najít parametry použité v ukázkových konfiguracích. K dispozici je krátký popis každého parametru a několik pokynů, kde najít ekvivalentní hodnoty ve vašem systému. Máte-li vlastní sadu hodnot, ujistěte se, že tyto hodnoty používáte při práci s příklady v této sekci.

Tyto příklady nepokrývají, jak nastavit komunikace, kde se používá klastrování. Informace o nastavení komunikace při použití klastrování naleznete v tématu [Konfigurace klastru správce front](#). Zde uvedené hodnoty konfigurace komunikace stále platí.

Existují příklady konfigurací pro následující platformy:

- **AIX** [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému AIX” na stránce 9](#)
- **IBM i** [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému IBM i” na stránce 15](#)
- **Linux** [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému Linux” na stránce 32](#)
- **Windows** [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému Windows” na stránce 38](#)
- **z/OS** [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému z/OS” na stránce 44](#)
- **z/OS** [“Příklad: Nastavení IBM MQ komunikace mezi platformami na systému z/OS pomocí QSGs” na stránce 49](#)
- **z/OS** [“Příklad: Nastavení IBM MQ mezisložkové komunikace pro řazení do front v rámci skupiny na systému z/OS” na stránce 57](#)

Povinnosti v oblasti IT

Chcete-li porozumět terminologii použité v příkladech, zvažte následující pokyny jako výchozí bod.

- Administrátor systému: Osoba (nebo skupina osob), která instaluje a konfiguruje software pro specifickou platformu.
- Správce sítě: Osoba, která řídí konektivitu LAN, přiřazení adres LAN, konvence pojmenování sítě a další úlohy sítě. Tato osoba může být v samostatné skupině nebo může být součástí skupiny administrace systému.

Ve většině instalací systému z/OS je skupina zodpovědná za aktualizaci softwaru ACF/VTAM, ACF/NCPa TCP/IP pro podporu konfigurace sítě. Osoby v této skupině jsou hlavním zdrojem informací potřebných pro připojení libovolné platformy IBM MQ k produktu IBM MQ for z/OS. Mohou také ovlivnit nebo nařídit konvence pojmenování sítě v sítích LAN a před vytvořením definic musíte ověřit jejich rozsah řízení.

- Specifický typ administrátora, například správce systému CICS , je uveden v případech, kdy můžeme jasněji popsat odpovědnost osoby.

Secke příkladu-konfigurace se nepokoušejí označit, kdo je zodpovědný za každý parametr a kdo je schopen jej nastavit. Obecně může být zapojeno několik různých lidí.

Související úlohy

“Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5

Tento příklad ukazuje, jak vytvořit funkční síť IBM MQ konfigurací odesílacího a přijímacího kanálu IBM MQ , aby byl umožněn obousměrný tok zpráv mezi platformami přes všechny podporované protokoly.

Související odkazy

[setmqenv](#)

Příklad: nastavení komunikace mezi platformami IBM MQ na systému AIX

Tento příklad ukazuje, jak nastavit komunikační odkazy z IBM MQ na AIX na IBM MQ na jiné platformě a vytvořit pracovní kanál na této platformě.

Než začnete

Informace o tomto příkladu a jeho použití naleznete v části “Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5 a “Jak používat příklady komunikace mezi platformami” na stránce 7.

Informace o této úloze

Tento příklad pokrývá nastavení komunikace mezi platformami z IBM MQ na AIX na následující platformy:

-  Windows
-  Linux
-  IBM i
-  z/OS
- VSE/ESA

Postup

1. Vytvořte síťové připojení pomocí jedné z následujících voleb.

- Vytvořte připojení LU 6.2 . Další informace o konfiguraci SNA přes TCP/IP naleznete v tématu [Komunikační server pro AIX knihovnu](#).
- Ustanovit připojení TCP.

Před spuštěním kanálů musí být modul listener explicitně spuštěn. Umožňuje automatické spuštění přijímacích kanálů v reakci na požadavek z příchozího odesílacího kanálu. Pomocí následujícího příkazu spusťte modul listener IBM MQ pro protokol TCP:

```
runmqclsr -t tcp
```

a. Upravte soubor `/etc/services`.

Poznámka: Chcete-li upravit soubor `/etc/services` , musíte být přihlášení jako superuživatel nebo uživatel root. Pokud v tomto souboru nemáte následující řádek, přidejte jej tak, jak je zobrazeno:

```
MQSeries      1414/tcp      # MQSeries channel listener
```

- b. Upravte soubor `/etc/inetd.conf`. Pokud v tomto souboru nemáte následující řádek, přidejte jej tak, jak je zobrazeno, a nahraďte adresář `MQ_INSTALLATION_PATH` adresářem vysoké úrovně, ve kterém je nainstalován produkt IBM MQ :

```
MQSeries stream tcp nowait root MQ_INSTALLATION_PATH/bin/amqcrista amqcrista  
[-m queue.manager.name]
```

- c. Zadejte příkaz `refresh -s inetd`.

Poznámka: Musíte přidat **root** do skupiny `mqm`. Nemusíte mít primární skupinu nastavenou na `mqm`. Dokud je `mqm` v sadě skupin, můžete použít příkazy. Pokud spouštíte pouze aplikace, které používají správce front, nepotřebujete oprávnění skupiny `mqm`.

2. Po vytvoření připojení definujte některé kanály, jak je popsáno v tématu [“Konfigurace kanálů v systému AIX”](#) na stránce 10.

Konfigurace kanálů v systému AIX

Chcete-li konfigurovat produkt IBM MQ pro ukázkou konfigurace v systému AIX, proveďte základní kroky konfigurace pro správce front a poté nakonfigurujte odesílací a přijímací kanály.

Než začnete

Poznámka:

1. Před zahájením procesu instalace se ujistěte, že jste nejprve vytvořili uživatele a skupinu `mqm` a nastavili heslo.
2. Pokud se instalace nezdaří v důsledku nedostatečného prostoru v systému souborů, můžete zvýšit velikost následujícím způsobem pomocí příkazu `smit C sna`. (Pomocí `df` zobrazíte stav systému souborů. Označuje logický disk, který je plný.)

```
-- Physical and Logical Storage  
-- File Systems  
-- Add / Change / Show / Delete File Systems  
-- Journalled File Systems  
-- Change/Show Characteristics of a Journalled File System
```

3. Spusťte libovolný kanál pomocí příkazu:

```
runmqchl -c channel.name
```

4. Ukázkové programy jsou nainstalovány v adresáři `MQ_INSTALLATION_PATH/samp`, kde `MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ.
5. Protokoly chyb jsou uloženy v adresáři `/var/mqm/qmgrs/qmgrname/errors`.
6. V systému AIX můžete spustit trasování komponent produktu IBM MQ pomocí standardních příkazů trasování systému IBM MQ nebo pomocí trasování systému AIX. Další informace o trasování systému IBM MQ Trace and AIX naleznete v tématu [Použití trasování](#).
7. Používáte-li k zadání příkazů administrace interpret příkazů **runmqsc**, znak `+` na konci řádku označuje, že další řádek je pokračováním. Ujistěte se, že mezi posledním parametrem a pokračujícím znakem je mezera.

Postup

1. Chcete-li provést základní konfiguraci pro správce front, postupujte takto:
 - a) Vytvořte správce front z příkazového řádku AIX pomocí příkazu:

```
crtmqm -u dlqname -q aix
```

kde:

aix

Název správce front

-q

Označuje, že se má stát výchozím správcem front

-u *dlname*

Určuje název nedoručitelné fronty zpráv.

Tento příkaz vytvoří správce front a sadu výchozích objektů.

b) Spusťte správce front z příkazového řádku AIX pomocí příkazu:

```
strmqm aix
```

kde *aix* je název zadaný správcem front při jeho vytvoření.

c) Spusťte příkaz **runmqsc** z příkazového řádku AIX a použijte jej k vytvoření nedoručitelné fronty zpráv zadáním příkazu:

```
def ql (dlname)
```

kde *dlname* je název zadaný nedoručitelné frontě zpráv při vytvoření správce front.

2. Nakonfigurujte kanály pro ukázkou konfigurace.

Další informace o parametrech použitých v následujících příkladech viz [“Konfigurační parametry kanálu pro AIX”](#) na stránce 12. V každém případě příklad zobrazuje příkaz MQSC. Buď spusťte příkaz **runmqsc** z příkazového řádku AIX a zadejte postupně každý příkaz, nebo sestavte příkazy do příkazového souboru.

Windows Tyto příklady slouží k připojení systému IBM MQ on AIX s IBM MQ on Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte místo hodnot parametru Windows příslušné hodnoty z tabulek v souboru [“Konfigurační parametry kanálu pro AIX”](#) na stránce 12 .

a) Definujte kanál odesílatele, jak je uvedeno v následujících příkladech:

- Použití SNA:

```
def ql (WINNT) +                               F
  usage(xmitq) +
  replace

def qr (WINNT.REMOTEQ) +                       D
  rname(WINNT.LOCALQ) +                       E
  rqmname(WINNT) +                             C
  xmitq(WINNT) +                               F
  replace

def chl (AIX.WINNT.SNA) chltype(sdr) +        G
  trptype(lu62) +
  conname('WINNTCPIC') +                      17
  xmitq(WINNT) +                               F
  replace
```

- Použití TCP:

```
def ql (WINNT) +                               F
  usage(xmitq) +
  replace

def qr (WINNT.REMOTEQ) +                       D
  rname(WINNT.LOCALQ) +                       E
  rqmname(WINNT) +                             C
  xmitq(WINNT) +                               F
  replace

def chl (AIX.WINNT.TCP) chltype(sdr) +        H
  trptype(tcp) +
```

```
conname(remote_tcpip_hostname) +
xmitq(WINNT) +
replace F
```

b) Definujte přijímací kanál, jak je uvedeno v následujících příkladech:

- Použití SNA:

```
def ql (AIX.LOCALQ) replace B
def chl (WINNT.AIX.SNA) chltype(rcvr) +
trptype(lu62) +
replace I
```

- Použití TCP:

```
def ql (WINNT) +
usage(xmitq) +
replace F
def qr (WINNT.REMOTEQ) +
rname(WINNT.LOCALQ) +
rqmname(WINNT) +
xmitq(WINNT) +
replace D
E
C
F
def chl (AIX.WINNT.TCP) chltype(sdr) +
trptype(tcp) +
conname(remote_tcpip_hostname) +
xmitq(WINNT) +
replace H
F
```

Poznámka: Existují alternativní způsoby, jak zajistit, aby se přijímací kanály SNA správně aktivovaly, když odesílací kanál zahájí konverzaci.

Během procesu konfigurace serveru AIX Communications Server byl vytvořen profil LU 6.2 TPN, který obsahoval úplnou cestu ke spustitelnému programu TP. V tomto příkladu byl soubor nazván `/u/interop/AIX.crs6a`. Můžete zvolit název, ale zvažte jeho zahrnutí do názvu správce front. Obsah spustitelného souboru musí být:

```
#!/bin/sh
MQ_INSTALLATION_PATH/bin/amqcrs6a -m aix
```

kde `aix` je název správce front (A) a `MQ_INSTALLATION_PATH` je adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ. Po vytvoření tohoto souboru jej povolte pro provedení spuštěním příkazu:

```
chmod 755 /u/interop/AIX.crs6a
```

Jako alternativu k vytvoření spustitelného souboru můžete zadat cestu na panelu Přidat profil TPN LU 6.2 pomocí parametrů příkazového řádku.

Zadáním cesty jedním z těchto dvou způsobů zajistíte, že kanály příjemce SNA budou správně aktivovány, když kanál odesílatele zahájí konverzaci.

Konfigurační parametry kanálu pro AIX

Parametry potřebné ke konfiguraci kanálů pro ukázkou konfigurace v systému AIX.

Krok “2” na stránce 11 z “Konfigurace kanálů v systému AIX” na stránce 10 popisuje konfiguraci, která má být provedena ve správci front AIX za účelem implementace kanálu popsaného v části “Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5. Příklady v části “Konfigurace kanálů v systému AIX” na stránce 10 jsou pro připojení IBM MQ for IBM i a IBM MQ for Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte hodnoty z příslušné tabulky namísto hodnot pro Windows.

Poznámka: Slova **tučně** jsou navrhované hodnoty a odrážejí názvy objektů IBM MQ použité v těchto příkladech. Můžete je změnit v instalaci produktu, ale pokud tak učiníte, ujistěte se, že při práci s příklady v této sekci používáte své vlastní hodnoty.

Definice lokálního uzlu

<i>Tabulka 1. Příklady konfigurace pro definici lokálního uzlu</i>			
ID	Název parametru	Odkaz	Použitý příklad
A	Název správce front		AIX
B	Název lokální fronty		AIX.LOCALQ

Připojení k IBM MQ on Windows

Windows

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro Windows” na stránce 42, jak je uvedeno.

<i>Tabulka 2. Příklady konfigurace pro připojení k systému IBM MQ on Windows</i>			
ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	WINNT
D	Název vzdálené fronty		WINNT.REMOTEQ
E	Název fronty na vzdáleném systému	B	WINNT.LOCALQ
F	Jméno přenosové fronty		WINNT
G	Název kanálu odesílatele (SNA)		AIX.WINNT.SNA
H	Název kanálu odesílatele (TCP/IP)		AIX.WINNT.TCP
I	Název kanálu příjemce (SNA)	G	WINNT.AIX.SNA
J	Název kanálu příjemce (TCP)	H	WINNT.AIX.TCP

Připojení k IBM MQ on Linux

Linux

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro Linux” na stránce 36, jak je uvedeno.

<i>Tabulka 3. Příklady konfigurace pro připojení k systému IBM MQ on Linux</i>			
ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	LINUX
D	Název vzdálené fronty		LINUX.REMOTEQ
E	Název fronty na vzdáleném systému	B	LINUX.LOCALQ
F	Jméno přenosové fronty		LINUX
G	Název kanálu odesílatele (SNA)		AIX.LINUX.SNA
H	Název kanálu odesílatele (TCP/IP)		AIX.LINUX.TCP
I	Název kanálu příjemce (SNA)	G	LINUX.AIX.SNA
J	Název kanálu příjemce (TCP/IP)	H	LINUX.AIX.TCP

Připojení k IBM MQ on IBM i

IBM i

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro IBM i” na stránce 29, jak je uvedeno.

Tabulka 4. Příklady konfigurace pro připojení k systému IBM MQ on IBM i

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	AS400
D	Název vzdálené fronty		AS400.REMOTEQ
E	Název fronty na vzdáleném systému	B	AS400.LOCALQ
F	Jméno přenosové fronty		AS400
G	Název kanálu odesílatele (SNA)		AIX.AS400.SNA
H	Název kanálu odesílatele (TCP)		AIX.AS400.TCP
I	Název kanálu příjemce (SNA)	G	AS400.AIX.SNA
J	Název kanálu příjemce (TCP)	H	AS400.AIX.TCP

Připojení k IBM MQ for z/OS

z/OS

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro z/OS” na stránce 47, jak je uvedeno.

Tabulka 5. Příklady konfigurace pro připojení k produktu IBM MQ for z/OS

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	MVS
D	Název vzdálené fronty		MVS.REMOTEQ
E	Název fronty na vzdáleném systému	B	MVS.LOCALQ
F	Jméno přenosové fronty		MVS
G	Název kanálu odesílatele (SNA)		AIX.MVS.SNA
H	Název kanálu odesílatele (TCP)		AIX.MVS.TCP
I	Název kanálu příjemce (SNA)	G	MVS.AIX.SNA
J	Název kanálu příjemce (TCP)	H	MVS.AIX.TCP

Připojení k produktu IBM MQ for z/OS pomocí skupin sdílení front

z/OS

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry sdíleného kanálu” na stránce 55, jak je uvedeno.

Tabulka 6. Příklady konfigurace pro připojení k produktu IBM MQ for z/OS pomocí skupin sdílení front

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	QSG
D	Název vzdálené fronty		QSG.REMOTEQ

Tabulka 6. Příklady konfigurace pro připojení k produktu IBM MQ for z/OS pomocí skupin sdílení front (pokračování)

ID	Název parametru	Odkaz	Použitý příklad
E	Název fronty na vzdáleném systému	B	QSG.SHAREDQ
F	Jméno přenosové fronty		QSG
G	Název kanálu odesílatele (SNA)		AIX.QSG.SNA
H	Název kanálu odesílatele (TCP)		AIX.QSG.TCP
I	Název kanálu příjemce (SNA)	G	QSG.AIX.SNA
J	Název kanálu příjemce (TCP)	H	QSG.AIX.TCP

IBM i **Příklad: nastavení komunikace mezi platformami IBM MQ na systému IBM i**




Tento příklad ukazuje, jak nastavit komunikační odkazy z IBM MQ na IBM i na IBM MQ na jiné platformě a vytvořit pracovní kanál na této platformě.

Než začnete

Informace o tomto příkladu a jeho použití naleznete v části [“Příklad: Nastavení komunikace mezi platformami pro IBM MQ”](#) na stránce 5 a [“Jak používat příklady komunikace mezi platformami”](#) na stránce 7.

Informace o této úloze

Tento příklad pokrývá nastavení komunikace mezi platformami z IBM MQ na IBM i na následující platformy:

-  Windows
-  AIX
-  Linux
-  z/OS nebo MVS
- VSE/ESA

Postup

1. Vytvořte síťové připojení pomocí jedné z následujících voleb.
 - Vytvořte připojení LU 6.2, jak je popsáno v tématu [“Vytvoření připojení LU 6.2 na systému IBM i”](#) na stránce 15.
 - Vytvořte připojení TCP, jak je popsáno v tématu [“Vytvoření připojení TCP na systému IBM i”](#) na stránce 24.
2. Po vytvoření připojení definujte některé kanály, jak je popsáno v tématu [“Konfigurace kanálů v systému IBM i”](#) na stránce 26.

IBM i **Vytvoření připojení LU 6.2 na systému IBM i**

Chcete-li vytvořit připojení LU 6.2 v systému IBM i, musíte nakonfigurovat lokální uzel a připojit jej k partnerskému uzlu.

Informace o této úloze

Další informace o parametrech, které jsou potřebné pro nastavení komunikace ze systému IBM i na jednu z ostatních platform IBM MQ, naleznete v tabulkách v části “[Konfigurační parametry pro připojení LU 6.2 v systému IBM i](#)” na stránce [20](#). Čísla v závorkách () v krocích úlohy odpovídají hodnotám ve sloupci *ID* těchto tabulek.

Chcete-li konfigurovat lokální uzel, musíte:

- Vytvořit popis linky
- Přidat položku směrování a poté spustit subsystém

Chcete-li se připojit k partnerskému uzlu, musíte:

- Vytvořit popis řadiče
- Vytvořit popis zařízení
- Vytvořit informace o straně CPI-C
- Přidat komunikační záznam pro APPC
- Přidat položku konfiguračního seznamu

Postup

1. Nakonfigurujte lokální uzel vytvořením popisu linky a přidáním záznamu směrování.

a) Vytvořte popis linky.

Pokud popis linky ještě nebyl vytvořen, použijte příkaz **CRTLINTRN** k uvedení hodnot pro **Popis linky** (6) a **Název prostředku** (7), jak ukazuje následující příklad:

```
Create Line Desc (token-ring) (CRTLINTRN)
Type choices, press Enter.

Line description . . . . . TOKENRINGL Name
Resource name . . . . . LIN041 Name, *NWID
NWI type . . . . . *FR *FR, *ATM
Online at IPL . . . . . *YES *YES, *NO
Vary on wait . . . . . *NOWAIT *NOWAIT, 15-180 (1 second)
Maximum controllers . . . . . 40 1-256
Attached NWI . . . . . *NONE Name, *NONE

Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys
Parameter LIND required. +
```

b) Přidejte položku směrování.

Zadejte příkaz **ADDRTGE** a stiskněte klávesu Enter, poté zadejte vlastní hodnotu pro **Popis subsystému** (5) a hodnoty, které jsou uvedeny v následujícím příkladu pro **Pořadové číslo položky směrování**, **Porovnat hodnotu** (8), **Počáteční pozici**, **Program pro volání knihovny** obsahující program pro volání.


```

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, * LI BL, *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
Parameter SBSDB required.
+

```

Spustíte subsystém zadáním příkazu STRSBS *subsystem description* (5) a stisknutím klávesy Enter.

2. Vytvořte připojení k partnerskému uzlu vytvořením popisu řadiče, popisu zařízení a informací o připojení CPI-C a přidáním záznamu komunikace pro APPC a záznamu konfiguračního seznamu.

Windows Tento příklad je pro připojení k systému Windows , ale kroky jsou stejné pro ostatní uzly.

a) Vytvořit popis řadiče

Na příkazovém řádku zadejte CRTCTLAPPC a stiskněte klávesu Enter, pak zadejte hodnoty pro **Popis řadiče** (12), nastavte **Typ odkazu** na *LANa nastavte **Online při IPL** na *NO.

```

Create Ctl Desc (APPC) (CRTCTLAPPC)

Type choices, press Enter.

Controller description . . . . . WINNTCP      Name
Link type . . . . . *LAN      *FAX, *FR, *IDLC,
*LAN...
Online at IPL . . . . . *NO      *YES, *NO

Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys
Parameter CTLD required.
+

```

Stiskněte dvakrát klávesu Enter, následovanou klávesou F10, pak uveďte hodnoty pro **Seznam komutovaných linek** (6), **Identifikátor vzdálené sítě** (9), **Vzdálený řídicí bod** (10) a **Adresa vzdáleného adaptéru LAN** (16) a stiskněte klávesu Enter.

```

Create Ctl Desc (APPC) (CRTCTLAPPC)

Type choices, press Enter.

Controller description . . . . . > WINNTCP      Name
Link type . . . . . > *LAN      *FAX, *FR, *IDLC, *LAN...
Online at IPL . . . . . > *NO      *YES, *NO
APPN-capable . . . . . *YES      *YES, *NO
Switched line list . . . . . TOKENRINGL Name
+ for more values
Maximum frame size . . . . . *LINKTYPE 265-16393, 256, 265, 512...
Remote network identifier . . . NETID      Name, *NETATR, *NONE, *ANY
Remote control point . . . . . WINNTCP      Name, *ANY
Exchange identifier . . . . . 00000000-FFFFFFF
Initial connection . . . . . *DIAL      *DIAL, *ANS
Dial initiation . . . . . *LINKTYPE *LINKTYPE, *IMMED, *DELAY
LAN remote adapter address . . 10005AFC5D83 000000000001-FFFFFFF
APPN CP session support . . . . *YES      *YES, *NO
APPN node type . . . . . *ENDNODE *ENDNODE, *LENNODE...
APPN transmission group number 1      1-20, *CALC
More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

```

b) Vytvořte popis zařízení.

Zadejte příkaz CRTDEVAPPC a stiskněte klávesu Enter, pak zadejte hodnoty pro **Popis zařízení (13)**, **Vzdálené umístění (11)**, **Lokální umístění (3)**, **Identifikátor vzdálené sítě (9)** a **Připojený řadič (12)**.

```

Create Device Desc (APPC) (CRTDEVAPPC)

Type choices, press Enter.

Device description . . . . . WINNTLU      Name
Remote location . . . . . WINNTLU      Name
Online at IPL . . . . . *YES      *YES, *NO
Local location . . . . . AS400LU      Name, *NETATR
Remote network identifier . . . NETID      Name, *NETATR, *NONE
Attached controller . . . . . WINNTCP      Name
Mode . . . . . *NETATR      Name, *NETATR
+ for more values
Message queue . . . . . QSYSOPR      Name, QSYSOPR
Library . . . . . *LIBL      Name, *LIBL, *CURLIB
APPN-capable . . . . . *YES      *YES, *NO
Single session:
Single session capable . . . . *NO      *NO, *YES
Number of conversations . . . . 1-512

Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys
Parameter DEVD required.      +

```

Poznámka: Můžete se vyhnout nutnosti vytvářet popisy řadičů a zařízení ručně tím, že využijete službu automatické konfigurace IBM i. Další informace naleznete v dokumentaci agenta IBM i.

c) Vytvořte informace o připojení CPI-C.

Zadejte CRTCSI a stiskněte klávesu F10, pak zadejte hodnoty pro **Informace o připojení (14)**, **Vzdálené umístění (11)**, **Transakční program (15)**, **Lokální umístění (3)**, **Režima Identifikátor vzdálené sítě (9)** a stiskněte klávesu Enter.

```

Create Comm Side Information (CRTCSI)

Type choices, press Enter.

Side information . . . . . NTCPIC      Name
Library . . . . . *CURLIB      Name, *CURLIB
Remote location . . . . . WINNTLU    Name
Transaction program . . . . . MQSERIES

Text 'description' . . . . . *BLANK

Additional Parameters

Device . . . . . *LOC      Name, *LOC
Local location . . . . . AS400LU    Name, *LOC, *NETATR
Mode . . . . . #INTER      Name, *NETATR
Remote network identifier . . . . . NETID    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
Parameter CSI required.

```

d) Přidejte komunikační záznam pro APPC.

Na příkazovém řádku zadejte ADDCMNE a stiskněte klávesu Enter, pak uveďte hodnoty pro **Popis subsystému** (5) a **Zařízení** (13) a stiskněte znovu klávesu Enter.

```

Add Communications Entry (ADDCMNE)

Type choices, press Enter.

Subsystem description . . . . . QCMN      Name
Library . . . . . *LIBL      Name, *LIBL, *CURLIB
Device . . . . . WINNTLU    Name, generic*, *ALL...
Remote location . . . . .      Name
Job description . . . . . *USRPRF    Name, *USRPRF, *SBSD
Library . . . . .      Name, *LIBL, *CURLIB
Default user profile . . . . . *NONE    Name, *NONE, *SYS
Mode . . . . . *ANY      Name, *ANY
Maximum active jobs . . . . . *NOMAX    0-1000, *NOMAX

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
Parameter SBSDB required.

```

e) Přidejte položku konfiguračního seznamu.

Zadejte ADDCFGLE *APPNRMT a stiskněte klávesu F4, pak uveďte hodnoty pro **Název vzdáleného systému** (11), **Identifikátor vzdálené sítě** (9), **Název lokálního systému** (3), **Název vzdáleného řídicího bodu** (10) a **ID sítě řídicího bodu** (9) a stiskněte klávesu Enter.

```

Add Configuration List Entries (ADDCFGLE)

Type choices, press Enter.

Configuration list type . . . . > *APPNRMT *APPNLCL, *APPNRMT...
APPN remote location entry:
Remote location name . . . . . WINNTLU Name, generic*, *ANY
Remote network identifier . . . NETID Name, *NETATR, *NONE
Local location name . . . . . AS400LU Name, *NETATR
Remote control point . . . . . WINNTCP Name, *NONE
Control point net ID . . . . . NETID Name, *NETATR, *NONE
Location password . . . . . *NONE
Secure location . . . . . *NO *YES, *NO
Single session . . . . . *NO *YES, *NO
Locally controlled session . . *NO *YES, *NO
Pre-established session . . . *NO *YES, *NO
Entry 'description' . . . . . *BLANK
Number of conversations . . . 10 1-512
+ for more values

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

```

Jak pokračovat dále

Připojení LU 6.2 je nyní navázáno. Jste připraveni dokončit konfiguraci, jak je popsáno v tématu [“Konfigurace kanálů v systému IBM i”](#) na stránce 26.

Související úlohy

[“Vytvoření připojení TCP na systému IBM i”](#) na stránce 24

Pokud je protokol TCP již nakonfigurován, nejsou žádné další konfigurační úlohy. Pokud není TCP/IP nakonfigurován, musíte přidat rozhraní TCP/IP, přidat rozhraní zpětné smyčky TCP/IP a přidat předvolenou přenosovou cestu.

Konfigurační parametry pro připojení LU 6.2 v systému IBM i

Parametry potřebné pro nastavení komunikace ze systému IBM MQ na systému IBM i na jednu z ostatních platforem IBM MQ pomocí připojení LU 6.2 .

Tyto tabulky použijte s tabulkami pro platformu, ke které se připojujete.

Pokud jsou čísla uvedena ve sloupci *Odkaz* , označují, že hodnota se musí shodovat s hodnotou v příslušné tabulce jinde v této sekci. Kroky úlohy v souboru [“Vytvoření připojení LU 6.2 na systému IBM i”](#) na stránce 15 odkazují na hodnoty ve sloupci *ID* této tabulky.

Položky ve sloupci *Název parametru* jsou vysvětleny v části [“Vysvětlení termínů použitých v tabulkách”](#) na stránce 23.

Definice lokálního uzlu

Tabulka 7. Příklady konfigurace pro definici lokálního uzlu			
ID	Název parametru	Odkaz	Použitý příklad
1	ID lokální sítě		ID sítě
2	Název lokálního řídicího bodu		AS400PU
3	Název jednotky LU		AS400LU
4	Cílová adresa LAN		10005A5962EF
5	Popis subsystému		QCMN
6	Popis linky		TOKENRINGL

Tabulka 7. Příklady konfigurace pro definici lokálního uzlu (pokračování)

ID	Název parametru	Odkaz	Použitý příklad
7	Název prostředku		LIN041
8	název lokálního programu transakce		MQSERIES

Připojení k IBM MQ on Windows

Windows

Windows

Tabulka 8. Příklady konfigurace pro připojení k systému IBM MQ on Windows

ID	Název parametru	Odkaz	Použitý příklad
9	ID sítě	2	ID sítě
10	Název řídicího bodu	3	WINNTCP
11	Název jednotky LU	5	WINNTLU
12	Popis řadiče		WINNTCP
13	Zařízení		WINNTLU
14	Informace o straně		NTCPIC
15	Transakční program	7	MQSERIES
16	Adresa adaptéru LAN	9	08005AA5FAB9
17	Režim	17	#INTER

Připojení k IBM MQ on AIX

AIX

Tabulka 9. Příklady konfigurace pro připojení k systému IBM MQ na systému AIX

ID	Název parametru	Odkaz	Použitý příklad
9	ID sítě	1	ID sítě
10	Název řídicího bodu	2	AIXPU
11	Název jednotky LU	4	AIXLU
12	Popis řadiče		AIXPU
13	Zařízení		AIXLU
14	Informace o straně		AIXCPIC
15	Transakční program	6	MQSERIES
16	Adresa adaptéru LAN	8	123456789012
17	Režim	14	#INTER

Připojení k systému IBM MQ na platformě Linux (x86)

Linux

<i>Tabulka 10. Příklady konfigurace pro připojení k systému IBM MQ on Linux (platformax86)</i>			
ID	Název parametru	Odkaz	Použitý příklad
9	ID sítě	4	ID sítě
10	Název řídicího bodu	2	LINUXPU
11	Název jednotky LU	5	LINUXLU
12	Popis řadiče		LINUXPU
13	Zařízení		LINUXLU
14	Informace o straně		LXCPIK
15	Transakční program	7	MQSERIES
16	Adresa adaptéru LAN	8	08005AC6DF33
17	Režim	6	#INTER

Připojení k IBM MQ for z/OS



<i>Tabulka 11. Příklady konfigurace pro připojení k produktu IBM MQ for z/OS</i>			
ID	Název parametru	Odkaz	Použitý příklad
9	ID sítě	2	ID sítě
10	Název řídicího bodu	3	MVSPU
11	Název jednotky LU	4	MVSLU
12	Popis řadiče		MVSPU
13	Zařízení		MVSLU
14	Informace o straně		MVSCPIK
15	Transakční program	7	MQSERIES
16	Adresa adaptéru LAN	8	400074511092
17	Režim	6	#INTER

Připojení k systému VSE/ESA

<i>Tabulka 12. Příklady konfigurace pro připojení k systému VSE/ESA</i>			
ID	Název parametru	Odkaz	Použitý příklad
9	ID sítě	1	ID sítě
10	Název řídicího bodu	2	VSEPU
11	Název jednotky LU	3	VSELU
12	Popis řadiče		VSEPU
13	Zařízení		VSELU
14	Informace o straně		VSECPIC
15	Transakční program	4	MQ01
16	Adresa adaptéru LAN	5	400074511092

Tabulka 12. Příklady konfigurace pro připojení k systému VSE/ESA (pokračování)			
ID	Název parametru	Odkaz	Použitý příklad
17	Režim		#INTER

Vysvětlení termínů použitých v tabulkách

1 2 3

Informace o tom, jak vyhledat nakonfigurované hodnoty, viz [“Jak najít atributy sítě”](#) na stránce 23.

4 LAN cílová adresa

Hardwarová adresa adaptéru token-ringů systému IBM i . Hodnotu můžete najít pomocí příkazu `DSPLIND Line description (6)`.

5 Popis subsystému

Tento parametr je název libovolného subsystému IBM i , který je aktivní při používání správce front. Název QCMN byl použit, protože se jedná o komunikační subsystém IBM i .

6 Popis linky

Pokud byl tento parametr uveden, je uveden v poli Popis názvu prostředku. Další informace viz téma [“Jak najít hodnotu názvu prostředku”](#) na stránce 24. Není-li hodnota uvedena, musíte vytvořit popis linky.

7 Název prostředku

Informace o tom, jak vyhledat nakonfigurovanou hodnotu, viz [“Jak najít hodnotu názvu prostředku”](#) na stránce 24.

8 Název lokálního transakčního programu

Aplikace IBM MQ , které se pokoušejí konverzovat s touto pracovní stanicí, uvádějí symbolický název programu, který se má spustit na přijímacím konci. Tento název je definován v definici kanálu u odesílatele. Pro zjednodušení, kdykoli je to možné, použijte název transakčního programu MQSERIES nebo v případě připojení k systému VSE/ESA, kde je délka omezena na 4 bajty, použijte MQTP.

Další informace naleznete v tématu [Nastavení v lokálním systému IBM i pro vzdálenou platformu správce front](#) .

12 Popis řadiče

Tento parametr je alias pro název řídicího bodu (nebo název uzlu) partnerského systému. Pro usnadnění jsme v tomto příkladu použili skutečné jméno partnera.

13 Zařízení

Tento parametr je alias pro LU partnerského systému. Pro usnadnění jsme v tomto příkladu použili jméno LU partnera.

14 Informace o straně

Tento parametr je název poskytnutý profilu informací o připojení CPI-C. Zadáte svůj vlastní osmiznakový název.

Jak najít atributy sítě

Lokální uzel byl částečně nakonfigurován jako součást instalace produktu IBM i . Chcete-li zobrazit aktuální atributy sítě, zadejte příkaz **DSPNETA**.

Potřebujete-li tyto hodnoty změnit, použijte příkaz **CHGNETA**. K použití změn může být požadován IPL.

```

Display Network Attributes
System: AS400PU
Current system name . . . . . : AS400PU
Pending system name . . . . . :
Local network ID . . . . . : NETID
Local control point name . . . . . : AS400PU
Default local location . . . . . : AS400LU
Default mode . . . . . : BLANK
APPN node type . . . . . : *ENDNODE
Data compression . . . . . : *NONE
Intermediate data compression . . . . . : *NONE
Maximum number of intermediate sessions . . . . . : 200
Route addition resistance . . . . . : 128
Server network ID/control point name . . . . . : NETID NETCP

```

More...
Press Enter to continue.

F3=Exit F12=Cancel

Zkontrolujte, zda hodnoty pro **ID lokální sítě (1)**, **název lokálního řídicího bodu (2)** a **výchozí lokální umístění (3)** odpovídají hodnotám v tabulce, nebo vaše vlastní hodnoty, pokud jste je změnili.

Jak najít hodnotu názvu prostředku

Chcete-li vyhledat hodnotu názvu prostředku, zadejte WRKHDWRSC TYPE(*CMN) a stiskněte klávesu Enter.

Zobrazí se panel Práce s prostředky komunikace. Hodnota pro **Název prostředku** je nalezena jako port token-ring. V tomto příkladu je to LIN041.

```

Work with Communication Resources
System: AS400PU
Type options, press Enter.
2=Edit 4=Remove 5=Work with configuration description
7=Add configuration description ...

```

```

Configuration
Opt Resource      Description Type Description
CC02              2636 Comm Processor
LIN04             2636 LAN Adapter
LIN041  TOKEN-RING 2636 Token-ring Port

```

Bottom
F3=Exit F5=Refresh F6=Print F11=Display resource addresses/statuses
F12=Cancel F23=More options

IBM i Vytvoření připojení TCP na systému IBM i

Pokud je protokol TCP již nakonfigurován, nejsou žádné další konfigurační úlohy. Pokud není TCP/IP nakonfigurován, musíte přidat rozhraní TCP/IP, přidat rozhraní zpětné smyčky TCP/IP a přidat předvolenou přenosovou cestu.

Postup

1. Přidejte rozhraní TCP/IP.

Na příkazovém řádku zadejte ADDTCPIFC a stiskněte klávesu Enter, pak uveďte **adresu IP a popis linky masku podsítě** počítače a stiskněte znovu klávesu Enter.

```
Add TCP/IP Interface (ADDTCPIFC)

Type choices, press Enter.

Internet address . . . . . 19.22.11.55
Line description . . . . . TOKENRINGL Name, *LOOPBACK
Subnet mask . . . . . 255.255.0.0
Type of service . . . . . *NORMAL *MINDELAY, *MAXTHRPUT..
Maximum transmission unit . . . *LIND 576-16388, *LIND
Autostart . . . . . *YES *YES, *NO
PVC logical channel identifier 001-FFF
+ for more values
X.25 idle circuit timeout . . . 60 1-600
X.25 maximum virtual circuits . 64 0-64
X.25 DDN interface . . . . . *NO *YES, *NO
TRLAN bit sequencing . . . . . *MSB *MSB, *LSB

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
```

2. Přidejte rozhraní zpětné smyčky TCP/IP.

Na příkazový řádek zadejte ADDTCPIFC a stiskněte klávesu Enter. Poté zadejte hodnoty pro **adresu IP, popis linky masku podsítě**.

```
Add TCP Interface (ADDTCPIFC)

Type choices, press Enter.

Internet address . . . . . 127.0.0.1
Line description . . . . . *LOOPBACK Name, *LOOPBACK
Subnet mask . . . . . 255.0.0.0
Type of service . . . . . *NORMAL *MINDELAY, *MAXTHRPUT..
Maximum transmission unit . . . *LIND 576-16388, *LIND
Autostart . . . . . *YES *YES, *NO
PVC logical channel identifier 001-FFF
+ for more values
X.25 idle circuit timeout . . . 60 1-600
X.25 maximum virtual circuits . 64 0-64
X.25 DDN interface . . . . . *NO *YES, *NO
TRLAN bit sequencing . . . . . *MSB *MSB, *LSB

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
```

3. Přidejte výchozí trasu.

Na příkazový řádek napište ADDTCP RTE a stiskněte klávesu Enter, pak uveďte hodnoty odpovídající vaší síti a stiskněte klávesu Enter pro vytvoření výchozího záznamu přenosové cesty.

```

Add TCP Route (ADDTCPRTE)

Type choices, press Enter.

Route destination . . . . . *DFTROUTE
Subnet mask . . . . . *NONE
Type of service . . . . . *NORMAL      *MINDELAY, *MAXTHRPUT.
Next hop . . . . . 19.2.3.4
Maximum transmission unit . . . 576      576-16388, *IFC

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
Command prompting ended when user pressed F12.

```

Jak pokračovat dále

Připojení TCP je nyní navázáno. Jste připraveni dokončit konfiguraci, jak je popsáno v tématu [“Konfigurace kanálů v systému IBM i”](#) na stránce 26.

Související úlohy

[“Vytvoření připojení LU 6.2 na systému IBM i”](#) na stránce 15

Chcete-li vytvořit připojení LU 6.2 v systému IBM i, musíte nakonfigurovat lokální uzel a připojit jej k partnerskému uzlu.

Konfigurace kanálů v systému IBM i

Chcete-li konfigurovat produkt IBM MQ pro ukázkou konfigurace v systému IBM i, proveďte základní kroky konfigurace pro správce front a poté nakonfigurujte odesílací a přijímací kanály.

Informace o této úloze

Pomocí příkazu **WRKMQMQ** zobrazte nabídku konfigurace IBM MQ .

Spusťte modul listener kanálu TCP pomocí příkazu **STRMQLSR**.

Spusťte libovolný odesílací kanál pomocí příkazu **STRMQMCHL** *CHLNAME(channel_name)*.

Poznámka: Chyby AMQ* jsou umístěny v protokolu vztahujícím se k úloze, která našla chybu. Pomocí příkazu **WRKACTJOB** zobrazte seznam úloh. Pod názvem subsystému QSYSWRK vyhledejte úlohu a zadejte pro ni hodnotu 5 , abyste mohli s touto úlohou pracovat. IBM MQ protokoly mají předponu AMQ.

Postup

1. Vytvořte správce front.
 - a) Napište CRTMQM a stiskněte klávesu Enter.

```

Create Message Queue Manager (CRTMQM)

Type choices, press Enter.
Message Queue Manager name . . .
Text 'description' . . . . . *BLANK
Trigger interval . . . . . 999999999 0-999999999
Undelivered message queue . . . *NONE
Default transmission queue . . . *NONE
Maximum handle limit . . . . . 256 1-999999999
Maximum uncommitted messages . . 1000 1-10000
Default Queue manager . . . . . *NO *YES, *NO

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

```

- b) Do pole **Název správce front zpráv** zadejte AS400 a do pole **Nedoručená fronta zpráv** zadejte DEAD.LETTER.QUEUE a stiskněte klávesu Enter.
- c) Spustíte správce front zadáním příkazu STRMQM MQMNAME(AS400).
- d) Vytvořte nedoručenou frontu zpráv pomocí následujících parametrů:

```

Local Queue
Queue name : DEAD.LETTER.QUEUE
Queue type : *LCL

```

Další informace a příklad, jak definovat frontu, viz krok "2" na stránce 27.

2. Definujte frontu.

- a) Do příkazového řádku zadejte CRTMQMQ .

```

Create MQM Queue (CRTMQMQ)

Type choices, press Enter.
Queue name . . . . .
Queue type . . . . . *ALS, *LCL, *RMT

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
Parameter QNAME required.

```

- b) Vyplňte dvě pole tohoto panelu a stiskněte klávesu Enter.
Pak se zobrazí další panel se zadávanými poli pro ostatní parametry, které máte. Předvolby lze použít pro všechny ostatní atributy fronty.

3. Definujte kanál.

- a) Zadáním hodnoty CRTMQMCHL do příkazového řádku zobrazte panel **Vytvořit kanál MQM**.

```
Create MQM Channel (CRTMQMCHL)
Type choices, press Enter.
Channel name . . . . .
Channel type . . . . .          *RCVR, *SDR, *SVR, *RQSTR

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
Parameter CHLNAME required.
```

- b) Vyplňte dvě pole tohoto panelu a stiskněte klávesu Enter.

Pak se zobrazí další panel, na kterém můžete zadat hodnoty pro ostatní parametry uvedené dříve. Výchozí nastavení lze použít pro všechny ostatní atributy kanálu.

4. Nakonfigurujte kanály pro ukázkou konfigurace.

Další informace o parametrech použitých v následujících příkladech viz [“Konfigurační parametry kanálu pro IBM i”](#) na stránce 29.

Windows Tyto příklady slouží k připojení systému IBM MQ on IBM i s IBM MQ on Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte místo hodnot parametru Windows příslušné hodnoty z tabulek v souboru [“Konfigurační parametry kanálu pro IBM i”](#) na stránce 29.

- a) Definujte kanál odesilatele, jak je uvedeno v následujících příkladech:

- Použití SNA:

```
Local Queue
  Queue name :      WINNT                F
  Queue type  :      *LCL
  Usage      :      *TMQ

Remote Queue
  Queue name :      WINNT.REMOTEQ        D
  Queue type  :      *RMT
  Remote queue :      WINNT.LOCALQ        E
Remote Queue Manager :      WINNT        C
Transmission queue :      WINNT          F

Sender Channel
  Channel Name :      AS400.WINNT.SNA     G
  Channel Type  :      *SDR
  Transport type :      *LU62
  Connection name :      WINNTCPIC        14
Transmission queue :      WINNT          F
```

- Použití TCP:

```
Local Queue
  Queue name :      WINNT                F
  Queue type  :      *LCL
  Usage      :      *TMQ
```

```

Remote Queue
  Queue name :    WINNT.REMOTEQ           D
  Queue type  :    *RMT
  Remote queue :    WINNT.LOCALQ         E
Remote Queue Manager :    WINNT          C
Transmission queue :    WINNT           F

Sender Channel
  Channel Name :    AS400.WINNT.TCP      H
  Channel Type :    *SDR
  Transport type :    *TCP
  Connection name :    WINNT.tcpip.hostname
  Transmission queue :    WINNT           F

```

b) Definujte přijímací kanál, jak je uvedeno v následujících příkladech:

- Použití SNA:

```

Local Queue
  Queue name :    AS400.LOCALQ           B
  Queue type  :    *LCL

Receiver Channel
  Channel Name :    WINNT.AS400.SNA      I
  Channel Type :    *RCVR
  Transport type :    *LU62

```

- Použití TCP:

```

Local Queue
  Queue name :    AS400.LOCALQ           B
  Queue type  :    *LCL

Receiver Channel
  Channel Name :    WINNT.AS400.TCP      J
  Channel Type :    *RCVR
  Transport type :    *TCP

```

Konfigurační parametry kanálu pro IBM i

Parametry potřebné ke konfiguraci kanálů pro ukázkou konfigurace v systému IBM i.

Krok “4” na stránce 28 z “Konfigurace kanálů v systému IBM i” na stránce 26 popisuje konfiguraci, která má být provedena ve správci front IBM i za účelem implementace kanálu popsaného v části “Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5. Příklady v části “Konfigurace kanálů v systému IBM i” na stránce 26 jsou pro připojení IBM MQ for IBM i a IBM MQ for Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte hodnoty z příslušné tabulky namísto hodnot pro Windows.

Poznámka:

1. Slova **tučně** jsou navrhované hodnoty a odrážejí názvy objektů IBM MQ použité v těchto příkladech. Můžete je změnit v instalaci produktu, ale pokud tak učiníte, ujistěte se, že při práci s příklady v této sekci používáte své vlastní hodnoty.
2. Příkaz IBM MQ channel ping (**PNGMQMCHL**) se spouští interaktivně, zatímco spuštění kanálu způsobí odeslání dávkové úlohy. Pokud je příkaz ping kanálu úspěšně dokončen, ale kanál se nespustí, jsou definice sítě a IBM MQ pravděpodobně správné, ale prostředí IBM i pro dávkovou úlohu ne. Například se ujistěte, že je v systémové části seznamu knihoven uveden řetězec QSYS2 , a nikoli pouze váš osobní seznam knihoven.

Další informace a příklady, jak vytvořit objekty uvedené v tabulkách, viz “Konfigurace kanálů v systému IBM i” na stránce 26.

Definice lokálního uzlu

Tabulka 13. Příklady konfigurace pro definici lokálního uzlu

ID	Název parametru	Odkaz	Použitý příklad
A	Název správce front		AS400
B	Název lokální fronty		AS400.LOCALQ

Připojení k IBM MQ on Windows

Windows

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro Windows” na stránce 42, jak je uvedeno.

Tabulka 14. Příklady konfigurace pro připojení k systému IBM MQ on Windows

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	WINNT
D	Název vzdálené fronty		WINNT.REMOTEQ
E	Název fronty na vzdáleném systému	B	WINNT.LOCALQ
F	Jméno přenosové fronty		WINNT
G	Název kanálu odesílatele (SNA)		AS400.WINNT.SNA
H	Název kanálu odesílatele (TCP/IP)		AS400.WINNT.TCP
I	Název kanálu příjemce (SNA)	G	WINNT.AS400.SNA
J	Název kanálu příjemce (TCP/IP)	H	WINNT.AS400.TCP

Připojení k IBM MQ on AIX

AIX

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro AIX” na stránce 12, jak je uvedeno.

Tabulka 15. Příklady konfigurace pro připojení k systému IBM MQ on AIX

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	AIX
D	Název vzdálené fronty		AIX.REMOTEQ
E	Název fronty na vzdáleném systému	B	AIX.LOCALQ
F	Jméno přenosové fronty		AIX
G	Název kanálu odesílatele (SNA)		AS400.AIX.SNA
H	Název kanálu odesílatele (TCP/IP)		AS400.AIX.TCP
I	Název kanálu příjemce (SNA)	G	AIX.AS400.SNA
J	Název kanálu příjemce (TCP)	H	AIX.AS400.TCP

Připojení k IBM MQ on Linux

Linux

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro Linux” na stránce 36, jak je uvedeno.

Tabulka 16. Příklady konfigurace pro připojení k systému IBM MQ on Linux

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	LINUX
D	Název vzdálené fronty		LINUX.REMOTEQ
E	Název fronty na vzdáleném systému	B	LINUX.LOCALQ
F	Jméno přenosové fronty		LINUX
G	Název kanálu odesílatele (SNA)		AS400.LINUX.SNA
H	Název kanálu odesílatele (TCP/IP)		AS400.LINUX.TCP
I	Název kanálu příjemce (SNA)	G	LINUX.AS400.SNA
J	Název kanálu příjemce (TCP/IP)	H	LINUX.AS400.TCP

Připojení k IBM MQ for z/OS



Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro z/OS” na stránce 47, jak je uvedeno.

Tabulka 17. Příklady konfigurace pro připojení k produktu IBM MQ for z/OS

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	MVS
D	Název vzdálené fronty		MVS.REMOTEQ
E	Název fronty na vzdáleném systému	B	MVS.LOCALQ
F	Jméno přenosové fronty		MVS
G	Název kanálu odesílatele (SNA)		AS400.MVS.SNA
H	Název kanálu odesílatele (TCP)		AS400.MVS.TCP
I	Název kanálu příjemce (SNA)	G	MVS.AS400.SNA
J	Název kanálu příjemce (TCP)	H	MVS.AS400.TCP

Připojení k systému VSE/ESA

Hodnoty v této části tabulky se musí shodovat s hodnotami používanými v systému VSE/ESA .

Tabulka 18. Příklady konfigurace pro připojení k systému VSE/ESA

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	VSE
D	Název vzdálené fronty		VSE.REMOTEQ
E	Název fronty na vzdáleném systému	B	VSE.LOCALQ
F	Jméno přenosové fronty		VSE
G	Název kanálu odesílatele		AS400.VSE.SNA

Tabulka 18. Příklady konfigurace pro připojení k systému VSE/ESA (pokračování)

ID	Název parametru	Odkaz	Použitý příklad
I	Název přijímacího kanálu	G	VSE.AS400.SNA

Linux **Příklad: nastavení komunikace mezi platformami IBM MQ na systému Linux**

Tento příklad ukazuje, jak nastavit komunikační odkazy z IBM MQ na Linux na IBM MQ na jiné platformě a vytvořit pracovní kanál na této platformě.

Než začnete

Informace o tomto příkladu a jeho použití naleznete v části “Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5 a “Jak používat příklady komunikace mezi platformami” na stránce 7.

Informace o této úloze

Tento příklad pokrývá nastavení komunikace mezi platformami z IBM MQ na Linux na následující platformy:

-  Windows
-  AIX
-  IBM i
-  z/OS

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

Vytvořte síťové připojení pomocí LU 6.2 nebo TCP.

Poznámka: Pro TCP některé distribuce systému Linux nyní používají rozšířený démon inet (XINETD) místo démona inet (INETD). Následující pokyny uvádějí, jak navázat připojení TCP pomocí démona inet nebo rozšířeného démona inet.

Postup

1. Vytvoření síťového připojení pomocí produktu LU6.2

Poznámka: Informace v této části platí pouze pro produkt IBM MQ for Linux (platformax86). Neplatí pro IBM MQ pro Linux (platformax86-64), IBM MQ pro Linux (platforma zSeries s390x) nebo IBM MQ pro Linux (platforma Power).

Nejnovější informace o konfiguraci SNA přes TCP/IP naleznete v příručce Administration Guide pro vaši verzi produktu Linux v následující dokumentaci: [Communications Server for Data Center Deployment on Linux library](#).

2. Vytvoření připojení TCP pomocí démona inet (INETD)

- a) Upravte soubor `/etc/services`.

Pokud v souboru nemáte následující řádek, přidejte jej tak, jak je zobrazeno:

```
MQSeries 1414/tcp # MQSeries channel listener
```

Poznámka: Chcete-li tento soubor upravit, musíte být přihlášení jako superuživatel nebo uživatel root.

- b) Upravte soubor `/etc/inetd.conf`.

Pokud v tomto souboru nemáte následující řádek, přidejte jej tak, jak je zobrazeno:

```
MQSeries stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta  
[-m queue.manager.name ]
```

c) Vyhleďte ID procesu inetd pomocí příkazu:

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

d) Zadejte následující příkaz:

```
kill -1 inetd processid
```

Máte-li v systému více než jednoho správce front, a proto potřebujete více než jednu službu, musíte přidat řádek pro každého dalšího správce front do adresáře `/etc/services` i `inetd.conf`.

Příklad:

```
MQSeries1 1414/tcp  
MQSeries2 1822/tcp
```

```
MQSeries1 stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta -m QM1  
MQSeries2 stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta -m QM2
```

Tím se vyhnete generování chybových zpráv, pokud existuje omezení počtu nevyřízených požadavků na připojení zařazených do fronty na jednom portu TCP. Informace o počtu nevyřízených požadavků na připojení naleznete v tématu [Použití volby nevyřízených požadavků modulu listener TCP](#).

Proces `inetd` v systému Linux může omezit četnost příchozích připojení na portu TCP. Výchozí hodnota je 40 připojení v 60sekundovém intervalu. Potřebujete-li vyšší rychlost, zadejte nový limit počtu příchozích připojení v 60sekundovém intervalu připojením tečky (.) následované novým limitem parametru `nowait` příslušné služby v souboru `inetd.conf`. Například pro limit 500 připojení v 60sekundovém intervalu použijte:

```
MQSeries stream tcp nowait.500 mqm / MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta -m QM1
```

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

3. Vytvoření připojení TCP pomocí přídatného démona inet (XINETD)

Následující pokyny popisují, jak je démon Extended inet implementován na systému Red Hat Linux. Pokud používáte jinou distribuci produktu Linux, možná budete muset tyto pokyny upravit.

a) Upravte soubor `/etc/services`.

Pokud v souboru nemáte následující řádek, přidejte jej tak, jak je zobrazeno:

```
MQSeries 1414/tcp # MQSeries channel listener
```

Pokud v souboru nemáte následující řádek, přidejte jej tak, jak je zobrazeno:

```
MQSeries 1414/tcp # MQSeries channel listener
```

b) Vytvořte soubor s názvem IBM MQ v konfiguračním adresáři XINETD `/etc/xinetd.d` přidáním následujícího oddílu do souboru:

```
# IBM MQ service for XINETD  
service MQSeries
```

```

{
  disable           = no
  flags             = REUSE
  socket_type      = stream
  wait             = no
  user             = mqm
  server           = MQ_INSTALLATION_PATH/bin/amqcista
  server_args      = -m queue.manager.name
  log_on_failure   += USERID
}

```

c) Restartujte démona extended inet zadáním následujícího příkazu:

```
/etc/rc.d/init.d/xinetd restart
```

Máte-li v systému více než jednoho správce front, a proto potřebujete více než jednu službu, musíte přidat řádek do souboru `/etc/services` pro každého dalšího správce front. Můžete vytvořit soubor v adresáři `/etc/xinetd.d` pro každou službu nebo můžete přidat další oddíly do souboru IBM MQ , který jste vytvořili dříve.

Proces `xinetd` v systému Linux může omezit četnost příchozích připojení na portu TCP. Výchozí hodnota je 50 připojení v intervalu 10 sekund. Potřebujete-li vyšší rychlost, zadejte nový limit rychlosti příchozích připojení zadáním atributu 'cps' v konfiguračním souboru `xinetd`. Například pro limit 500 připojení v 60sekundovém intervalu použijte:

```
cps = 500 60
```

4. Dokončete konfiguraci nyní, když je ustanoveno připojení TCP/IP.

Přejděte na část [“Konfigurace kanálů v systému Linux”](#) na stránce 34.

Linux Konfigurace kanálů v systému Linux

Chcete-li konfigurovat produkt IBM MQ pro ukázkou konfigurace v systému Linux, proveďte základní kroky konfigurace pro správce front a poté nakonfigurujte odesílací a přijímací kanály.

Než začnete

Před zahájením procesu se ujistěte, že jste nejprve vytvořili ID uživatele `mqm` a skupinu `mqm`, a nastavte heslo.

Spusťte libovolný kanál pomocí příkazu:

```
runmqchl -c channel.name
```

Informace o této úloze

Notes:

1. Ukázkové programy jsou nainstalovány v adresáři `MQ_INSTALLATION_PATH/samp`, kde `MQ_INSTALLATION_PATH` představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .
2. Protokoly chyb jsou uloženy v chybách `/var/mqm/qmgrs/ qmgrname /`.
3. Používáte-li k zadání příkazů administrace interpret příkazů **runmqsc** , znak + na konci řádku označuje, že další řádek je pokračováním. Ujistěte se, že mezi posledním parametrem a pokračujícím znakem je mezera.

Postup

1. Nastavení základní konfigurace:

a) Vytvořte správce front a sadu výchozích objektů z příkazového řádku UNIX pomocí příkazu:

```
crtmqm -u dlqname -q linux
```

kde:

linux

Název správce front

-q

Označuje, že se má stát výchozím správcem front

-u dlqname

Určuje název fronty nedoručených zpráv.

b) Spusťte správce front z příkazového řádku UNIX pomocí příkazu:

```
strmqm linux
```

kde *linux* je název zadaný správci front při jeho vytvoření.

2. Nakonfigurujte kanály pro ukázkou konfigurace.

Další informace o parametrech použitých v následujících příkladech viz [“Konfigurační parametry kanálu pro Linux”](#) na stránce 36. V každém případě příklad zobrazuje příkaz MQSC. Buď spusťte příkaz **runmqsc** z příkazového řádku Linux a zadejte postupně každý příkaz, nebo sestavte příkazy do příkazového souboru.

Windows Tyto příklady slouží k připojení systému IBM MQ on Linux s IBM MQ on Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte místo hodnot parametru Windows příslušné hodnoty z tabulek v souboru [“Konfigurační parametry kanálu pro Linux”](#) na stránce 36 .

a) Definujte kanál odesilatele, jak je uvedeno v následujících příkladech:

• Použití SNA

```
def ql (WINNT) +                               F
  usage(xmitq) +
  replace

def qr (WINNT.REMOTEQ) +                       D
  rname(WINNT.LOCALQ) +                       E
  rqmname(WINNT) +                             C
  xmitq(WINNT) +                               F
  replace

def chl (LINUX.WINNT.SNA) chltype(sdr) +      G
  trptype(lu62) +
  conname('WINNTCPIC') +                       14
  xmitq(WINNT) +                               F
  replace
```

• Použití TCP

```
def ql (WINNT) +                               F
  usage(xmitq) +
  replace

def qr (WINNT.REMOTEQ) +                       D
  rname(WINNT.LOCALQ) +                       E
  rqmname(WINNT) +                             C
  xmitq(WINNT) +                               F
  replace

def chl (LINUX.WINNT.TCP) chltype(sdr) +      H
  trptype(tcp) +
  conname(remote_tcpip_hostname) +
  xmitq(WINNT) +                               F
  replace
```

b) Definování přijímacího kanálu, jak je uvedeno v následujících příkladech:

- Použití SNA:

```
def ql (LINUX.LOCALQ) replace B
def chl (WINNT.LINUX.SNA) chltype(rcvr) + I
  trptype(lu62) +
  replace
```

- Použití TCP:

```
def ql (LINUX.LOCALQ) replace B
def chl (WINNT.LINUX.TCP) chltype(rcvr) + J
  trptype(tcp) +
  replace
```

Linux Konfigurační parametry kanálu pro Linux

Parametry potřebné ke konfiguraci kanálů pro ukázkou konfigurace v systému Linux.

Krok “2” na stránce 35 z “Konfigurace kanálů v systému Linux” na stránce 34 popisuje konfiguraci, která má být provedena ve správci front Linux za účelem implementace kanálu popsaného v části “Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5. Příklady v části “Konfigurace kanálů v systému Linux” na stránce 34 jsou pro připojení IBM MQ for IBM i a IBM MQ for Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte hodnoty z příslušné tabulky namísto hodnot pro Windows.

Poznámka: Slova **tučně** jsou navrhované hodnoty a odrážejí názvy objektů IBM MQ použité v těchto příkladech. Můžete je změnit v instalaci produktu, ale pokud tak učiníte, ujistěte se, že při práci s příklady v této sekci používáte své vlastní hodnoty.

Definice lokálního uzlu

Tabulka 19. Příklady konfigurace pro definici lokálního uzlu			
ID	Název parametru	Odkaz	Použitý příklad
A	Název správce front		LINUX
B	Název lokální fronty		LINUX.LOCALQ

Připojení k IBM MQ on Windows

Windows

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro Windows” na stránce 42, jak je uvedeno.

Tabulka 20. Příklady konfigurace pro připojení k systému IBM MQ on Windows			
ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	WINNT
D	Název vzdálené fronty		WINNT.REMOTEQ
E	Název fronty na vzdáleném systému	B	WINNT.LOCALQ
F	Jméno přenosové fronty		WINNT
G	Název kanálu odesílatele (SNA)		LINUX.WINNT.SNA
H	Název kanálu odesílatele (TCP/IP)		LINUX.WINNT.TCP
I	Název kanálu příjemce (SNA)	G	WINNT.LINUX.SNA

Tabulka 20. Příklady konfigurace pro připojení k systému IBM MQ on Windows (pokračování)

ID	Název parametru	Odkaz	Použitý příklad
J	Název kanálu příjemce (TCP)	H	WINNT.LINUX.TCP

Připojení k IBM MQ on AIX

AIX

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “[Konfigurace kanálů v systému AIX](#)” na stránce 10, jak je uvedeno.

Tabulka 21. Příklady konfigurace pro připojení k systému IBM MQ on AIX

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	AIX
D	Název vzdálené fronty		AIX.REMOTEQ
E	Název fronty na vzdáleném systému	B	AIX.LOCALQ
F	Jméno přenosové fronty		AIX
G	Název kanálu odesílatele (SNA)		.LINUX.AIX.SNA
H	Název kanálu odesílatele (TCP/IP)		LINUX.AIX.TCP
I	Název kanálu příjemce (SNA)	G	AIX.LINUX.SNA
J	Název kanálu příjemce (TCP/IP)	H	AIX.LINUX.TCP

Připojení k IBM MQ for IBM i

IBM i

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “[Konfigurační parametry kanálu pro IBM i](#)” na stránce 29, jak je uvedeno.

Tabulka 22. Příklady konfigurace pro připojení k systému IBM MQ on IBM i

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	AS400
D	Název vzdálené fronty		AS400.REMOTEQ
E	Název fronty na vzdáleném systému	B	AS400.LOCALQ
F	Jméno přenosové fronty		AS400
G	Název kanálu odesílatele (SNA)		LINUX.AS400.SNA
H	Název kanálu odesílatele (TCP)		LINUX.AS400.TCP
I	Název kanálu příjemce (SNA)	G	AS400.LINUX.SNA
J	Název kanálu příjemce (TCP)	H	AS400.LINUX.TCP

Připojení k IBM MQ for z/OS

z/OS

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “[Konfigurační parametry kanálu pro z/OS](#)” na stránce 47, jak je uvedeno.

Tabulka 23. Příklady konfigurace pro připojení k produktu IBM MQ for z/OS

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	MVS
D	Název vzdálené fronty		MVS.REMOTEQ
E	Název fronty na vzdáleném systému	B	MVS.LOCALQ
F	Jméno přenosové fronty		MVS
G	Název kanálu odesílatele (SNA)		LINUX.MVS.SNA
H	Název kanálu odesílatele (TCP)		LINUX.MVS.TCP
I	Název kanálu příjemce (SNA)	G	MVS.LINUX.SNA
J	Název kanálu příjemce (TCP)	H	MVS.LINUX.TCP

Připojení k produktu IBM MQ for z/OS pomocí skupin sdílení front



Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry sdíleného kanálu” na stránce 55, jak je uvedeno.

Tabulka 24. Příklady konfigurace pro připojení k produktu IBM MQ for z/OS pomocí skupin sdílení front

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	QSG
D	Název vzdálené fronty		QSG.REMOTEQ
E	Název fronty na vzdáleném systému	B	QSG.SHAREDQ
F	Jméno přenosové fronty		QSG
G	Název kanálu odesílatele (SNA)		LINUX.QSG.SNA
H	Název kanálu odesílatele (TCP)		LINUX.QSG.TCP
I	Název kanálu příjemce (SNA)	G	QSG.LINUX.SNA
J	Název kanálu příjemce (TCP)	H	QSG.LINUX.TCP

Windows **Příklad: nastavení komunikace mezi platformami IBM MQ na systému Windows**

Tento příklad ukazuje, jak nastavit komunikační odkazy z IBM MQ na Windows na IBM MQ na jiné platformě a vytvořit pracovní kanál na této platformě.

Než začnete

Informace o tomto příkladu a jeho použití naleznete v části “Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5 a “Jak používat příklady komunikace mezi platformami” na stránce 7.

Informace o této úloze

Tento příklad pokrývá nastavení komunikace mezi platformami z IBM MQ na Windows na následující platformy:

- AIX

-  IBM i
-  Linux
-  z/OS

Postup

1. Vytvořte síťové připojení pomocí produktu LU6.2.

Informace o konfiguraci AnyNet SNA přes TCP/IP viz [AnyNet SNA přes TCP/IP](#) a [Communications Server pro Windows](#) .

2. Vytvořte síťové připojení pomocí protokolu TCP.

Zásobník TCP dodávaný se systémy Windows nezahrnuje démona *inet* nebo jeho ekvivalent.

Před spuštěním kanálů je nutné modul listener spustit explicitně. Umožňuje automatické spuštění přijímacích kanálů v reakci na požadavek z příchozího odesílajícího kanálu.

Ke spuštění modulu listener produktu IBM MQ TCP použijte následující příkaz:

```
runmqclsr -t tcp
```

3. Vytvořte síťové připojení pomocí rozhraní NetBIOS.

- a) Na každém konci kanálu zadejte lokální název systému NetBIOS , který mají používat procesy kanálu IBM MQ v konfiguračním souboru správce front `qm.ini`.

Například sekce NETBIOS v Windows na odesílajícím konci může vypadat takto:

```
NETBIOS:
LocalName=WNTNETB1
```

a na přijímacím konci, vypadat takto:

```
NETBIOS:
LocalName=WNTNETB2
```

Každý proces IBM MQ musí používat jiný lokální název NetBIOS . Nepoužívejte název systému jako název systému NetBIOS , protože jej systém Windows již používá.

- b) Na každém konci kanálu ověřte číslo adaptéru LAN používané v systému.

Předvolba IBM MQ for Windows pro logický adaptér číslo 0 je NetBIOS spuštěný přes síť Internet Protocol . Chcete-li použít nativní systém NetBIOS , musíte vybrat logický adaptér číslo 1. Viz [Zavedení čísla adaptéru LAN](#).

Uveďte správné číslo adaptéru LAN v sekci NETBIOS registru Windows . Příklad:

```
NETBIOS:
AdapterNum=1
```

- c) Aby inicializace odesílacího kanálu fungovala, zadejte lokální název NetBIOS pomocí proměnné prostředí MQNAME:

```
SET MQNAME=WNTNETB1I
```

Poznámka: Tento název musí být jedinečný.

- d) Na odesílajícím konci definujte kanál s názvem NetBIOS , který se používá na druhém konci kanálu. Příklad:

```
DEFINE CHANNEL (WINNT.OS2.NET) CHLTYPE(SDR) +
```

```
TRPTYPE (NETBIOS) +  
CONNNAME (WNTNETB2) +  
XMITQ (OS2) +  
MCATYPE (THREAD) +  
REPLACE
```

Musíte zadat volbu MCATYPE (THREAD) , protože v systému Windows musí být odesílací kanály spuštěny jako podprocesy.

- e) Na přijímacím konci definujte odpovídající přijímací kanál.

Příklad:

```
DEFINE CHANNEL (WINNT.OS2.NET) CHLTYPE (RCVR) +  
TRPTYPE (NETBIOS) +  
REPLACE
```

- f) Spustíte inicializátor kanálu.

Každý nový kanál je spuštěn spíše jako podproces než jako nový proces:

```
runmqchi
```

- g) Na přijímacím konci spustíte modul listener IBM MQ :

```
runmqclsr -t netbios
```

Volitelně můžete zadat hodnoty pro název správce front, lokální název NetBIOS , počet relací, počet názvů a počet příkazů. Další informace o nastavení připojení NetBIOS naleznete v tématu [Definování připojení NetBIOS na systému Windows](#) .

4. Dokončete konfiguraci nyní, když je ustanoveno síťové připojení. Viz [“Konfigurace kanálů v systému Windows”](#) na stránce 40.

Windows Konfigurace kanálů v systému Windows

Chcete-li konfigurovat produkt IBM MQ pro ukázkou konfigurace v systému Windows, proveďte základní kroky konfigurace pro správce front a poté nakonfigurujte odesílací a přijímací kanály.

Informace o této úloze

Notes:

1. Ukázkový program AMQSBCG můžete použít k zobrazení obsahu a záhlaví všech zpráv ve frontě.
Příklad:

```
AMQSBCG q_name qmgr_name
```

zobrazuje obsah fronty *q_name* definované ve správci front *qmgr_name*.

Případně můžete použít prohlížeč zpráv v Průzkumníku IBM MQ .

2. Můžete spustit libovolný kanál z příkazového řádku pomocí příkazu

```
runmqchl -c channel.name
```

3. Protokoly chyb lze nalézt v adresářích *MQ_INSTALLATION_PATH\qmgs\qmgrname\errors* a *MQ_INSTALLATION_PATH\qmgs\@system\errors*. V obou případech jsou nejnovější zprávy na konci *amqerr01.log*.

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

4. Používáte-li k zadání příkazů administrace interpret příkazů **runmqsc**, znak + na konci řádku označuje, že další řádek je pokračováním. Ujistěte se, že mezi posledním parametrem a pokračujícím znakem je mezera.

Postup

1. Chcete-li nastavit základní konfiguraci pomocí příkazového řádku, postupujte takto:

- a) Vytvořte správce front a sadu výchozích objektů pomocí příkazu:

```
crtmqm -u dlqname -q winnt
```

kde:

winnt

Název správce front

-q

Označuje, že se má stát výchozím správcem front

-u dlqname

Určuje název nedoručitelné fronty zpráv.

- b) Spusťte správce front pomocí příkazu:

```
strmqm winnt
```

kde *winnt* je název zadaný správcí front při jeho vytvoření.

2. Nakonfigurujte kanály pro ukázkou konfigurace.

Další informace o parametrech použitých v následujících příkladech viz [“Konfigurační parametry kanálu pro Windows”](#) na stránce 42. V každém případě příklad zobrazuje příkaz MQSC. Buď spusťte příkaz **runmqsc** z příkazového řádku Linux a zadejte postupně každý příkaz, nebo sestavte příkazy do příkazového souboru. Tyto příklady jsou pro připojení IBM MQ for Windows a IBM MQ for AIX. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte místo hodnot parametru IBM MQ for AIX příslušné hodnoty z tabulek v souboru [“Konfigurační parametry kanálu pro Windows”](#) na stránce 42.

- a) Definujte kanál odesilatele, jak je uvedeno v následujících příkladech:

- Použití SNA

```
def ql (AIX) +                               F
  usage(xmitq) +
  replace

def qr (AIX.REMOTEQ) +                       D
  rname(AIX.LOCALQ) +                       E
  rqmname(AIX) +                             C
  xmitq(AIX) +                               F
  replace

def chl (WINNT.AIX.SNA) chltype(sdr) +       G
  trptype(lu62) +
  conname(AIXCPIC) +                         18
  xmitq(AIX) +                               F
  replace
```

- Použití TCP

```
def ql (AIX) +                               F
  usage(xmitq) +
  replace

def qr (AIX.REMOTEQ) +                       D
  rname(AIX.LOCALQ) +                       E
  rqmname(AIX) +                             C
  xmitq(AIX) +                               F
```

```

replace

def chl (WINNT.AIX.TCP) chltype(sdr) +           H
  trptype(tcp) +
  conname(remote_tcpip_hostname) +
  xmitq(AIX) +                                   F
  replace

```

b) Definujte přijímací kanál, jak je uvedeno v následujících příkladech:

- Použití SNA:

```

def ql (WINNT.LOCALQ) replace                   B

def chl (AIX.WINNT.SNA) chltype(rcvr) +        I
  trptype(lu62) +
  replace

```

- Použití TCP:

```

def ql (WINNT.LOCALQ) replace                   B

def chl (AIX.WINNT.TCP) chltype(rcvr) +        J
  trptype(tcp) +
  replace

```

Jak pokračovat dále

Automatické spuštění

Produkt IBM MQ for Windows umožňuje automatizovat spuštění správce front a jeho inicializátoru kanálu, kanálů, modulů listener a příkazových serverů.

Pomocí modulu snap-in IBM MQ Services definujte služby pro správce front. Po úspěšném dokončení testování nastavení komunikace nastavte příslušné služby v modulu snap-in na hodnotu **automaticky**. Tento soubor může být přečten dodanou službou IBM MQ při spuštění systému.

Další informace viz [Administrace IBM MQ](#).

Spuštění kanálů jako procesů nebo podprocesů

Produkt IBM MQ for Windows poskytuje flexibilitu pro spouštění odesílacích kanálů jako Windows procesy nebo Windows podprocesy. Tato hodnota je určena v parametru MCATYPE v definici kanálu odesílatele.

Většina instalací spouští své odesílací kanály jako podprocesy, protože virtuální a reálná paměť potřebná pro podporu mnoha souběžných připojení kanálů je omezena. Avšak připojení NetBIOS potřebuje samostatný proces pro odeslání agenta kanálu zpráv.

Windows Konfigurační parametry kanálu pro Windows

Parametry potřebné ke konfiguraci kanálů pro ukázkou konfigurace v systému Windows.

Krok "2" na stránce 41 z "Konfigurace kanálů v systému Windows" na stránce 40 popisuje konfiguraci, která má být provedena ve správci front Linux za účelem implementace kanálu popsaného v části "Příklad: Nastavení komunikace mezi platformami pro IBM MQ" na stránce 5. Příklady v části "Konfigurace kanálů v systému Windows" na stránce 40 jsou pro připojení IBM MQ for Windows a IBM MQ for AIX. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte hodnoty z příslušné tabulky namísto hodnot pro Windows.

Poznámka: Slova **tučně** jsou navrhované hodnoty a odrážejí názvy objektů IBM MQ použité v těchto příkladech. Můžete je změnit v instalaci produktu, ale pokud tak učiníte, ujistěte se, že při práci s příklady v této sekci používáte své vlastní hodnoty.

V každém případě se zobrazí příkaz MQSC. Buď spusťte příkaz **runmqsc** z příkazového řádku a zadejte postupně každý příkaz, nebo sestavte příkazy do příkazového souboru.

Příklady jsou uvedeny pro připojení IBM MQ for Windows a IBM MQ for AIX. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte odpovídající sadu hodnot z tabulky namísto hodnot pro produkt Windows.

Definice lokálního uzlu

Tabulka 25. Příklady konfigurace pro definici lokálního uzlu

ID	Název parametru	Odkaz	Použitý příklad
A	Název správce front		WINNT
B	Název lokální fronty		WINNT.LOCALQ

Připojení k IBM MQ on AIX



Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “[Konfigurační parametry kanálu pro AIX](#)” na stránce 12, jak je uvedeno.

Tabulka 26. Příklady konfigurace pro připojení k systému IBM MQ on AIX

	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	AIX
D	Název vzdálené fronty		AIX.REMOTEQ
E	Název fronty na vzdáleném systému	B	AIX.LOCALQ
F	Jméno přenosové fronty		AIX
G	Název kanálu odesílatele (SNA)		WINNT.AIX.SNA
H	Název kanálu odesílatele (TCP)		WINNT.AIX.TCP
I	Název kanálu příjemce (SNA)	G	AIX.WINNT.SNA
J	Název kanálu příjemce (TCP)	H	AIX.WINNT.TCP

Připojení k IBM MQ on IBM i



Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “[Konfigurační parametry kanálu pro IBM i](#)” na stránce 29, jak je uvedeno.

Tabulka 27. Příklady konfigurace pro připojení k systému IBM MQ on IBM i

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	AS400
D	Název vzdálené fronty		AS400.REMOTEQ
E	Název fronty na vzdáleném systému	B	AS400.LOCALQ
F	Jméno přenosové fronty		AS400
G	Název kanálu odesílatele (SNA)		WINNT.AS400.SNA
H	Název kanálu odesílatele (TCP)		WINNT.AS400.TCP
I	Název kanálu příjemce (SNA)	G	AS400.WINNT.SNA

Tabulka 27. Příklady konfigurace pro připojení k systému IBM MQ on IBM i (pokračování)

ID	Název parametru	Odkaz	Použitý příklad
J	Název kanálu příjemce (TCP)	H	AS400.WINNT.TCP

Připojení k IBM MQ for z/OS



Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro z/OS” na stránce 47, jak je uvedeno.

Tabulka 28. Příklady konfigurace pro připojení k produktu IBM MQ for z/OS

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	MVS
D	Název vzdálené fronty		MVS.REMOTEQ
E	Název fronty na vzdáleném systému	B	MVS.LOCALQ
F	Jméno přenosové fronty		MVS
G	Název kanálu odesílatele (SNA)		WINNT.MVS.SNA
H	Název kanálu odesílatele (TCP)		WINNT.MVS.TCP
I	Název kanálu příjemce (SNA)	G	MVS.WINNT.SNA
J	Název kanálu příjemce (TCP)	H	MVS.WINNT.TCP

Připojení k produktu IBM MQ for z/OS pomocí skupin sdílení front



Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry sdíleného kanálu” na stránce 55, jak je uvedeno.

Tabulka 29. Příklady konfigurace pro připojení k produktu IBM MQ for z/OS pomocí skupin sdílení front

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	QSG
D	Název vzdálené fronty		QSG.REMOTEQ
E	Název fronty na vzdáleném systému	B	QSG.SHAREDQ
F	Jméno přenosové fronty		QSG
G	Název kanálu odesílatele (SNA)		WINNT.QSG.SNA
H	Název kanálu odesílatele (TCP)		WINNT.QSG.TCP
I	Název kanálu příjemce (SNA)	G	QSG.WINNT.SNA
J	Název kanálu příjemce (TCP)	H	QSG.WINNT.TCP

Příklad: nastavení komunikace mezi platformami IBM MQ na systému z/OS

Tento příklad ukazuje, jak nastavit komunikační odkazy z IBM MQ na z/OS na IBM MQ na jiné platformě a vytvořit pracovní kanál na této platformě.

Než začnete

Informace o tomto příkladu a jeho použití naleznete v části “Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5 a “Jak používat příklady komunikace mezi platformami” na stránce 7.

Informace o této úloze

Tento příklad pokrývá nastavení komunikace mezi platformami z IBM MQ na z/OS na následující platformy:

-  Windows
-  AIX
-  Linux
-  IBM i
- VSE/ESA

Můžete také připojit jakoukoli z následujících možností:

- z/OS na z/OS
- z/OS do MVS
- MVS na MVS

Postup

1. Vytvořte síťové připojení.

- Vytvoření připojení LU 6.2

Nejnovější informace o konfiguraci SNA přes TCP/IP naleznete v následující online dokumentaci IBM : [Communications Server pro z/OS](#) .

- Vytvoření připojení TCP

Pomocí následujícího příkazu změňte objekt správce front tak, aby používal správné parametry distribuovaného řazení do front. Musíte přidat název adresního prostoru TCP do atributu správce front TCPNAME.

```
ALTER QMGR TCPNAME(TCPIP)
```

Připojení TCP je nyní navázáno. Jste připraveni dokončit konfiguraci.

2. Nakonfigurujte kanály.

Podrobnosti o způsobu konfigurace kanálů naleznete v části “[Konfigurace kanálů v systému IBM MQ for z/OS](#)” na stránce 45 .

Konfigurace kanálů v systému IBM MQ for z/OS

Chcete-li nakonfigurovat IBM MQ pro ukázkou konfigurace na systému z/OS, spusťte a nakonfigurujte kanály a moduly listener.

Postup

1. Spusťte inicializátor kanálu pomocí příkazu:

```
/cpf START CHINIT 1
```

2. Spusťte modul listener LU 6.2 pomocí příkazu:

```
/cpf START LSTR LUNAME( M1 ) TRPTYPE(LU62)
```

LUNAME M1 odkazuje na symbolické jméno, které jste dali své LU (5). Musíte zadat TRPTYPE (LU62), jinak modul listener předpokládá, že chcete protokol TCP.

3. Spusťte modul listener TCP pomocí příkazu:

```
/cpf START LSTR
```

Chcete-li použít jiný port než 1414 (výchozí port IBM MQ), použijte příkaz:

```
/cpf START LSTR PORT( 1555 )
```

Kanály IBM MQ se neinicializují úspěšně, pokud vyjednávání kanálu zjistí, že se pořadové číslo zprávy na obou koncích liší. Možná budete muset tyto kanály resetovat ručně.

4. Nakonfigurujte kanály pro ukázkou konfigurace.

Další informace o parametrech použitých v následujících příkladech viz “Konfigurační parametry kanálu pro z/OS” na stránce 47. Tyto příklady jsou pro připojení IBM MQ for z/OS a IBM MQ for Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte hodnoty z příslušné tabulky v souboru “Konfigurační parametry kanálu pro z/OS” na stránce 47 namísto hodnot pro Windows.

a) Definujte kanál odesilatele, jak ukazuje následující příklad: s

Pro LU 6.2:

```
Local Queue
  Object type : QLOCAL
  Name       : WINNT
  Usage     : X (XmitQ)
  F

Remote Queue
  Object type : QREMOTE
  Name       : WINNT.REMOTEQ
  D
Name on remote system : WINNT.LOCALQ
  E
Remote system name   : WINNT
  C
Transmission queue  : WINNT
  F

Sender Channel
  Channel name : MVS.WINNT.SNA
  G
Transport type  : L (LU6.2)
Transmission queue name : WINNT
  F
Connection name : M3
  13
```

Pro TCP:

```
Local Queue
  Object type : QLOCAL
  Name       : WINNT
  Usage     : X (XmitQ)
  F

Remote Queue
  Object type : QREMOTE
  Name       : WINNT.REMOTEQ
  D
Name on remote system : WINNT.LOCALQ
  E
Remote system name   : WINNT
  C
Transmission queue  : WINNT
  F

Sender Channel
  Channel name : MVS.WINNT.TCP
  H
Transport type  : T (TCP)
Transmission queue name : WINNT
  F
Connection name : winnt.tcpip.hostname
```

b) Definujte přijímací kanál, jak je uvedeno v následujících příkladech:

Pro LU 6.2:

```

Local Queue
  Object type : QLOCAL
                Name : MVS.LOCALQ      B
                Usage : N (Normal)

Receiver Channel
  Channel name : WINNT.MVS.SNA      I

```

Pro TCP:

```

Local Queue
  Object type : QLOCAL
                Name : MVS.LOCALQ      B
                Usage : N (Normal)

Receiver Channel
  Channel name : WINNT.MVS.TCP      J

```

Konfigurační parametry kanálu pro z/OS

Parametry potřebné ke konfiguraci kanálů pro ukázkou konfigurace v systému z/OS.

Krok “4” na stránce 46 z “Konfigurace kanálů v systému IBM MQ for z/OS” na stránce 45 popisuje konfiguraci, která má být provedena ve správci front z/OS za účelem implementace kanálu popsaného v části “Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5. Příklady v části “Konfigurace kanálů v systému IBM MQ for z/OS” na stránce 45 jsou pro připojení IBM MQ for z/OS a IBM MQ for Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte hodnoty z příslušné tabulky namísto hodnot pro Windows.

Poznámka: Slova **tučně** jsou navrhované hodnoty a odrážejí názvy objektů IBM MQ použité v těchto příkladech. Můžete je změnit v instalaci produktu, ale pokud tak učiníte, ujistěte se, že při práci s příklady v této sekci používáte své vlastní hodnoty.

Definice lokálního uzlu

Tabulka 30. Příklady konfigurace pro definici lokálního uzlu

ID	Název parametru	Odkaz	Použitý příklad
A	Název správce front		MVS
B	Název lokální fronty		MVS.LOCALQ

Připojení k IBM MQ on Windows



Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro Windows” na stránce 42, jak je uvedeno.

Tabulka 31. Příklady konfigurace pro připojení k systému IBM MQ on Windows

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	WINNT
D	Název vzdálené fronty		WINNT.REMOTEQ
E	Název fronty na vzdáleném systému	B	WINNT.LOCALQ
F	Jméno přenosové fronty		WINNT
G	Jméno kanálu odesílatele (LU 6.2)		MVS.WINNT.SNA
H	Název kanálu odesílatele (TCP)		MVS.WINNT.TCP

Tabulka 31. Příklady konfigurace pro připojení k systému IBM MQ on Windows (pokračování)

ID	Název parametru	Odkaz	Použitý příklad
I	Jméno kanálu příjemce (LU 6.2)	G	WINNT.MVS.SNA
J	Název kanálu příjemce (TCP/IP)	H	WINNT.MVS.TCP

Připojení k IBM MQ on AIX

AIX

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro AIX” na stránce 12, jak je uvedeno.

Tabulka 32. Příklady konfigurace pro připojení k systému IBM MQ on AIX

ID	Název parametru	Odkaz	Použitý příklad
<p>AIX AIX Připojení k IBM MQ for AIX</p>			
C	Název vzdáleného správce front	A	AIX
D	Název vzdálené fronty		AIX.REMOTEQ
E	Název fronty na vzdáleném systému	B	AIX.LOCALQ
F	Jméno přenosové fronty		AIX
G	Jméno kanálu odesílatele (LU 6.2)		MVS.AIX.SNA
H	Název kanálu odesílatele (TCP/IP)		MVS.AIX.TCP
I	Jméno kanálu příjemce (LU 6.2)	G	AIX.MVS.SNA
J	Název kanálu příjemce (TCP/IP)	H	AIX.MVS.TCP

Připojení k IBM MQ on Linux

Linux

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro Linux” na stránce 36, jak je uvedeno.

Tabulka 33. Příklady konfigurace pro připojení k systému IBM MQ on Linux

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	LINUX
D	Název vzdálené fronty		LINUX.REMOTEQ
E	Název fronty na vzdáleném systému	B	LINUX.LOCALQ
F	Jméno přenosové fronty		LINUX
G	Jméno kanálu odesílatele (LU 6.2)		MVS.LINUX.SNA
H	Název kanálu odesílatele (TCP)		MVS.LINUX.TCP
I	Jméno kanálu příjemce (LU 6.2)	G	LINUX.MVS.SNA
J	Název kanálu příjemce (TCP/IP)	H	LINUX.MVS.TCP

Připojení k IBM MQ on IBM i

IBM i

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro IBM i” na stránce 29, jak je uvedeno.

Tabulka 34. Příklady konfigurace pro připojení k systému IBM MQ on IBM i

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	AS400
D	Název vzdálené fronty		AS400.REMOTEQ
E	Název fronty na vzdáleném systému	B	AS400.LOCALQ
F	Jméno přenosové fronty		AS400
G	Jméno kanálu odesílatele (LU 6.2)		MVS.AS400.SNA
H	Název kanálu odesílatele (TCP/IP)		MVS.AS400.TCP
I	Jméno kanálu příjemce (LU 6.2)	G	AS400.MVS.SNA
J	Název kanálu příjemce (TCP/IP)	H	AS400.MVS.TCP

z/OS **Příklad: Nastavení IBM MQ komunikace mezi platformami na systému z/OS pomocí QSGs**

Tento příklad ukazuje, jak nastavit komunikační odkazy na skupinu sdílení front (QSG) z IBM MQ na Windows a AIX. Můžete se také připojit z z/OS do z/OS.

Než začnete

Nastavení komunikačních odkazů ze skupiny sdílení front na jinou platformu než z/OS je stejné, jak je popsáno v části [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému z/OS”](#) na stránce 44.

Informace o tomto příkladu a jeho použití naleznete v části [“Příklad: Nastavení komunikace mezi platformami pro IBM MQ”](#) na stránce 5 a [“Jak používat příklady komunikace mezi platformami”](#) na stránce 7.

Postup

1. Vytvořte síťové připojení pomocí jedné z následujících voleb.
 - Vytvořte připojení LU 6.2 , jak je popsáno v tématu [“Vytvoření připojení LU 6.2 ke skupině sdílení front”](#) na stránce 49.
 - Vytvořte připojení TCP pomocí distributoru prostředí sysplex, jak je popsáno v tématu [“Vytvoření připojení TCP pomocí distributoru prostředí sysplex”](#) na stránce 53.
2. Definujte některé kanály pro dokončení konfigurace po navázání připojení.
Podrobnosti o tomto procesu viz [“Konfigurace sdílených kanálů v systému IBM MQ for z/OS”](#) na stránce 54 .

z/OS **Vytvoření připojení LU 6.2 ke skupině sdílení front**

Existují dva kroky pro vytvoření připojení LU 6.2 . Definování sebe sama do sítě a definování připojení k partnerovi.

Informace o této úloze

Poznámka: Tento příklad je pro připojení k systému Windows , ale úloha je stejná pro ostatní platformy.

Postup

1. Použijte generické prostředky VTAM, chcete-li mít jeden název připojení pro připojení ke skupině sdílení front.

- a) SYS1.PARMLIB(APPCPMxx) obsahuje parametry spuštění pro APPC. Musíte přidat řádek do tohoto souboru, abyste sdělili APPC, kde umístit sideinfo.

Tento řádek musí být ve tvaru:

```
SIDEINFO
  DATASET (APPC .APPCSI)
```

- b) Přidejte další řádek do SYS1.PARMLIB(APPCPMxx) definuje jméno lokální LU, které chcete použít pro modul listener skupiny IBM MQ LU 6.2 .

Řádek, který přidáte, musí mít tvar

```
LUADD ACBNAME (mvslu1)
      NOSCHED
      TPDATA (csq.appctp)
      GRNAME (mvsg1)
```

Zadejte hodnoty pro ACBNAME (9), TPDATA a GRNAME (10) .

Parametr NOSCHED sděluje APPC, že naše nová logická jednotka nepoužívá plánovač LU 6.2 (ASCH), ale má vlastní. TPDATA odkazuje na datovou sadu transakčního programu, ve které LU 6.2 ukládá informace o transakčních programech. Produkt IBM MQ tento parametr opět nepoužívá, ale je vyžadován syntaxí příkazu LUADD.

- c) Spustíte subsystém APPC pomocí příkazu:

```
START APPC , SUB=MSTR , APPC=xx
```

kde *xx* je přípona člena PARMLIB, do kterého jste přidali LU v kroku 1.

Poznámka: Pokud je APPC již spuštěn, lze jej obnovit příkazem:

```
SET APPC=xx
```

Tento efekt je kumulativní, to znamená, že APPC neztrácí své znalosti o objektech, které jsou pro něj již definovány v tomto členu nebo jiném členu PARMLIB.

- d) Přidejte novou logickou jednotku do vhodné definice hlavního uzlu VTAM. Ty jsou obvykle v SYS1.VTAMLST.

Definice APPL bude vypadat jako zobrazená ukázka.

```

MVSLU APPL ACBNAME=MVSLU1,      9
           APPXC=YES,
           AUTOSES=0,
           DDRAINL=NALLOW,
           DLOGMOD=#INTER,      6
           DMINWML=10,
           DMINWNR=10,
           DRESPL=NALLOW,
           DSESLIM=60,
           LMDENT=19,
           MODETAB=MTCICS,
           PARSESS=YES,
           VERIFY=NONE,
           SECACPT=ALREADYV,
           SRBEXIT=YES
```

- e) Aktivujte hlavní uzel.

Tuto aktivaci můžete provést pomocí příkazu:

```
V, NET, ACT, majornode
```

- f) Pomocí obslužného programu APPC ATBSDFMU přidejte do datové sady informací na straně CPI-C položky definující vaše jméno LU a generické prostředky.

Ukázkový soubor JCL se nachází v *thlqual.SCSQPROC* (CSQ4SIDE) (kde *thlqual* je kvalifikátor vysoké úrovně cílové knihovny pro datové sady IBM MQ ve vaší instalaci.)

Položky, které přidáte, budou vypadat takto:

```
SIADD
  DESTNAME (G1)           11
  MODENAME (#INTER)
  TPNAME (MQSERIES)
  PARTNER_LU (MVSLU1)    9
SIADD
  DESTNAME (G2)           12
  MODENAME (#INTER)
  TPNAME (MQSERIES)
  PARTNER_LU (MVSGR)    10
```

- g) Pomocí následujícího příkazu změňte objekt správce front tak, aby používal správné parametry distribuovaného řazení do front.

Musíte zadat lokální logickou jednotku (9) přiřazenou ke správci front v atributu LUGROUP správce front.

```
ALTER QMGR LUGROUP (MVSLU1)
```

2. Definujte připojení k partnerovi přidáním položky do datové sady informací na straně CPI-C.

- a) Přidejte položku do datové sady informací na straně CPI-C, abyste definovali připojení.

Ukázkový soubor JCL pro tuto definici je v adresáři *thlqual.SCSQPROC* (CSQ4SIDE).

Položka, kterou přidáte, vypadá takto:

```
SIADD
  DESTNAME (M3)           13
  MODENAME (#INTER)      14
  TPNAME (MQSERIES)      15
  PARTNER_LU (WINNTLU)   16
```

Jak pokračovat dále

Připojení je nyní navázáno. Jste připraveni dokončit konfiguraci.

Přejděte na část [“Konfigurace sdílených kanálů v systému IBM MQ for z/OS”](#) na stránce 54.

Konfigurační parametry pro připojení LU 6.2

Následující tabulka uvádí všechny parametry požadované pro nastavení komunikace ze systému z/OS do systému IBM MQ na jiné platformě.

Kroky potřebné k nastavení připojení LU 6.2 jsou popsány v části [“Vytvoření připojení LU 6.2 ke skupině sdílení front”](#) na stránce 49s očíslovanými křížovými odkazy na parametry v příkladu.

Čísla ve sloupci Odkaz označují, že hodnota se musí shodovat s hodnotou v příslušném příkladu jinde v této sekci. Příklady, které následují v této sekci, odkazují na hodnoty ve sloupci ID. Položky ve sloupci Název parametru jsou vysvětleny v části [“Vysvětlení pojmů”](#) na stránce 52.

Definice lokálního uzlu pomocí generických prostředků

Tabulka 35. Příklady konfigurace pro definici lokálního uzlu pomocí generických prostředků

ID	Název parametru	Odkaz	Použitý příklad
1	Předpona příkazu		/cpf
2	ID sítě		ID sítě
3	Název uzlu		MVSPU
6	MODENAME		#INTER
7	název lokálního programu transakce		MQSERIES
8	Cílová adresa LAN		400074511092
9	Název lokální LU		MVSLU1
10	Generický název prostředku		MVSGR
11	Symbolické místo určení		G1
12	Symbolické místo určení pro generický název prostředku		G2

Připojení k IBM MQ on Windows

Windows

Tabulka 36. Příklady konfigurace pro připojení k systému IBM MQ na systému Windows pomocí LU 6.2

ID	Název parametru	Odkaz	Použitý příklad
13	Symbolické místo určení		M3
14	MODENAME	21	#INTER
15	Název vzdáleného transakčního programu	7	MQSERIES
16	Jméno partnerské LU	5	WINNTLU
21	ID vzdáleného uzlu	4	05D 30F65

Připojení k IBM MQ on AIX

AIX

Tabulka 37. Příklady konfigurace pro připojení k systému IBM MQ na systému AIX pomocí LU 6.2

ID	Název parametru	Odkaz	Použitý příklad
13	Symbolický cíl		M4
14	MODENAME	18	#INTER
15	Název vzdáleného transakčního programu	6	MQSERIES
16	Jméno partnerské LU	4	AIXLU

Vysvětlení pojmů

1 Předpona příkazu

Tento termín je jedinečnou předponou příkazu subsystému správce front IBM MQ for z/OS. Systémový programátor z/OS definuje tuto hodnotu v době instalace v systému SYS1.PARMLIB(IEFSSNss) a může vám sdělit hodnotu.

2 ID sítě

Spouštěcí procedura VTAM ve vaší instalaci je částečně upravena členem ATCSTRxx datové sady, na kterou odkazuje DDNAME VTAMLST. ID sítě je hodnota uvedená pro parametr NETID v tomto členu. Pro ID sítě musíte uvést název NETID, který vlastní komunikační subsystém IBM MQ . Hodnotu vám může sdělit administrátor sítě.

3 Název uzlu

VTAM, který je nízkovstupním síťovým uzlem, nemá název řídicího bodu pro použití protokolu APPN (Advanced Peer-to-Peer Networking). Má však název řídicího bodu systémových služeb (SSCPNAME). Pro název uzlu musíte uvést název SSCP, který vlastní komunikační subsystém IBM MQ . Tato hodnota je definována ve stejném členu ATCSTRxx jako ID sítě. Hodnotu vám může sdělit administrátor sítě.

9 Název lokální LU

Logická jednotka (LU) je software, který slouží jako rozhraní nebo překladač mezi transakčním programem a sítí. Spravuje výměnu dat mezi transakčními programy. Lokální název LU je jedinečné VTAM APPLID tohoto subsystému IBM MQ . Tuto hodnotu vám může sdělit administrátor sítě.

11 12 13 Symbolická destinace

Tento termín je název, který jste dali profilu informací na straně CPI-C. Potřebujete položku informací o straně pro každý modul listener LU 6.2 .

6 14 Název modemu

Tento termín je název určený pro sadu parametrů, které řídí konverzaci LU 6.2 . Záznam s tímto názvem a podobnými atributy musí být definován na každém konci relace. Ve VTAM to odpovídá položce tabulky režimu. Tuto položku tabulky vám může přiřadit administrátor sítě.

7 15 Název transakčního programu

Aplikace IBM MQ , které se pokoušejí konverzovat s tímto správcem front, uvádějí symbolický název programu, který má být spuštěn na přijímacím konci. Tato hodnota byla určena v atributu TPNAME v definici kanálu u odesilatele. Pro zjednodušení, kdykoli je to možné, použijte název transakčního programu MQSERIES nebo v případě připojení k produktu VSE/ESA, kde je délka omezena na 4 bajty, použijte MQTP.

Další informace viz [Definování připojení LU6.2 pro z/OS pomocí APPC/MVS](#) .

8 LAN cílová adresa

Tento termín je cílová adresa LAN, kterou partnerské uzly používají ke komunikaci s tímto hostitelem. Používáte-li síťový radič 3745, je to hodnota uvedená v parametru LOCADD pro definici linky, ke které je váš partner fyzicky připojen. Pokud vaše partnerské uzly používají jiná zařízení, jako například zařízení 317X nebo 6611, adresa se nastaví během přizpůsobení těchto zařízení. Tuto hodnotu vám může sdělit administrátor sítě.

10 Generický název prostředku

Generický název prostředku je jedinečný název přiřazený skupině názvů LU používaných inicializátory kanálu ve skupině sdílení front.

16 Jméno partnerské LU

Tento termín je název LU správce front IBM MQ v systému, se kterým nastavujete komunikaci. Tato hodnota je uvedena v položce informací o straně pro vzdáleného partnera.

21 ID vzdáleného uzlu

Pro připojení k systému Windows je toto ID ID lokálního uzlu na systému Windows , se kterým nastavujete komunikaci.

Vytvoření připojení TCP pomocí distributoru prostředí sysplex

Můžete nastavit distributora prostředí sysplex tak, aby pro připojení ke skupině sdílení front používal jeden název připojení.

Postup

1. Definujte distribuovanou adresu DVIPA následujícím způsobem:
 - a) Přidejte příkaz DYNAMICXCF do souboru IPCONFIG. Tento příkaz se používá pro konektivitu mezi obrazy pomocí dynamicky vytvořených propojení XCF TCP/IP.

b) Použijte VIPADYNAMIC blok na každém obrázku v prostředí sysplex.

Na vlastním obrazu kódujte příkaz VIPADEFINE, abyste vytvořili příkaz DVIPA Then a VIPADISTRIBUTE, abyste jej distribuovali na všechny ostatní nebo vybrané obrazy.

Na záložním obrazu kódujte příkaz VIPABACKUP pro adresu DVIPA.

2. Přidejte volbu SHAREPORT pro port, který má být sdílen v seznamu rezervací PORT v datové sadě PROFILE, pokud má být v libovolné oblasti LPAR v prostředí sysplex spuštěn více než jeden inicializátor kanálu.

Další informace viz [Příkaz PORT](#) v příručce *z/OS Communications Server: IP Configuration Reference*.

Po provedení těchto kroků se vytvoří připojení TCP. Jste připraveni dokončit konfiguraci.

Jak pokračovat dále

Přejděte na část [“Konfigurace sdílených kanálů v systému IBM MQ for z/OS”](#) na stránce 54.

Konfigurace sdílených kanálů v systému IBM MQ for z/OS

Nakonfigurujte sdílený kanál spuštěním inicializátoru kanálu a zadáním příslušných příkazů pro vaši konfiguraci.

Informace o této úloze

V daném okamžiku může být spuštěna pouze jedna instance sdíleného kanálu. Pokud se pokusíte spustit druhou instanci kanálu, dojde k selhání (chybová zpráva se liší v závislosti na dalších faktorech). Sdílená fronta synchronizace sleduje stav kanálu.

Důležité: Kanály IBM MQ se neinicializují úspěšně, pokud vyjednávání kanálu zjistí, že se pořadové číslo zprávy na obou koncích liší. Možná budete muset resetovat ručně.

Postup

1. Spusťte inicializátor kanálu pomocí příkazu:

```
/cpf START CHINIT
```

2. Spusťte modul listener skupiny LU6.2 pomocí příkazu:

```
/cpf START LSTR TRPTYPE(LU62) LUNAME( G1 ) INDISP(GROUP)
```

LUNAME G1 odkazuje na symbolické jméno, které jste dali své LU (11).

3. Pokud používáte virtuální adresování IP pomocí distributoru prostředí sysplex a chcete naslouchat na specifické adrese, použijte následující příkaz:

```
/cpf START LSTR TRPTYPE(TCP) PORT(1555) IPADDR( mvsvipa ) INDISP(GROUP)
```

4. Nakonfigurujte kanály pro ukázkou konfigurace.

Další informace o parametrech použitých v následujících příkladech viz [“Konfigurační parametry sdíleného kanálu”](#) na stránce 55. Tyto příklady jsou pro připojení IBM MQ for z/OS a Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte místo hodnot parametru Windows příslušné hodnoty z tabulek v souboru [“Konfigurační parametry sdíleného kanálu”](#) na stránce 55.

- a) Definujte sdílený odesílací kanál, jak je uvedeno v následujících příkladech.

Použití LU 6.2:

```
Local Queue  
Object type : QLOCAL
```

```

Name : WINNT F
Usage : X (XmitQ)
Disposition : SHARED

Remote Queue
Object type : QREMOTE
Name : WINNT.REMOTEQ D
Name on remote system : WINNT.LOCALQ E
Remote system name : WINNT C
Transmission queue : WINNT F
Disposition : GROUP

Sender Channel
Channel name : MVS.WINNT.SNA G
Transport type : L (LU6.2)
Transmission queue name : WINNT F
Connection name : M3 13
Disposition : GROUP

```

Použití TCP

```

Local Queue
Object type : QLOCAL
Name : WINNT F
Usage : X (XmitQ)
Disposition : SHARED

Remote Queue
Object type : QREMOTE
Name : WINNT.REMOTEQ D
Name on remote system : WINNT.LOCALQ E
Remote system name : WINNT C
Transmission queue : WINNT F
Disposition : GROUP

Sender Channel
Channel name : QSG.WINNT.TCP H
Transport type : T (TCP)
Transmission queue name : WINNT F
Connection name : winnt.tcpip.hostname
Disposition : GROUP

```

b) Definujte sdílený přijímací kanál, jak je uvedeno v následujících příkladech.

Použití LU 6.2:

```

Local Queue
Object type : QLOCAL
Name : QSG.SHAREDQ B
Usage : N (Normal)
Disposition : SHARED

Receiver Channel
Channel name : WINNT.QSG.SNA I
Disposition : GROUP

```

Použití TCP:

```

Local Queue
Object type : QLOCAL
Name : QSG.SHAREDQ B
Usage : N (Normal)
Disposition : SHARED

Receiver Channel
Channel name : WINNT.QSG.TCP J
Disposition : GROUP

```

Konfigurační parametry sdíleného kanálu

Parametry potřebné ke konfiguraci sdíleného kanálu pro vzorovou konfiguraci v systému z/OS.

Krok “4” na stránce 54 z “Konfigurace sdílených kanálů v systému IBM MQ for z/OS” na stránce 54 popisuje konfiguraci, která má být provedena ve správci front z/OS za účelem implementace kanálu

popsaného v části “Příklad: Nastavení komunikace mezi platformami pro IBM MQ” na stránce 5. Příklady v části “Konfigurace sdílených kanálů v systému IBM MQ for z/OS” na stránce 54 jsou pro připojení IBM MQ for z/OS a Windows. Chcete-li se připojit k produktu IBM MQ na jiné platformě, použijte hodnoty z příslušné tabulky namísto hodnot pro Windows.

Poznámka: Slova **tučně** jsou navrhované hodnoty a odrážejí názvy objektů IBM MQ použité v těchto příkladech. Můžete je změnit v instalaci produktu, ale pokud tak učiníte, ujistěte se, že při práci s příklady v této sekci používáte své vlastní hodnoty.

Definice lokálního uzlu

Tabulka 38. Příklady konfigurace pro definici lokálního uzlu

ID	Název parametru	Odkaz	Použitý příklad
A	Název správce front		QSG
B	Název lokální fronty		QSG.SHAREDQ

Připojení k IBM MQ on Windows

Windows

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro Windows” na stránce 42, jak je uvedeno.

Tabulka 39. Příklady konfigurace pro připojení k systému IBM MQ on Windows

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front	A	WINNT
D	Název vzdálené fronty		WINNT.REMOTEQ
E	Název fronty na vzdáleném systému	B	WINNT.LOCALQ
F	Jméno přenosové fronty		WINNT
G	Jméno kanálu odesílatele (LU 6.2)		QSG.WINNT.SNA
H	Název kanálu odesílatele (TCP)		QSG.WINNT.TCP
I	Jméno kanálu příjemce (LU 6.2)	G	WINNT.QSG.SNA
J	Název kanálu příjemce (TCP/IP)	H	WINNT.QSG.TCP

Připojení k IBM MQ on AIX

AIX

Hodnoty v této sekci tabulky se musí shodovat s hodnotami používanými v souboru “Konfigurační parametry kanálu pro AIX” na stránce 12, jak je uvedeno.

Tabulka 40. Příklady konfigurace pro připojení k systému IBM MQ on AIX

ID	Název parametru	Odkaz	Použitý příklad
C	Název vzdáleného správce front		AIX
D	Název vzdálené fronty		AIX.REMOTEQ
E	Název fronty na vzdáleném systému	B	AIX.LOCALQ
F	Jméno přenosové fronty		AIX
G	Jméno kanálu odesílatele (LU 6.2)		QSG.AIX.SNA

Tabulka 40. Příklady konfigurace pro připojení k systému IBM MQ on AIX (pokračování)

ID	Název parametru	Odkaz	Použitý příklad
H	Název kanálu odesílatele (TCP/IP)		QSG.AIX.TCP
I	Jméno kanálu příjemce (LU 6.2)	G	AIX.QSG.SNA
J	Název kanálu příjemce (TCP/IP)	H	AIX.QSG.TCP

Příklad: Nastavení IBM MQ mezikomunikace pro řazení do front v rámci skupiny na systému z/OS

Tento příklad ukazuje, jak lze migrovat typickou aplikaci dotazu na mzdy, která aktuálně používá distribuované řazení do front pro přenos malých zpráv mezi správci front, aby používala skupiny sdílení front a sdílené fronty.

Informace o této úloze

Pro ilustraci použití distribuovaných front, front v rámci skupiny se sdílenými frontami a sdílených front jsou popsány tři konfigurace. Přidružené diagramy zobrazují pouze tok dat v jednom směru, tj. ze správce front QMG1 do správce front QMG3.

Postup

1. Nastavení a spuštění konfigurace 1.
Další informace viz téma [“Nastavení a spuštění konfigurace 1”](#) na stránce 57.
2. Nastavte a spusťte konfiguraci 2.
Další informace viz téma [“Nastavení a spuštění konfigurace 2”](#) na stránce 60.
3. Nastavte a spusťte konfiguraci 3.
Další informace viz téma [“Nastavení a spuštění konfigurace 3”](#) na stránce 62.

Jak pokračovat dále

Příklad můžete rozšířit několika způsoby:

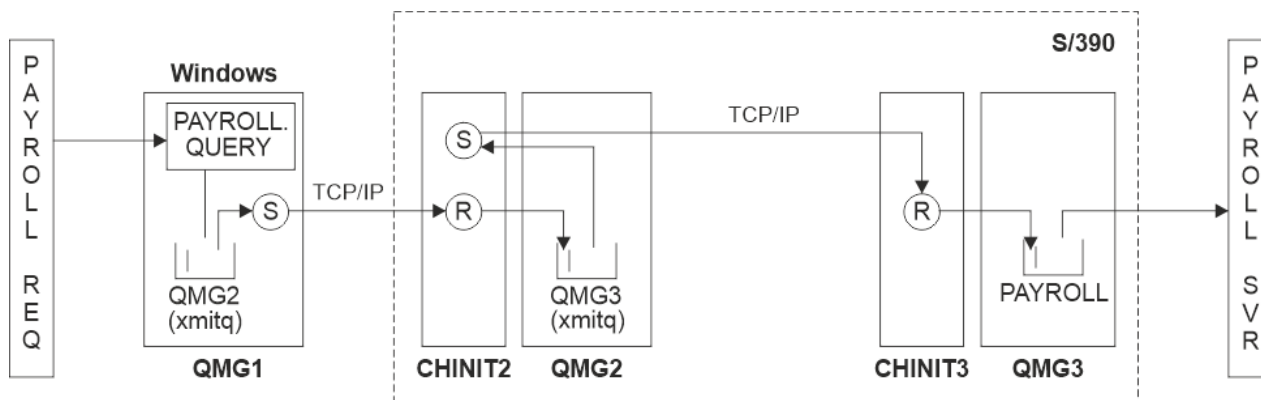
- Použití kanálu spouštění, stejně jako aplikace (PAYROLL a PAYROLL.REPLY queue), spouští se.
- Konfigurace pro komunikaci pomocí produktu LU6.2.
- Konfigurování dalších správců front pro skupinu sdílení front. Poté lze serverovou aplikaci klonovat tak, aby se spouštěla v jiných instancích správce front, a poskytovat tak více serverů pro frontu dotazů PAYROLL.
- Zvýšení počtu instancí dotazu na mzdu, které požadují aplikaci, aby demonstrovaly zpracování požadavků od více klientů.
- Použití zabezpečení (IGQAUT a IGQUSER).

Nastavení a spuštění konfigurace 1

Konfigurace 1 popisuje, jak se distribuované řazení do front aktuálně používá k přenosu zpráv mezi správci front QMG1 a QMG3.

Informace o této úloze

Konfigurace 1 zobrazuje distribuovaný systém front, který se používá k přenosu zpráv přijatých správcem front QMG1 z dotazu na mzdy do správce front QMG2 a nakonec do správce front QMG3, který má být odeslán na mzdový server.



Obrázek 2. Konfigurace 1: z/OS používající řazení do front v rámci skupiny

Tok operací je následující:

1. Dotaz je zadán pomocí aplikace požadavku na mzdu připojené ke správci front QMG1.
2. Aplikace požadavku na mzdu vloží dotaz do vzdálené fronty PAYROLL.QUERY. Jako fronta PAYROLL.QUERY se interpretuje jako přenosová fronta QMG2, dotaz se vloží do přenosové fronty QMG2.
3. Odesílací kanál (S) ve správci front QMG1 doručí dotaz partnerskému přijímacímu kanálu (R) ve správci front QMG2.
4. Přijímací kanál (R) ve správci front QMG2 vloží dotaz do fronty PAYROLL ve správci front QMG3. Jak se fronta PAYROLL na QMG3 interpretuje jako přenosová fronta QMG3, dotaz se vloží do přenosové fronty QMG3.
5. Odesílací kanál (S) ve správci front QMG2 doručí dotaz partnerskému přijímacímu kanálu (R) ve správci front QMG3.
6. Přijímací kanál (R) ve správci front QMG3 vloží dotaz do lokální fronty PAYROLL.
7. Aplikace mzdového serveru připojená ke správci front QMG3 načte dotaz z lokální fronty PAYROLL, zpracuje jej a vygeneruje vhodnou odpověď.

Definice požadované pro konfiguraci 1 jsou následující (všimněte si, že definice neberou v úvahu spuštění a že jsou poskytnuty pouze definice kanálů pro komunikaci pomocí TCP/IP).

Postup

1. Procedura na QMG1:

a) Nastavte definici vzdálené fronty:

```
DEFINE QREMOTE(PAYROLL.QUERY) DESCR('Remote queue for QMG3') REPLACE +
PUT(ENABLED) RNAME(PAYROLL) RQMNAME(QMG3) XMITQ(QMG2)
```

b) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QMG2) DESCR('Transmission queue to QMG2') REPLACE +
PUT(ENABLED) USAGE(XMITQ) GET(ENABLED)
```

c) Nastavení definice odesílacího kanálu pomocí protokolu TCP/IP:

```
DEFINE CHANNEL(QMG1.TO.QMG2) CHLTYPE(SDR) TRPTYPE(TCP) REPLACE +
DESCR('Sender channel to QMG2') XMITQ(QMG2) CONNAME('MVSQMG2(1415)')
```

Poznámka: Proměnnou MVSQMG2(1415) nahraďte názvem připojení a portem správce front.

d) Nastavte definici přijímacího kanálu pomocí protokolu TCP/IP:

```
DEFINE CHANNEL(QMG2.TO.QMG1) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QMG2')
```

e) Nastavte definici fronty pro odpověď:

```
DEFINE QLOCAL(PAYROLL.REPLY) REPLACE PUT(ENABLED) GET(ENABLED) +
DESCR('Reply queue for replies to payroll queries sent to QMG3')
```

2. Procedura na QMG2:

a) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QMG1) DESCR('Transmission queue to QMG1') REPLACE +
PUT(ENABLED) USAGE(XMITQ) GET(ENABLED)

DEFINE QLOCAL(QMG3) DESCR('Transmission queue to QMG3') REPLACE +
PUT(ENABLED) USAGE(XMITQ) GET(ENABLED)
```

b) Nastavte definice odesílacího kanálu pomocí protokolu TCP/IP:

```
DEFINE CHANNEL(QMG2.TO.QMG1) CHLTYPE(SDR) TRPTYPE(TCP) REPLACE +
DESCR('Sender channel to QMG1') XMITQ(QMG1) CONNAME('WINTQMG1(1414)')
```

Poznámka: Proměnnou WINTQMG1(1414) nahraďte názvem připojení a portem správce front.

```
DEFINE CHANNEL(QMG2.TO.QMG3) CHLTYPE(SDR) TRPTYPE(TCP) REPLACE +
DESCR('Sender channel to QMG3') XMITQ(QMG3) CONNAME('MVSQMG3(1416)')
```

Poznámka: Proměnnou MVSQMG3(1416) nahraďte názvem připojení a portem správce front.

c) Nastavte definice přijímacího kanálu pomocí protokolu TCP/IP:

```
DEFINE CHANNEL(QMG1.TO.QMG2) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QMG1')

DEFINE CHANNEL(QMG3.TO.QMG2) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QMG3')
```

3. Procedura na QMG3:

a) Nastavte definici lokální fronty:

```
DEFINE QLOCAL(PAYROLL) DESCR('Payroll query request queue') REPLACE +
PUT(ENABLED) USAGE(NORMAL) GET(ENABLED) SHARE

DEFINE QLOCAL(QMG2) DESCR('Transmission queue to QMG2') REPLACE +
PUT(ENABLED) USAGE(XMITQ) GET(ENABLED)
```

b) Nastavení definice odesílacího kanálu pomocí protokolu TCP/IP:

```
DEFINE CHANNEL(QMG3.TO.QMG2) CHLTYPE(SDR) TRPTYPE(TCP) REPLACE +
DESCR('Sender channel to QMG2') XMITQ(QMG2) CONNAME('MVSQMG2(1415)')
```

Poznámka: Proměnnou MVSQMG2(1415) nahraďte názvem připojení a portem správce front.

c) Nastavte definici přijímacího kanálu pomocí protokolu TCP/IP:

```
DEFINE CHANNEL(QMG2.TO.QMG3) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QMG2')
```

4. Chcete-li spustit konfiguraci 1, postupujte takto:

- a) Spustíte správce front QMG1, QMG2 a QMG3.
- b) Spustíte iniciátory kanálu pro QMG2 a QMG3.

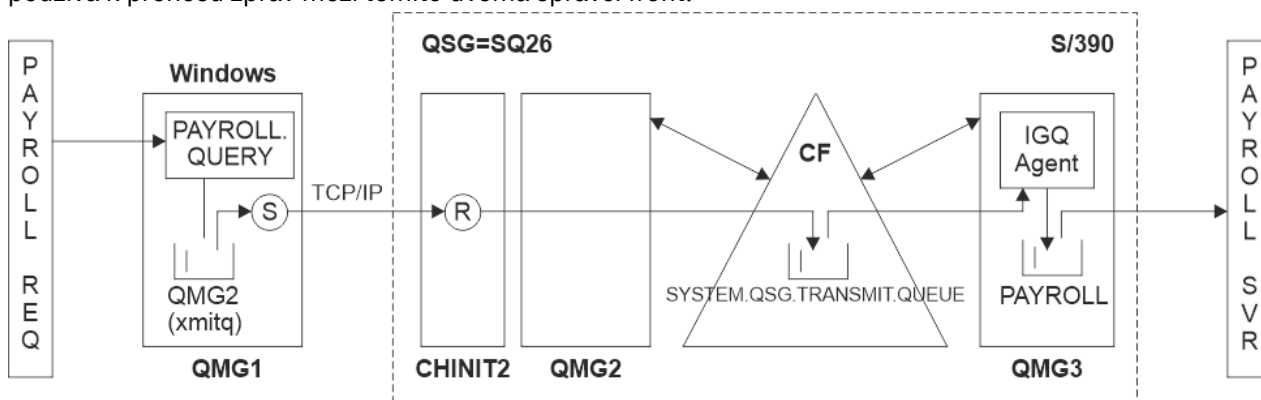
- c) Spustíte moduly listener na QMG1 , aby naslouchaly na portu 1414, QMG2 , aby naslouchaly na portu 1415, a QMG3 , aby naslouchaly na portu 1416.
- d) Spustíte odesílací kanály na systémech QMG1, QMG2a QMG3.
- e) Spustíte mzdový dotaz požadující aplikaci připojenou k QMG1.
- f) Spustíte aplikaci mzdového serveru připojenou k QMG3.
- g) Odešlete požadavek na dotaz na mzdu na QMG3 a počkejte na odpověď na mzdu.

Nastavení a spuštění konfigurace 2

Konfigurace 2 popisuje, jak lze použít skupiny sdílení front a řazení do front v rámci skupiny, aniž by to mělo vliv na back-endovou aplikaci mzdového serveru, k přenosu zpráv mezi správci front QMG1 a QMG3.

Informace o této úloze

Konfigurace 2 zobrazuje distribuovaný systém front, který používá skupiny sdílení front a fronty v rámci skupiny k přenosu zpráv z aplikace požadavku na mzdu na server mezd. Tato konfigurace odstraňuje potřebu definic kanálů mezi správci front QMG2 a QMG3 , protože řazení do front v rámci skupiny se používá k přenosu zpráv mezi těmito dvěma správci front.



Obrázek 3. Konfigurace 2

Tok operací je následující:

1. Dotaz je zadán pomocí aplikace požadavku na mzdu připojené ke správci front QMG1.
2. Aplikace požadavku na mzdu vloží dotaz do vzdálené fronty PAYROLL.QUERY. Jako fronta PAYROLL.QUERY se interpretuje jako přenosová fronta QMG2, dotaz se vloží do přenosové fronty QMG2.
3. Odesílací kanál (S) ve správci front QMG1 doručí dotaz partnerskému přijímacímu kanálu (R) ve správci front QMG2.
4. Přijímací kanál (R) ve správci front QMG2 vloží dotaz do fronty PAYROLL ve správci front QMG3. Jako fronta PAYROLL na QMG3 se interpretuje jako sdílená přenosová fronta SYSTEM.QSG.TRANSMIT.QUEUE, dotaz je vložen do sdílené přenosové fronty SYSTEM.QSG.TRANSMIT.QUEUE.
5. Agent IGQ ve správci front QMG3 načte dotaz ze sdílené přenosové fronty SYSTEM.QSG.TRANSMIT.QUEUE a vloží ji do lokální fronty PAYROLL ve správci front QMG3.
6. Aplikace mzdového serveru připojená ke správci front QMG3 načte dotaz z lokální fronty PAYROLL, zpracuje jej a vygeneruje vhodnou odpověď.

Notes:

- Příklad dotazu na mzdy přenáší pouze malé zprávy. Potřebujete-li přenést trvalé i dočasné zprávy, můžete vytvořit kombinaci konfigurace 1 a konfigurace 2, aby bylo možné přenášet velké zprávy pomocí distribuované trasy řazení do front, zatímco malé zprávy lze přenášet pomocí potenciálně rychlejší trasy řazení do front v rámci skupiny.

- Definice neberou v úvahu spouštění a jsou poskytnuty pouze definice kanálů pro komunikaci pomocí TCP/IP.
- Příklad předpokládá, že jste již nakonfigurovali správce front QMG2 a QMG3 jako členy stejné skupiny sdílení front.

Postup

1. Procedura na QMG1:

a) Nastavte definici vzdálené fronty:

```
DEFINE QREMOTE(PAYROLL.QUERY) DESCR('Remote queue for QMG3') REPLACE +
PUT(ENABLED) RNAME(PAYROLL) RQNAME(QMG3) XMITQ(QMG2)
```

b) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QMG2) DESCR('Transmission queue to QMG2') REPLACE +
PUT(ENABLED) USAGE(XMITQ) GET(ENABLED)
```

c) Nastavení definice odesílacího kanálu pro protokol TCP/IP:

```
DEFINE CHANNEL(QMG1.TO.QMG2) CHLTYPE(SDR) TRPTYPE(TCP) REPLACE +
DESCR('Sender channel to QMG2') XMITQ(QMG2) CONNAME('MVSQMG2(1415)')
```

Poznámka: Proměnnou MVSQMG2(1415) nahraďte názvem připojení a portem správce front.

d) Nastavení definice přijímacího kanálu pro protokol TCP/IP:

```
DEFINE CHANNEL(QMG2.TO.QMG1) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QMG2')
```

e) Nastavte definici fronty pro odpověď:

```
DEFINE QLOCAL(PAYROLL.REPLY) REPLACE PUT(ENABLED) GET(ENABLED) +
DESCR('Reply queue for replies to payroll queries sent to QMG3')
```

2. Procedura na QMG2:

a) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QMG1) DESCR('Transmission queue to QMG1') REPLACE +
PUT(ENABLED) USAGE(XMITQ) GET(ENABLED)

DEFINE QLOCAL(SYSTEM.QSG.TRANSMIT.QUEUE) QSGDISP(SHARED) +
DESCR('IGQ Transmission queue') REPLACE PUT(ENABLED) USAGE(XMITQ) +
GET(ENABLED) INDXTYPE(CORRELID) CFSTRUCT('APPLICATION1') +
DEFSOPT(SHARED) DEFPSIST(NO)
```

Poznámka: Nahraďte APPLICATION1 svým definovaným názvem struktury prostředku CF. Tato fronta, která je sdílenou frontou, musí být definována pouze v jednom ze správců front ve skupině sdílení front.

b) Nastavte definice odesílacího kanálu pro protokol TCP/IP:

```
DEFINE CHANNEL(QMG2.TO.QMG1) CHLTYPE(SDR) TRPTYPE(TCP) REPLACE +
DESCR('Sender channel to QMG1') XMITQ(QMG1) CONNAME('WINTQMG1(1414)')
```

Poznámka: Proměnnou WINTQMG1(1414) nahraďte názvem připojení a portem správce front.

c) Nastavení definice přijímacího kanálu pro protokol TCP/IP:

```
DEFINE CHANNEL(QMG1.TO.QMG2) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QMG1')
```

d) Nastavte definici správce front:

```
ALTER QMGR IGQ(ENABLED)
```

3. Procedura na QMG3:

a) Nastavte definici lokální fronty:

```
DEFINE QLOCAL(PAYROLL) DESCR('Payroll query request queue') REPLACE +
PUT(ENABLED) USAGE(NORMAL) GET(ENABLED) SHARE
```

b) Nastavte definici správce front:

```
ALTER QMGR IGQ(ENABLED)
```

4. Chcete-li spustit konfiguraci 2, postupujte takto:

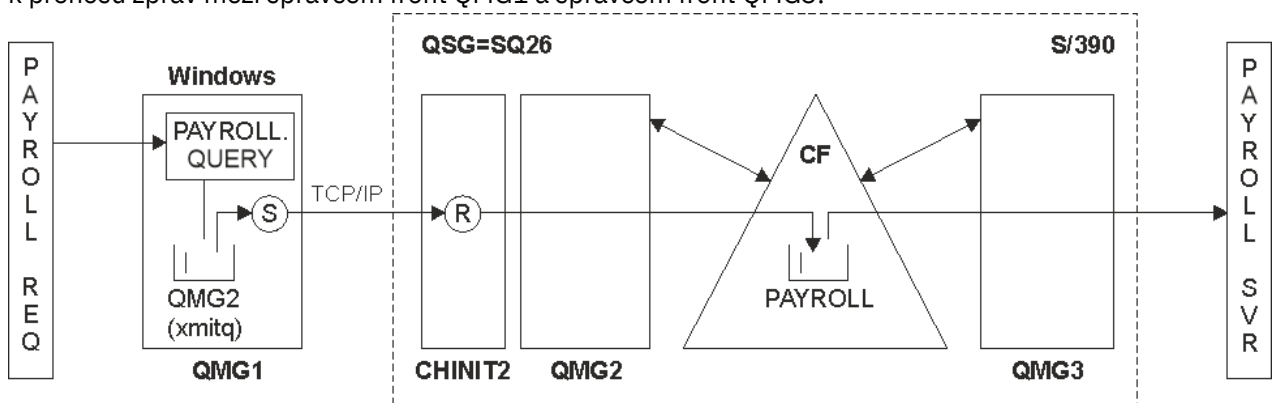
- Spustte správce front QMG1, QMG2a QMG3.
- Spustte inicializátor kanálu pro QMG2.
- Spustte moduly listener na QMG1 , aby naslouchaly na portu 1414, a QMG2 , aby naslouchaly na portu 1415.
- Spustte kanál odesilatele na QMG1 a QMG2.
- Spustte mzdový dotaz požadující aplikaci připojenou k QMG1.
- Spustte aplikaci mzdového serveru připojenou k QMG3.
- Odešlete požadavek na dotaz na mzdu na QMG3 a počkejte na odpověď na mzdu.

z/OS Nastavení a spuštění konfigurace 3

Konfigurace 3 popisuje, jak lze použít skupiny sdílení front a sdílené fronty, bez vlivu na back-endovou aplikaci mzdového serveru, k přenosu zpráv mezi správci front QMG1 a QMG3.

Informace o této úloze

Konfigurace 3 zobrazuje distribuovaný systém front, který používá skupiny sdílení front a sdílené fronty k přenosu zpráv mezi správcem front QMG1 a správcem front QMG3.



Obrázek 4. Konfigurace 3

Tok operací je:

- Dotaz je zadán pomocí aplikace požadavku na mzdu připojené ke správci front QMG1.

2. Aplikace požadavku na mzdu vloží dotaz do vzdálené fronty PAYROLL.QUERY. Jako fronta PAYROLL.QUERY se interpretuje jako přenosová fronta QMG2, dotaz se vloží do přenosové fronty QMG2.
3. Odesílací kanál (S) ve správci front QMG1 doručí dotaz partnerskému přijímacímu kanálu (R) ve správci front QMG2.
4. Přijímací kanál (R) ve správci front QMG2 vloží dotaz do sdílené fronty PAYROLL.
5. Aplikace mzdového serveru připojená ke správci front QMG3 načte dotaz ze sdílené fronty PAYROLL, zpracuje jej a vygeneruje vhodnou odpověď.

Tato konfigurace je jistě nejjednodušší konfigurace. Pro přenos odpovědí (generovaných aplikací mzdového serveru připojenou ke správci front QMG3) ze správce front QMG3 do správce front QMG2a poté do správce front QMG1však budete muset nakonfigurovat distribuované fronty nebo fronty v rámci skupiny.

Informace o konfiguraci použité k přenosu odpovědí zpět do aplikace Požadavek na mzdu naleznete v části [“Příklad: Plánování kanálu zpráv pro z/OS pomocí skupin sdílení front”](#) na stránce 159.

Notes:

- K dispozici jsou pouze definice kanálů pro komunikaci pomocí protokolu TCP/IP.
- Příklad předpokládá, že jste již nakonfigurovali správce front QMG2 a QMG3 jako členy stejné skupiny sdílení front.
- Na QMG3nejsou vyžadovány žádné definice.

Postup

1. Procedura na QMG1:

- a) Nastavte definici vzdálené fronty:

```
DEFINE QREMOTE(PAYROLL.QUERY) DESCR('Remote queue for QMG3') REPLACE +
PUT(ENABLED) RNAME(PAYROLL) RQNAME(QMG3) XMITQ(QMG2)
```

- b) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QMG2) DESCR('Transmission queue to QMG2') REPLACE +
PUT(ENABLED) USAGE(XMITQ) GET(ENABLED)
```

- c) Nastavte definici odesílacího kanálu:

```
DEFINE CHANNEL(QMG1.TO.QMG2) CHLTYPE(SDR) TRPTYPE(TCP) +
REPLACE DESCR('Sender channel to QMG2') XMITQ(QMG2) CONNAME('MVSQMG2(1415)')
```

Poznámka: Proměnnou MVSQMG2(1415) nahraďte názvem připojení a portem správce front.

- d) Nastavte definici přenosového kanálu:

```
DEFINE CHANNEL(QMG2.TO.QMG1) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QMG2')
```

- e) Nastavte definici fronty pro odpověď:

```
DEFINE QLOCAL(PAYROLL.REPLY) REPLACE PUT(ENABLED) GET(ENABLED) +
DESCR('Reply queue for replies to payroll queries sent to QMG3')
```

2. Procedura na QMG2:

- a) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QMG1) DESCR('Transmission queue to QMG1') REPLACE +
PUT(ENABLED) USAGE(XMITQ) GET(ENABLED)
```

b) Nastavte definice odesílacího kanálu pro protokol TCP/IP:

```
DEFINE CHANNEL(QMG2.TO.QMG1) CHLTYPE(SDR) TRPTYPE(TCP) +
REPLACE DESCR('Sender channel to QMG1') XMITQ(QMG1) CONNAME('WINTQMG1(1414)')
```

Poznámka: Proměnnou WINTQMG1(1414) nahraďte názvem připojení a portem správce front.

c) Nastavte definice přijímacího kanálu pro protokol TCP/IP:

```
DEFINE CHANNEL(QMG1.TO.QMG2) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QMG1')
```

d) Nastavte definici lokální fronty:

```
DEFINE QLOCAL(PAYROLL) QSGDISP(SHARED) DESCR('Payroll query request queue') +
REPLACE PUT(ENABLED) USAGE(NORMAL) GET(ENABLED) SHARE +
DEFSOPT(SHARED) DEFPSIST(NO) CFSTRUCT(APPLICATION1)
```

Poznámka: Nahraďte APPLICATION1 svým definovaným názvem struktury prostředku CF. Také tato fronta, která je sdílenou frontou, musí být definována pouze v jednom ze správců front ve skupině sdílení front.

3. Chcete-li spustit konfiguraci 3, postupujte takto:

- a) Spusťte správce front QMG1, QMG2 a QMG3.
- b) Spusťte inicializátor kanálu pro QMG2.
- c) Spusťte moduly listener na QMG1 , aby naslouchaly na portu 1414, a QMG2 , aby naslouchaly na portu 1415.
- d) Spusťte odesílací kanály na QMG1 a QMG2.
- e) Spusťte mzdový dotaz požadující aplikaci připojenou k QMG1.
- f) Spusťte aplikaci mzdového serveru připojenou k QMG3.
- g) Odešlete požadavek na dotaz na mzdu na QMG3 a počkejte na odpověď na mzdu.

Linux

IBM i

AIX

IBM MQ oprávnění systému souborů

použitá pro /var/mqm

Následující informace popisují zabezpečení použité na soubory a adresáře v adresáři /var/mqm/ a proč jsou oprávnění systému souborů nastavena tak, jak jsou. Chcete-li zajistit správnou funkci produktu IBM MQ , neměli byste měnit oprávnění systému souborů, jak je nastaveno v souboru IBM MQ .

crtmqdir příkaz

Pokud váš podnik změnil libovolné oprávnění k souboru /var/mqm , můžete z jakéhokoli důvodu aktualizovat oprávnění nebo přidat adresáře pomocí příkazu **crtmqdir** .

IBM MQ zabezpečení systému souborů na systémech AIX, Linuxu a IBM i

Soubory v datovém adresáři IBM MQ (/var/mqm) se používají k uložení:

- IBM MQ konfigurační data
- Data aplikace (objekty IBM MQ a data obsažená ve zprávách IBM MQ)
- Informace o běhovém řízení
- Monitorovací informace (zprávy a soubory FFST)

Přístup k těmto datům je řízen pomocí oprávnění systému souborů s některými daty, která jsou přístupná všem uživatelům, zatímco ostatní data jsou omezena pouze na členy IBM MQ skupiny administrátorů 'mqm' (nebo QMQM na IBM i).

Přístup je udělován v těchto třech kategoriích:

pouze skupina mqm

Soubory a adresáře v této kategorii jsou přístupné pouze administrátorům IBM MQ (členům skupiny 'mqm') a procesům správce front IBM MQ .

Oprávnění k souborům pro tyto soubory a adresáře jsou:

```
-rwxrwx--- mqm:mqm      (UNIX and Linux)
-rwxrwx--- QMQMADM:QMQM (IBM i)
```

Příkladem souborů a adresářů v této kategorii je:

```
/var/mqm/qmgrs/QMGR/qm.ini
/var/mqm/qmgrs/QMGR/channel/
/var/mqm/qmgrs/QMGR/channel/SYSTEM!DEF!SCRVONN
/var/mqm/qmgrs/QMGR/queues/
/var/mqm/qmgrs/QMGR/queues/SYSTEM!DEFAULT!LOCAL!QUEUES/
/var/mqm/qmgrs/QMGR/errors/
/var/mqm/qmgrs/QMGR/errors/AMQERR01.LOG
/var/mqm/qmgrs/QMGR/ssl/
/var/mqm/qmgrs/QMGR/@qmgr/
/var/mqm/qmgrs/QMGR/@qmpersist/
...
```

Všichni uživatelé přístup pro čtení-členové skupiny mqm přístup pro čtení a zápis

Soubory a adresáře v této kategorii mohou číst všichni uživatelé, ale pouze členové skupiny 'mqm' mohou tyto soubory upravovat a manipulovat s těmito adresáři.

Oprávnění k souborům pro tyto soubory a adresáře jsou:

```
-rwxrwxr-x mqm:mqm      (UNIX and Linux)
-rwxrwxr-x QMQMADM:QMQM (IBM i)
```

Příkladem souborů a adresářů v této kategorii je:

```
/var/mqm/mqs.ini
/var/mqm/exits/
/var/mqm/qmgrs/
/var/mqm/qmgrs/QMGR/
/var/mqm/qmgrs/QMGR/@app/
/var/mqm/qmgrs/QMGR/@ipcc/
```



Upozornění: Oprávnění k provádění byste měli nastavit pouze pro spustitelné soubory a skripty. Například v systému Linux , když se spustí příkaz **crtmqm** , jsou nastavena následující oprávnění k souboru:

```
-rw-rw---- mqm mqm /var/mqm/qmgrs/QMGR/qm.ini
-rw-rw---- mqm mqm /var/mqm/qmgrs/QMGR/channel/SYSTEM!DEF!SCRVONN
-rw-rw---- mqm mqm /var/mqm/qmgrs/QMGR/errors/AMQERR01.LOG
-rw-rw-r-- mqm mqm /var/mqm/mqs.ini
```

IBM MQ 8.0:

```
/var/mqm/sockets/@SYSTEM
/var/mqm/sockets/QMGR/@app/hostname
/var/mqm/sockets/QMGR/@ipcc/hostname
```

Přístup pro čtení a zápis všech uživatelů

Soubory, které mají přístup pro čtení a zápis pro všechny uživatele

IBM MQ nemá žádné *běžné* soubory, které by měly oprávnění k souborům s oprávněním k zápisu pro všechny (777). Existuje však řada *speciálních* souborů, které se jeví jako soubory s oprávněním k zápisu pro všechny.

Tyto speciální soubory neposkytují žádné bezpečnostní riziko. Ačkoli jsou oprávnění zobrazena jako 777, nejedná se o *běžné* soubory a nelze do nich přímo zapisovat.

Jedná se o tyto speciální soubory:

Symbolické odkazy

Symbolické odkazy jsou identifikovány znakem 'l' na začátku jejich oprávnění. Oprávnění na symbolickém odkazu nemají žádný vliv na to, kdo má přístup k cílovému souboru, protože přístup k příkazu je řízen oprávněními na cíli symbolického odkazu.

Na většině systémů AIX and Linux není možné měnit oprávnění pro symbolické odkazy, takže se vždy zobrazují jako `lrwxrwxrwx`.

Soubory soketů

Soubory soketů jsou speciální soubory vytvořené operačním systémem v důsledku procesu vytváření soketu domény UNIX . Tyto soubory lze identifikovat pomocí 's' na začátku oprávnění k souboru, tj. `srwxrwxrwx`.

Oprávnění na souboru neudělují přístup k samotnému souboru, ale definují, kdo se může připojit k soketu domény UNIX .

Produkt IBM MQ používá řadu těchto souborů soketu a oprávnění jsou vždy nastavena podle toho, kdo může se soketem komunikovat.

Následující adresáře obsahují soubory soketů, které mají oprávnění ke čtení/zápisu pro všechny uživatele (`srwxrwxrwx`).

IBM MQ 8.0:

```
/var/mqm/sockets/QMGR/zsocketEC/hostname/Zsocket_*
```

Soubory soketů používané aplikacemi, které se připojují k produktu IBM MQ pomocí izolovaných vazeb.

```
/var/mqm/sockets/QMGR/@ipcc/ssem/hostname/*
```

Adresáře, které mají přístup pro čtení a zápis pro všechny uživatele

Jsou chvíle, kdy aplikace IBM MQ potřebují vytvořit soubory v datovém adresáři IBM MQ . Chcete-li zajistit, aby aplikace byly schopny vytvářet soubory, když jsou požadovány, je jim udělen přístup pro zápis do celého světa, což znamená, že každý uživatel v systému může vytvářet soubory v tomto adresáři.

S výjimkou souborů protokolu chyb, do kterých může zapisovat kterýkoli člen skupiny 'mqm', jsou všechny soubory vytvořené v těchto adresářích vytvořeny s omezenými oprávněními, která povolují pouze přístup pro zápis tvůrce souboru. To umožňuje administrátorovi systému sledovat ID uživatele všech dat zapsaných do souborů v těchto adresářích.

/var/mqm/errors/

Tento adresář obsahuje soubory protokolu chyb systému a soubory FFST. Oprávnění tohoto adresáře je 'drwxrwsrwt', což znamená, že všichni uživatelé v systému mohou vytvářet soubory v tomto adresáři.

SetGroupId bit 's' označuje, že všechny soubory vytvořené v tomto adresáři mají skupinové vlastnictví 'mqm'.

Bit sticky 't' není v tomto adresáři standardně nastaven, ale administrátor systému IBM MQ jej může nastavit explicitně, aby umožnil uživatelům odstranit pouze soubory, které vytvořili.

Poznámka:  Tato funkce není v systému IBM i k dispozici.

AMQERR0*.LOG

Tyto soubory protokolu chyb mohou být zapsány pouze přímo členy group , ale každý uživatel může číst zprávy zapsané do těchto souborů (oprávnění: -rw-rw-r--).

AMQnnnnn.*.FDC

Tyto soubory obsahují informace FFST zapsané při výskytu chyby ve správci front nebo v aplikaci napsané uživatelem. Tyto soubory jsou vytvořeny s oprávněními -rw-r-----.

/var/mqm/trace/

Trasovací soubory se zapisují do tohoto adresáře, když je povoleno trasování IBM MQ . Trasování produktu IBM MQ je zapisováno všemi procesy přidruženými ke správci front, pro kterého je trasování povoleno.

Oprávnění tohoto adresáře jsou 'drwxrwsrwt', což znamená, že všichni uživatelé v systému mohou vytvářet soubory v tomto adresáři.

SetGroupId bit 's' označuje, že všechny soubory vytvořené v tomto adresáři mají skupinové vlastnictví 'mqm' .

Bit sticky 't' není v tomto adresáři standardně nastaven, ale administrátor systému IBM MQ jej může nastavit explicitně, aby umožnil uživatelům odstranit pouze soubory, které vytvořili.

Poznámka:  Tato funkce není v systému IBM i k dispozici.

AMQnnnnn.*.TRC

Tyto soubory obsahují data trasování zapsaná každým procesem, který trasuje, a jsou vytvořeny s oprávněními -rw-r----- .

Oprávnění k tomuto adresáři jsou drwxrwsrwt a oprávnění k souborům soketu vytvořeným v tomto adresáři jsou srwx-----.

IBM MQ 8.0:

```
/var/mqm/sockets/QMGR/zsocketapp/hostname/
```


Tento adresář používají aplikace, které se připojují ke správci front IBM MQ pomocí *izolovaných* vazeb. Během zpracování připojení je soubor soketu vytvořen připojující se aplikaci v tomto adresáři. Soubor soketu je odebrán po vytvoření připojení ke správci front.

Oprávnění k tomuto adresáři jsou drwxrwsrwt a oprávnění k souborům soketu vytvořeným v tomto adresáři jsou srwx-----.

SetGroupId bit 's' v tomto adresáři zajišťuje, že všechny soubory vytvořené v tomto adresáři mají skupinové vlastnictví 'mqm'.

Na všech platformách kromě operačního systému IBM i mají tyto adresáře také sadu bitů sticky 't', která uživateli brání v odstranění všech souborů kromě těch, jejichž jsou vlastníkem. To brání neoprávněnému uživateli v odstranění souborů, které nevlastní.

```
/var/mqm/sockets/QMGR/@ipcc/ssem/hostname/  
/var/mqm/sockets/QMGR/@app/ssem/hostname/
```

 Pro procesy, které se připojují k produktu IBM MQ pomocí *sdílených* vazeb, lze k synchronizaci mezi aplikací a správcem front použít sokety domény UNIX . Když se používají sokety domény UNIX , v těchto adresářích se vytvoří přidružený soubor soketu.

Oprávnění k těmto adresářům jsou drwxrwsrwt a oprávnění k souborům soketu vytvořeným v těchto adresářích jsou srwxrwxrwx.

SetGroupId bit 's' na těchto adresářích zajišťuje, že všechny soubory vytvořené v těchto adresářích mají skupinové vlastnictví 'mqm'.

Na všech platformách s výjimkou operačního systému IBM mají tyto adresáře také nastaven nalepovací bit 't', který uživateli brání v odstranění jakýchkoli souborů kromě těch, jejichž jsou vlastníkem. To brání neoprávněnému uživateli v odstranění souborů, které nevlastní.

HOME

Adresář `/${HOME}/.mqm` je vytvořen při použití neregistrované nebo neinstalované verze produktu IBM MQ, například redistribuovatelného klienta.

Adresář je vytvořen tak, že produkt IBM MQ má spolehlivý způsob přístupu k jeho souborům soketu pomocí cesty, která se vejde do délky `sun_path`. Pokud produkt IBM MQ nemůže zapisovat do adresáře HOME, obdržíte chybovou zprávu.

Použití prostředků System V IPC podle IBM MQ

Produkt IBM MQ používá sdílenou paměť System V a semaforey pro komunikaci mezi procesy. Tyto prostředky jsou seskupeny podle toho, jak jsou používány, přičemž každá skupina má odpovídající vlastnictví a přístupová oprávnění.

Chcete-li ověřit, které prostředky System V IPC v systému patří do IBM MQ, můžete:

- Zkontrolujte vlastnictví.

Vlastnícím uživatelem prostředků IBM MQ System V IPC je vždy uživatel 'mqm' na platformách AIX and Linux. V systému IBM i je vlastnícím uživatelem 'QMQM'.

- IBM MQ 8.0 a novější, použijte obslužný program `amqspdbg`.

Obslužný program `amqspdbg` dodávaný s produktem IBM MQ lze použít k zobrazení sdílené paměti a ID semaforu pro daného správce front.

Musíte zadat příkaz jednou pro skupinu 'system' prostředků System V vytvořenou produktem IBM MQ

```
# amqspbg -z -I
```

a poté čtyřikrát pro každého správce front v systému, abyste získali úplný seznam prostředků System V používaných produktem IBM MQ. Předpokládejme název správce front QMGR1 v následujících příkladech:

```
# amqspdbg -i QMGR1 -I
# amqspdbg -q QMGR1 -I
# amqspdbg -p QMGR1 -I
# amqspdbg -a QMGR1 -I
```

Přístupová oprávnění k prostředkům System V vytvořeným produktem IBM MQ jsou nastavena tak, aby povoleným uživatelům udělila pouze správnou úroveň přístupu. Řada prostředků System V IPC vytvořených produktem IBM MQ je přístupná všem uživatelům v počítači a má oprávnění `-rw-rw-rw-`.

Parametr `-g ApplicationGroup` v příkazu `crtmqm` lze použít k omezení přístupu ke správci front na členství ve specifické skupině operačních systémů. Použití této omezené funkce skupiny dále omezuje oprávnění udělená na prostředcích System V IPC.

Linux

AIX

IBM MQ oprávnění k souboru v /opt/mqm s setuid pro mqm

Následující informace pokrývají situaci, kdy váš tým zabezpečení označil některé spustitelné soubory IBM MQ v adresářovém stromu `$/MQ_INSTALLATION_PATH` v rozporu s lokálními zásadami zabezpečení. Výchozí umístění v adresáři AIX je `/usr/mqm` a pro ostatní operační systémy UNIX je `/opt/mqm`. Pokud jste nainstalovali produkt IBM MQ do jiného než výchozího adresáře, jako např. `/opt/mqm90`, nebo máte-li více instalací, platí i nadále podrobnosti v tomto tématu.

Příčina problému

Váš tým zabezpečení identifikoval v části `$MQ_INSTALLATION_PATH` následující oblasti, které jsou předmětem obav:

1. Soubory v adresáři `/opt/mqm/bin` jsou `setuid` pro vlastníka adresářového stromu, kde jsou umístěny. Příklad:

```
dr-xr-xr-x  mqm mqm  ${MQ_INSTALLATION_PATH}/bin
-r-sr-s---  mqm mqm  ${MQ_INSTALLATION_PATH}/bin/addmqinf
-r-sr-s---  mqm mqm  ${MQ_INSTALLATION_PATH}/bin/amqcrista
-r-sr-s---  mqm mqm  ${MQ_INSTALLATION_PATH}/bin/amqfcxba
...
```

2. Prakticky všechny adresáře a soubory jsou vlastněny "mqm:mqm" s výjimkou následujících, které jsou vlastněny uživatelem root:

```
dr-xr-x---  root mqm  ${MQ_INSTALLATION_PATH}/bin/security
-r-sr-x---  root mqm  ${MQ_INSTALLATION_PATH}/bin/security/amqoamax
-r-sr-x---  root mqm  ${MQ_INSTALLATION_PATH}/bin/security/amqoampx
```

Tento podadresář musí být vlastněn uživatelem root, protože se jedná o spustitelné soubory, které interagují s operačním systémem, když uživatel z klienta IBM MQ zadá heslo, a toto heslo předá správce front IBM MQ operačnímu systému, aby potvrdil, zda je heslo platné nebo neplatné.

3. Uživatel nevládní soubory v `/opt/mqm/lib/iconv` adresáři (tento adresář v systému AIX neexistuje). Příklad:

```
dr-xr-xr-x  mqm mqm  ${MQ_INSTALLATION_PATH}/lib/iconv
-r--r--r--  bin bin  ${MQ_INSTALLATION_PATH}/lib/iconv/002501B5.tbl
-r--r--r--  bin bin  ${MQ_INSTALLATION_PATH}/lib/iconv/002501F4.tbl
-r--r--r--  bin bin  ${MQ_INSTALLATION_PATH}/lib/iconv/00250333.tbl
...
```

4. Adresář údržby opravné sady na systémech Linux založených na RPM. Když jsou nainstalovány opravné sady, jsou existující soubory uloženy v tomto adresáři ve struktuře podobné té, která je uvedena v následujícím příkladu, kromě toho, že v tomto příkladu `V.R` představuje číslo verze a vydání IBM MQ a podadresáře, které se objeví, závisí na instalovaných opravných sadách:

```
drwx-----  root root  ${MQ_INSTALLATION_PATH}/maintenance
drwxr-xr-x   root root  ${MQ_INSTALLATION_PATH}/maintenance/V.R.0.1
drwxr-xr-x   root root  ${MQ_INSTALLATION_PATH}/maintenance/V.R.0.3
drwxr-xr-x   root root  ${MQ_INSTALLATION_PATH}/maintenance/V.R.0.4
...
```

Řešení problému

Jedním z problémů v systémech UNIX s ohledem na programy `setuid` bylo, že zabezpečení systému může být ohroženo manipulací s proměnnými prostředí, jako např. `LD*` (`LD_LIBRARY_PATH`, `LIBPATH` on AIX atd.). To již není problém, protože různé operační systémy UNIX nyní ignorují tyto proměnné prostředí `LD*` při načítání programů `setuid`.

1. Proč jsou některé z programů IBM MQ `mqm-setuid` nebo `mqm-setgid`.

V produktu IBM MQ jsou ID uživatele "mqm" a jakékoli ID, které je součástí skupiny "mqm", administrativní uživatelé produktu IBM MQ .

Prostředky správce front IBM MQ jsou chráněny ověřením vůči tomuto uživateli. Vzhledem k tomu, že procesy správce front používají a upravují tyto prostředky správce front, procesy správce front vyžadují pro přístup k prostředkům oprávnění "mqm". Proto jsou procesy podpory správce front IBM MQ navrženy tak, aby byly spuštěny s efektivním ID uživatele "mqm".

Produkt IBM MQ poskytuje funkci OAM (Object Authority Manager), která umožňuje neadministrativním uživatelům přistupovat k objektům produktu IBM MQ . Oprávnění lze udělit a odvolat v případě potřeby aplikace spuštěné neadministrativním uživatelem.

Díky schopnosti udělit různé úrovně ověření pro uživatele a skutečnosti, že programy **setuid** a **setgid** ignorují proměnné LD*, binární soubory IBM MQ a soubory knihovny nijak neohrožují zabezpečení vašeho systému.

2. Není možné změnit oprávnění tak, aby splňovala zásady zabezpečení vašeho podniku, aniž by byla ohrožena funkčnost produktu IBM MQ .

Nesmíte měnit oprávnění a vlastnictví žádných binárních souborů a knihoven IBM MQ . V důsledku tohoto druhu změn může dojít k potížím s funkčností produktu IBM MQ , což může způsobit, že procesy správce front nebudou mít přístup k některým prostředkům.

Všimněte si, že oprávnění a vlastnictví nepředstavují pro systém žádnou bezpečnostní hrozbu.

Linux pevné jednotky/disky, kde je nainstalován produkt IBM MQ nebo kde jsou umístěna data IBM MQ , nesmí být připojeny s volbou nosuid . Tato konfigurace může bránit funkčnosti produktu IBM MQ .

Další informace viz [“IBM MQ oprávnění systému souborů použítá pro /var/mqm”](#) na stránce 64.

Související pojmy

[Systém souborů](#)

Windows IBM MQ oprávnění systému souborů na Windows

Následující informace popisují zabezpečení použité na soubory a adresáře v systému Windows. Chcete-li zajistit správnou funkci produktu IBM MQ , neměli byste měnit oprávnění systému souborů nastavená pomocí parametru IBM MQ.

Datový adresář

Poznámka: Oprávnění nastavená v kořenovém adresáři tohoto adresáře se dědí směrem dolů v rámci adresářové struktury.

Adresáře pod datovým adresářem (DATADIR) jsou nastaveny s následujícími oprávněními, kromě výjimek uvedených v následujícím textu.

Administrátoři

Úplné řízení

skupina mqm

Úplné řízení

SYSTÉM

Úplné řízení

Každý

Čtení a provádění

Výjimky jsou:

Chyby \DATADIR

Plná kontrola všech

DATADIR \trace

Plná kontrola všech

DATADIR \log

Administrátoři

Úplné řízení

skupina mqm

Úplné řízení

SYSTÉM

Úplné řízení

Každý
Číst

DATADIR \log \ < qmgrname> \active

Administrátoři
Úplné řízení

skupina mqm
Úplné řízení

SYSTÉM
Úplné řízení

Všem nebyl udělen žádný přístup.

Soubory protokolu chyb AMQERR01.LOGatd. nedědí svá nastavení zabezpečení ze svého adresáře, ale místo toho jsou nastavena na hodnotu Všichni: Úplné řízení.

Dřívější vydání produktu

Ve vydáních produktu před verzí IBM MQ 8.0 byly společně umístěny výchozí datové adresáře programu a výchozí datové adresáře.

Ve všech instalacích, které byly původně nainstalovány před produktem IBM MQ 8.0. a který byl nainstalován do výchozích umístění a poté upgradován z těchto umístění, datové a programové adresáře zůstávají umístěny společně (v adresáři C:\Program Files\IBM\WebSphere MQ).

V případě společně umístěných datových a programových adresářů se předchozí informace vztahují pouze na adresáře, které patří do datového adresáře, a nikoli na ty, které jsou součástí programového adresáře.

Omezení pojmenování pro fronty

Délka názvů front je omezena. Některé názvy front jsou vyhrazeny pro fronty definované správcem front.

Omezení délky názvu

Fronty mohou mít názvy až 48 znaků.

Vyhrazené názvy front

Názvy začínající na "SYSTEM." jsou vyhrazeny pro fronty definované správcem front. Pomocí příkazů **ALTER** nebo **DEFINE REPLACE** můžete tyto definice front změnit tak, aby vyhovovaly vaší instalaci. Následující názvy jsou definovány pro IBM MQ:

Název fronty	Popis
SYSTEM.ADMIN.ACTIVITY.QUEUE	Fronta pro sestavy aktivity
SYSTEM.ADMIN.CHANNEL.EVENT	Fronta pro události kanálu
SYSTEM.ADMIN.COMMAND.EVENT	Fronta pro události příkazů
SYSTEM.ADMIN.COMMAND.QUEUE	Fronta, do které jsou odesílány zprávy příkazu PCF
SYSTEM.ADMIN.CONFIG.EVENT	Fronta pro události konfigurace
SYSTEM.ADMIN.PERFM.EVENT	Fronta pro události výkonu
SYSTEM.ADMIN.PUBSUB.EVENT	Fronta událostí související s publikováním/odběry systému
SYSTEM.ADMIN.QMGR.EVENT	Fronta pro události správce front
SYSTEM.ADMIN.TRACE.ROUTE.QUEUE	Fronta pro zprávy s odpovědí trasovací trasy

Tabulka 41. Vyhrazené názvy a popisy front (pokračování)

Název fronty	Popis
SYSTEM.AUTH.DATA.QUEUE	Fronta, která obsahuje seznamy přístupových práv pro správce front. (Není určeno pro z/OS)
SYSTEM.CHANNEL.INITQ	Inicializační fronta pro kanály
SYSTEM.CHANNEL.SYNCQ	Fronta, která uchovává data synchronizace pro kanály
SYSTEM.CHLAUTH.DATA.QUEUE	Datová fronta ověření kanálu IBM MQ
SYSTEM.CICS.INITIATION.QUEUE	Fronta použitá pro spuštění (ne pro z/OS)
SYSTEM.CLUSTER.COMMAND.QUEUE	Fronta používaná ke komunikaci změn úložiště mezi správci front
SYSTEM.CLUSTER.HISTORY.QUEUE	Fronta se používá k uložení historie informací o stavu klastru pro servisní účely.
SYSTEM.CLUSTER.REPOSITORY.QUEUE	Fronta používaná k uchování informací o úložišti
SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE	Fronta použitá k vytvoření jednotlivých přenosových front pro každý odesílací kanál klastru.
SYSTEM.CLUSTER.TRANSMIT.QUEUE	Přenosová fronta pro všechny cíle spravované podporou klastru
SYSTEM.COMMAND.INPUT	Fronta, do které jsou odesílány zprávy příkazů v systému z/OS
SYSTEM.COMMAND.REPLY.MODEL	Definice modelové fronty pro odpovědi na příkazy (pro z/OS)
SYSTEM.DEAD.LETTER.QUEUE	Fronta nedoručených zpráv (ne pro z/OS)
SYSTEM.DEFAULT.ALIAS.QUEUE	Výchozí definice alias fronty
SYSTEM.DEFAULT.INITIATION.QUEUE	Fronta použitá ke spuštění uvedeného procesu (ne pro z/OS)
SYSTEM.DEFAULT.LOCAL.QUEUE	Výchozí definice lokální fronty
SYSTEM.DEFAULT.MODEL.QUEUE	Výchozí definice modelové fronty
SYSTEM.DEFAULT.REMOTE.QUEUE	Výchozí definice vzdálené fronty
SYSTEM.DURABLE.SUBSCRIBER.QUEUE	Lokální fronta používaná k uchování trvalé kopie trvalých odběrů ve správci front.
SYSTEM.HIERARCHY.STATE	Fronta používaná k uchování informací o stavu vztahů mezi správci front v hierarchii publikování/odběru
SYSTEM.JMS.TEMPQ.MODEL	Model pro dočasné fronty JMS
SYSTEM.INTERNAL.REPLY.QUEUE	IBM MQ interní fronta odpovědí (ne pro z/OS)
SYSTEM.INTER.QMGR.CONTROL	Fronta používaná v hierarchii publikování/odběru k přijímání požadavků od vzdáleného správce front za účelem vytvoření proxy odběru
SYSTEM.INTER.QMGR.PUBS	Fronta použitá v hierarchii publikování/odběru pro příjem publikování ze vzdáleného správce front
SYSTEM.INTER.QMGR.FANREQ	Fronta používaná v hierarchii publikování/odběru ke zpracování požadavků na vytvoření proxy odběru ve vzdáleném správci front

Tabulka 41. Vyhrazené názvy a popisy front (pokračování)

Název fronty	Popis
SYSTEM.MQEXPLORER.REPLY.MODEL	Definice modelové fronty pro odpovědi pro IBM MQ Explorer
SYSTEM.MQSC.REPLY.QUEUE	Definice modelové fronty pro odpovědi na příkaz MQSC (nikoli pro z/OS)
SYSTEM.QSG.CHANNEL.SYNCQ	Sdílená lokální fronta používaná pro ukládání zpráv obsahujících synchronizační informace pro sdílené kanály (pouze z/OS)
SYSTEM.QSG.TRANSMIT.QUEUE	Sdílená lokální fronta používaná agentem řazení do front v rámci skupiny při přenosu zpráv mezi správci front ve stejné skupině sdílení front (pouze z/OS)
SYSTEM.RETAINED.PUB.QUEUE	Lokální fronta používaná k uchování kopie každého zachovaného publikování ve správci front.
SYSTEM.SELECTION.EVALUATION.QUEUE	IBM MQ interní fronta vyhodnocení výběru (ne pro z/OS)
SYSTEM.SELECTION.VALIDATION.QUEUE	IBM MQ interní fronta ověření výběru (ne pro z/OS)

Omezení pojmenování pro jiné objekty

Délka názvů objektů je omezena. Některé názvy objektů jsou vyhrazeny pro objekty definované správcem front.

Omezení délky názvu

Procesy, seznamy názvů, klastry, témata, služby a objekty ověřovacích informací mohou mít názvy až 48 znaků.

Kanály mohou mít názvy o délce až 20 znaků.

Paměťové třídy mohou mít názvy až 8 znaků.

Struktury prostředku CF mohou mít názvy o délce až 12 znaků.

Vyhrazené názvy objektů

Názvy začínající na SYSTEM. jsou vyhrazeny pro objekty definované správcem front. Pomocí příkazů **ALTER** nebo **DEFINE REPLACE** můžete tyto definice objektů změnit tak, aby vyhovovaly vaší instalaci. Následující názvy jsou definovány pro IBM MQ:

Tabulka 42. Názvy a popisy vyhrazených objektů

Název objektu	Popis
SYSTEM.ADMIN.SVRCONN	Kanál připojení serveru používaný pro vzdálenou administraci správce front
SYSTEM.AUTO.RECEIVER	Výchozí přijímací kanál pro automatickou definici (pouze systémy AIX, Linux, and Windows)
SYSTEM.AUTO.SVRCONN	Výchozí kanál připojení serveru pro automatickou definici (pouze Multiplatforms)
SYSTEM.BASE.TOPIC	Základní téma pro rozlišení ASPARENT. Pokud konkrétní objekt administrativního tématu nemá žádné nadřazené objekty administrativního tématu, budou z tohoto objektu zděděny všechny atributy ASPARENT.

Tabulka 42. Názvy a popisy vyhrazených objektů (pokračování)

Název objektu	Popis
SYSTEM.DEF.CLNTCONN	Výchozí definice kanálu připojení klienta
SYSTEM.DEF.CLUSRCVR	Výchozí definice přijímacího kanálu klastru
SYSTEM.DEF.CLUSSDR	Výchozí definice odesílacího kanálu klastru
SYSTEM.DEF.RECEIVER	Výchozí definice přijímacího kanálu
SYSTEM.DEF.REQUESTER	Výchozí definice kanálu žadatele
SYSTEM.DEF.SENDER	Výchozí definice odesílacího kanálu
SYSTEM.DEF.SERVER	Výchozí definice kanálu serveru
SYSTEM.DEF.SVRCONN	Výchozí definice kanálu připojení serveru
SYSTEM.DEFAULT.AUTHINFO.CRLLDAP	Výchozí definice objektu ověřovacích informací pro definování objektů ověřovacích informací typu CRLLDAP
SYSTEM.DEFAULT.AUTHINFO.OCSP	Výchozí definice objektu ověřovacích informací pro definování objektů ověřovacích informací typu OCSP
SYSTEM.DEFAULT.LISTENER.LU62	Výchozí modul listener SNA (pouzeWindows)
SYSTEM.DEFAULT.LISTENER.NETsystem BIOS	Výchozí modul listener NetBIOS (pouzeWindows)
SYSTEM.DEFAULT.LISTENER.SPX	Výchozí modul listener SPX (pouzeWindows)
SYSTEM.DEFAULT.LISTENER.TCP	Výchozí modul listener TCP/IP (pouze pro více platform)
SYSTEM.DEFAULT.NAMELIST	Výchozí definice seznamu názvů
SYSTEM.DEFAULT.PROCESS	Výchozí definice procesu
SYSTEM.DEFAULT.SERVICE	Výchozí služba (pouze Multiplatforms)
SYSTEM.DEFAULT.TOPIC	Výchozí definice tématu
SYSTEM.QPUBSUB.QUEUE.NAMELIST	Seznam front pro rozhraní publikování/odběru ve frontě k monitorování
z/OS z/OS SYSTEMST	Výchozí definice paměťové třídy (pouzez/OS)

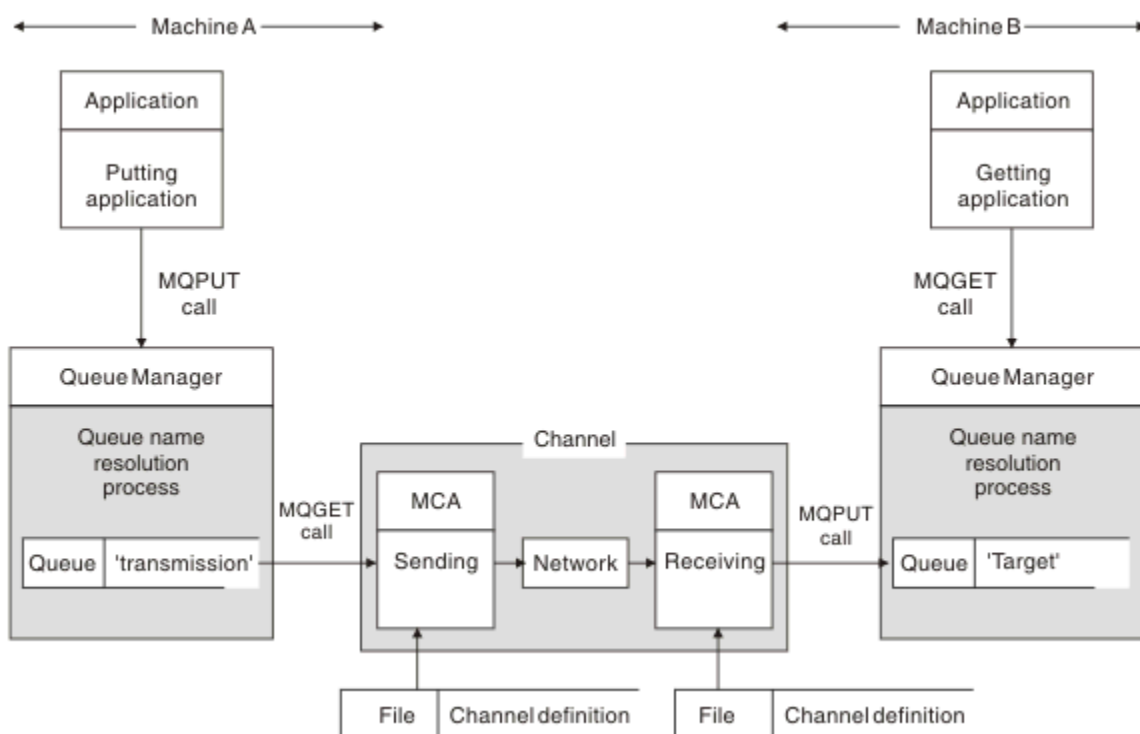
Rozlišení názvu fronty

Ve větších sítích má použití správců front řadu výhod oproti jiným formám komunikace. Tyto výhody jsou odvozeny z funkce rozpoznávání názvů v distribuované správě front, která zajišťuje, že rozpoznávání názvů front je prováděno správci front na odesílajícím i přijímajícím konci kanálu.

Hlavní výhody tohoto přístupu jsou následující:

- Aplikace nemusí provádět rozhodnutí o směrování
- Aplikace nemusí znát strukturu sítě
- Síťové odkazy jsou vytvářeny administrátory systémů.
- Síťová struktura je řízena síťovými plánovači
- Mezi uzly lze k rozdělení provozu použít více kanálů.

Následující obrázek ukazuje příklad rozlišení názvu fronty. Na obrázku jsou uvedeny dva počítače v síti, jeden se spuštěnou aplikací put a druhý se spuštěnou aplikací get. Aplikace spolu komunikují prostřednictvím kanálu IBM MQ řízeného adaptéry MCA.



Obrázek 5. Rozlišení názvu

S odkazem na Obrázek 5 na stránce 75 je základní mechanismus vkládání zpráv do vzdálené fronty, pokud jde o aplikaci, stejný jako při vkládání zpráv do lokální fronty:

- Aplikace, která vložila zprávu, vydá volání MQOPEN a MQPUT za účelem vložení zpráv do cílové fronty.
- Aplikace, která získává zprávy, vydává volání MQOPEN a MQGET za účelem získání zpráv z cílové fronty.

Pokud jsou obě aplikace připojeny ke stejnému správci front, není vyžadována komunikace mezi správcem front a cílová fronta je pro obě aplikace popsána jako *lokální*.

Pokud jsou však aplikace připojeny k různým správcům front, jsou do přenosu zapojeny dva MCA a jejich přidružené síťové připojení, jak ukazuje obrázek. V tomto případě je cílová fronta považována za *vzdálenou frontu* pro vkládající aplikaci.

Posloupnost událostí je následující:

1. Vkládající aplikace vydává volání MQOPEN a MQPUT za účelem vložení zpráv do cílové fronty.
2. Během volání MQOPEN funkce *name resolution* zjistí, že cílová fronta není lokální, a rozhodne, která přenosová fronta je vhodná. Poté jsou všechny zprávy ve voláních MQPUT přidružených k volání MQOPEN umístěny do této přenosové fronty.
3. Odesílající agent MCA získá zprávy z přenosové fronty a předá je přijímajícímu adaptéru MCA ve vzdáleném počítači.
4. Přijímající agent MCA vloží zprávy do cílové fronty nebo front.
5. Při získávání aplikací došlo k volání MQOPEN a MQGET za účelem získání zpráv z cílové fronty.

Poznámka: Pouze krok 1 a krok 5 zahrnují kód aplikace; kroky 2 až 4 jsou prováděny lokálními správci front a programy MCA. Vkládající aplikace neví o umístění cílové fronty, která by mohla být ve stejném procesoru, nebo v jiném procesoru na jiném kontinentu.

Kombinace odesílání MCA, síťového připojení a přijímajícího MCA se nazývá *kanál zpráva* je ze své podstaty jednosměrným zařízením. Za normálních okolností je nutné přesunout zprávy v obou směrech, a dva kanály jsou nastaveny pro tento pohyb, jeden v každém směru.

Související úlohy

Vkládání zpráv do vzdálených front

Co je rozlišení názvu fronty?

Rozlišování názvů front je důležité pro správu distribuovaných front. Odstraňuje potřebu, aby se aplikace zabývaly fyzickým umístěním front, a izoluje aplikace od podrobností sítí.

Administrátor systému může přesouvat fronty z jednoho správce front do jiného a měnit směřování mezi správci front, aniž by o tom musely aplikace něco vědět.

Chcete-li od návrhu aplikace odpojit přesnou cestu, kterou data procházejí, existuje úroveň nesměru mezi názvem použitým aplikací, když odkazuje na cílovou frontu, a pojmenováním kanálu, přes který dochází k toku. Tento nepřímý odkaz je dosažen pomocí mechanismu rozlišení názvu fronty.

V podstatě platí, že když aplikace odkazuje na název fronty, je název mapován mechanismem rozlišení buď na přenosovou frontu, nebo na lokální frontu, která není přenosovou frontou. Pro mapování na přenosovou frontu je v místě určení vyžadováno rozlišení druhého jména a přijatá zpráva je umístěna do cílové fronty podle záměru návrháře aplikací. Aplikace si není vědoma přenosové fronty a kanálu použitého pro přesun zprávy.

Poznámka: Definice fronty a kanálu je zodpovědná za správu systému a může být změněna operátorem nebo obslužným programem pro správu systému bez nutnosti měnit aplikace.

Důležitým požadavkem pro správu systému toků zpráv je, že mezi správci front musí být uvedeny alternativní cesty. Obchodní požadavky mohou například diktovat, že různé *provozní třídy* jsou odesílány přes různé kanály do stejného místa určení. Toto rozhodnutí je rozhodnutím správy systému a mechanismus rozpoznávání názvů front poskytuje flexibilní způsob, jak jej dosáhnout. Příručka Application Programming Guide to podrobně popisuje, ale základní myšlenkou je použít rozlišení názvů front v odesílajícím správci front k mapování názvu fronty dodaného aplikací na příslušnou přenosovou frontu pro daný typ provozu. Podobně na přijímacím konci, rozlišení názvu fronty mapuje název v deskriptoru zprávy na lokální (ne přenosovou) frontu nebo znovu na odpovídající přenosovou frontu.

Nejenže je možné, aby cesta předávání z jednoho správce front na jiného byla rozdělena na různé typy provozu, ale návratová zpráva, která je odeslána do definice fronty pro odpověď v odchozí zprávě, může také používat stejné rozdělení provozu. Rozlišení názvu fronty splňuje tento požadavek a návrhář aplikací nemusí být zapojen do těchto rozhodnutí o rozdělení provozu na oblasti.

Bod, ve kterém se mapování provádí v odesílajících i přijímajících správcích front, je důležitým aspektem způsobu, jakým rozlišování názvů funguje. Toto mapování umožňuje namapovat název fronty zadané aplikací vkládání na lokální frontu nebo přenosovou frontu v odesílajícím správci front a znovu přemapovat na lokální frontu nebo přenosovou frontu v přijímajícím správci front.

Zprávy s odpověďmi od přijímajících aplikací nebo MCA mají rozlišení názvů provedeno stejným způsobem, což umožňuje zpětné směřování přes specifické cesty s definicemi front ve všech správcích front na trase.

Jak se rozlišují atributy cílového objektu pro aliasy, vzdálené fronty a fronty klastru?

Když se překlad názvů provádí jménem volání rozhraní API aplikace, atributy ovlivňující použití objektu jsou interpretovány z kombinace původně pojmenovaného objektu, "cesty" (viz "Rozlišení názvu fronty" na stránce 74) a interpretovaného cílového objektu. V klastru správců front je daným "pojmenovaným objektem" definice klastrovaného objektu (fronty nebo tématu). Jedná se o podmnožinu atributů objektů sdílených mezi správci front a viditelných prostřednictvím, například **DISPLAY QCLUSTER**.

Pokud může být atribut definován na pojmenovaném objektu otevřeném aplikací, má to přednost. Například všechny atributy DEF* *** (výchozí perzistence, priorita a asynchronní odezva vložení) lze konfigurovat v definicích aliasů a vzdálených front. Tyto se projeví, když je alias nebo vzdálená fronta otevřena aplikací, a nikoli jakoukoli vyřešenou cílovou frontou nebo přenosovou frontou.

Atributy navržené tak, aby omezovaly nebo omezovaly interakci aplikace s cílovým objektem, nemohou být obvykle definovány na pojmenovaném objektu (definice vzdálené fronty nebo alias). Například položky **MAXMSGL** a **MAXDEPTH** nelze nastavit v definici nebo aliasu vzdálené fronty a nejsou předávány mezi členy klastru správců front. Tyto atributy jsou proto převzaty z vyřešené fronty (například lokální fronta, příslušná přenosová fronta nebo systém **SYSTEM.CLUSTER.TRANSMIT.QUEUE**). Při příchodu do vzdáleného správce front může být při doručení do cílové fronty uplatněno druhé omezení, což může vést k umístění zprávy do fronty nedoručených zpráv nebo k vynucenému zastavení kanálu.

Všimněte si, že speciálním případem rozpoznání atributu je **PUT** a **GET** povolení. Pro oba tyto atributy má jakákoli instance produktu **DISABLED** v cestě fronty za následek celkový vyřešený atribut **DISABLED**.

Systémové a výchozí objekty

Zobrazí seznam systémových a výchozích objektů vytvořených příkazem **crtmqm**.

Když vytvoříte správce front pomocí řídicího příkazu **crtmqm**, systémové objekty a výchozí objekty se vytvoří automaticky.

- Systémové objekty jsou objekty IBM MQ potřebné pro práci se správcem front nebo kanálem.
- Výchozí objekty definují všechny atributy objektu. Při vytváření objektu, například lokální fronty, jsou všechny atributy, které neurčíte explicitně, zděděny z výchozího objektu.

V následujících tabulkách jsou uvedeny systémové a výchozí objekty vytvořené produktem **crtmqm**.

Poznámka: V tabulkách nejsou obsaženy další dva výchozí objekty: objekt správce front a katalog objektů. Jedná se o objekty v tom smyslu, že jsou protokolovány a obnovitelné.

- [Systémové a výchozí objekty: fronty](#)
- [Systémové a výchozí objekty: témata](#)
- [Systémové a výchozí objekty: kanály serveru](#)
- [Systémové a výchozí objekty: kanály klienta](#)
- [Systémové a výchozí objekty: ověřovací informace](#)
- [Systémové a výchozí objekty: informace o komunikacích](#)
- [Systémové a výchozí objekty: listenery](#)
- [Systémové a výchozí objekty: seznamy názvů](#)
- [Systémové a výchozí objekty: procesy](#)
- [Systémové a výchozí objekty: služby](#)

<i>Tabulka 43. Systémové a výchozí objekty: fronty</i>	
Název objektu	Popis
SYSTEM.ADMIN.ACCOUNTING.QUEUE	Fronta pro data zpráv evidence generovaná při odpojení aplikace od správce front.
SYSTEM.ADMIN.ACTIVITY.QUEUE	Fronta, která zadržuje vrácené zprávy sestavy aktivity.
SYSTEM.ADMIN.CHANNEL.EVENT	Fronta událostí pro kanály.
SYSTEM.ADMIN.COMMAND.EVENT	Fronta událostí pro události příkazů.
SYSTEM.ADMIN.COMMAND.QUEUE	Fronta příkazů administrace. Používá se pro vzdálené příkazy MQSC a PCF.
SYSTEM.ADMIN.CONFIG.EVENT	Fronta událostí pro události konfigurace.
SYSTEM.ADMIN.LOGGER.EVENT	Fronta událostí pro zprávy události modulu protokolování (žurnálový zásobník).
SYSTEM.ADMIN.PERFM.EVENT	Fronta událostí pro události výkonu.

Tabulka 43. Systémové a výchozí objekty: fronty (pokračování)

Název objektu	Popis
SYSTEM.ADMIN.PUBSUB.EVENT	Fronta událostí související s publikováním/odběry systému
SYSTEM.ADMIN.QMGR.EVENT	Fronta událostí pro události správce front.
SYSTEM.ADMIN.STATISTICS.QUEUE	Fronta, která uchovává data monitorování MQI, statistiky fronty a kanálu.
SYSTEM.ADMIN.TRACE.ACTIVITY.QUEUE	Fronta, která zobrazuje aktivitu trasování.
SYSTEM.ADMIN.TRACE.ROUTE.QUEUE	Fronta, která zadržuje vrácené zprávy s odpovědí na trasovací trasu.
SYSTEM.AMQP.COMMAND.QUEUE	IBM MQ Fronta příkazů administrace pro AMQP
SYSTEM.AUTH.DATA.QUEUE	Fronta, která obsahuje seznamy přístupových práv pro správce front. Používá správce oprávnění k objektu (OAM).
SYSTEM.BROKER.ADMIN.STREAM	Administrační proud pro rozhraní publikování/odběru ve frontě
SYSTEM.BROKER.CONTROL.QUEUE	Fronta řízení rozhraní publikování/odběru.
SYSTEM.BROKER.DEFAULT.STREAM	Výchozí proud pro rozhraní publikování/odběru ve frontě
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	Zprostředkovatel pro frontu komunikace zprostředkovatele.
SYSTEM.CHANNEL.INITQ	Inicializační fronta kanálu.
SYSTEM.CHANNEL.SYNCQ	Fronta, která uchovává data synchronizace pro kanály.
SYSTEM.CHLAUTH.DATA.QUEUE	Datová fronta ověření kanálu IBM MQ
SYSTEM.CICS.INITIATION.QUEUE	Výchozí inicializační fronta CICS .
SYSTEM.CLUSTER.COMMAND.QUEUE	Fronta používaná k přenášení zpráv do správce front úložiště.
SYSTEM.CLUSTER.HISTORY.QUEUE	Fronta použitá k uložení historie informací o stavu klastru pro servisní účely.
SYSTEM.CLUSTER.REPOSITORY.QUEUE	Fronta použitá k uložení všech informací o úložišti.
SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE	Fronta použitá k vytvoření jednotlivých přenosových front pro každý odesílací kanál klastru.
SYSTEM.CLUSTER.TRANSMIT.QUEUE	Přenosová fronta pro všechny zprávy pro všechny klastry.
SYSTEM.DEAD.LETTER.QUEUE	Fronta nedoručených zpráv (nedoručených zpráv).
SYSTEM.DEFAULT.ALIAS.QUEUE	Výchozí alias fronta.
SYSTEM.DEFAULT.INITIATION.QUEUE	Výchozí inicializační fronta.
SYSTEM.DEFAULT.LOCAL.QUEUE	Výchozí lokální fronta.
SYSTEM.DEFAULT.MODEL.QUEUE	Výchozí modelová fronta.
SYSTEM.DEFAULT.REMOTE.QUEUE	Výchozí vzdálená fronta.
SYSTEM.DOTNET.XARECOVERY.QUEUE	IBM MQ Fronta zotavení .NET XA

Tabulka 43. Systémové a výchozí objekty: fronty (pokračování)

Název objektu	Popis
SYSTEM.DURABLE.MODEL.QUEUE	Fronta použitá jako model pro spravované trvalé odběry.
SYSTEM.DURABLE.SUBSCRIBER.QUEUE	Fronta používaná k uchování trvalé kopie trvalých odběrů ve správci front.
SYSTEM.HIERARCHY.STATE	IBM MQ stav vztahu distribuované hierarchie publikování/odběru.
SYSTEM.INTER.QMGR.CONTROL	IBM MQ distribuovaná řídicí fronta publikování/odběru.
SYSTEM.INTER.QMGR.FANREQ	IBM MQ Distribuovaná vstupní fronta procesu výstupního větvení serveru proxy pro publikování/odběr.
SYSTEM.INTER.QMGR.PUBS	IBM MQ distribuovaných publikování publikování/odběru.
SYSTEM.INTERNAL.REPLY.QUEUE	
SYSTEM.INTERNAL.REQUEST.QUEUE	
SYSTEM.JMS.TEMPQ.MODEL	Model pro dočasné fronty JMS
SYSTEM.MQEXPLORER.REPLY.MODEL	Fronta pro odpověď IBM MQ Explorer . Jedná se o modelovou frontu, která vytváří dočasnou dynamickou frontu pro odpovědi na IBM MQ Explorer.
SYSTEM.MQSC.REPLY.QUEUE	Fronta pro odpověď příkazu MQSC. Jedná se o modelovou frontu, která vytváří dočasnou dynamickou frontu pro odpovědi na vzdálené příkazy MQSC.
SYSTEM.NDURABLE.MODEL.QUEUE	Fronta používaná jako model pro spravované dočasné odběry.
SYSTEM.PENDING.DATA.QUEUE	Podpora odložených zpráv v souboru JMS.
SYSTEM.PROTECTION.ERROR.QUEUE	IBM MQ Fronta chyb ochrany zpráv.
SYSTEM.PROTECTION.POLICY.QUEUE	IBM MQ Fronta zásad ochrany zpráv.
SYSTEM.REST.REPLY.QUEUE	
SYSTEM.RETAINED.PUB.QUEUE	Fronta používaná k uchování kopie každého zachovaného publikování ve správci front.
SYSTEM.SELECTION.EVALUATION.QUEUE	
SYSTEM.SELECTION.VALIDATION.QUEUE	

Tabulka 44. Systémové a výchozí objekty: témata

Název objektu	Popis
SYSTEM.ADMIN.TOPIC	Téma administrace.

Tabulka 44. Systémové a výchozí objekty: témata (pokračování)

Název objektu	Popis
SYSTEM.BASE.TOPIC	Základní téma pro rozlišení ASPARENT . Pokud konkrétní téma nemá žádné nadřazené objekty administrativních témat nebo tyto nadřazené objekty mají také ASPARENT, všechny zbývající atributy ASPARENT se zdědí od tohoto objektu.
SYSTEM.BROKER.ADMIN.STREAM	Administrativní proud používaný rozhraním pro publikování/odběr ve frontě.
SYSTEM.BROKER.DEFAULT.STREAM	Výchozí proud používaný rozhraním pro publikování/odběr ve frontě.
SYSTEM.BROKER.DEFAULT.SUBPOINT	Výchozí dílčí bod používaný rozhraním pro publikování/odběr ve frontě.
SYSTEM.DEFAULT.TOPIC	Výchozí definice tématu.

Tabulka 45. Systémové a výchozí objekty: kanály serveru

Název objektu	Popis
SYSTEM.AUTO.RECEIVER	Dynamický přijímací kanál.
SYSTEM.AUTO.SVRCONN	Kanál dynamického připojení serveru.
SYSTEM.DEF.AMQP	Výchozí kanál AMQP. Všimněte si, že objekt je definován, ale služba AMQP není podporována.
SYSTEM.DEF.CLUSRCVR	Výchozí přijímací kanál pro klastr, který se používá k zadání výchozích hodnot pro všechny atributy, které nejsou určeny při vytvoření kanálu CLUSRCVR ve správci front v klastru.
SYSTEM.DEF.CLUSSDR	Výchozí kanál odesílatele pro klastr používaný k zadání výchozích hodnot pro všechny atributy, které nejsou určeny při vytvoření kanálu CLUSSDR ve správci front v klastru.
SYSTEM.DEF.RECEIVER	Výchozí přijímací kanál.
SYSTEM.DEF.REQUESTER	Výchozí kanál žadatele.
SYSTEM.DEF.SENDER	Výchozí kanál odesílatele.
SYSTEM.DEF.SERVER	Výchozí kanál serveru.
SYSTEM.DEF.SVRCONN	Výchozí kanál připojení serveru.
SYSTEM.DEFAULT.AUTHINFO.IDPWLDAP	
SYSTEM.DEFAULT.AUTHINFO.IDPWOS	

Tabulka 46. Systémové a výchozí objekty: kanály klienta

Název objektu	Popis
SYSTEM.DEF.CLNTCONN	Výchozí kanál připojení klienta.




Tabulka 47. Systémové a výchozí objekty: ověřovací informace

Název objektu	Popis
SYSTEM.DEFAULT.AUTHINFO.CRLLDAP	Výchozí objekt ověřovacích informací pro definování objektů ověřovacích informací typu CRLLDAP.
SYSTEM.DEFAULT.AUTHINFO.OCSP	Výchozí objekt ověřovacích informací pro definování objektů ověřovacích informací typu OCSP.

Tabulka 48. Systémové a předvolené objekty: informace o komunikacích

Název objektu	Popis
SYSTEM.DEFAULT.COMMINFO.MULTICAST	Výchozí objekt informací o komunikaci pro výběrové vysílání.

Tabulka 49. Systémové a výchozí objekty: listenery

Název objektu	Popis
SYSTEM.DEFAULT.LISTENER.TCP	Výchozí modul listener pro přenos TCP.
 SYSTEM.DEFAULT.LISTENER.LU62	Výchozí modul listener LU62 .
 SYSTEM.DEFAULT.LISTENER.NETBIOS	Výchozí modul listener NETBIOS.
 SYSTEM.DEFAULT.LISTENER.SPX	Výchozí modul listener SPX.

Tabulka 50. Systémové a výchozí objekty: seznamy názvů

Název objektu	Popis
SYSTEM.DEFAULT.NAMELIST	Výchozí definice seznamu názvů.
SYSTEM.QPUBSUB.QUEUE.NAMELIST	Seznam názvů front monitorovaných rozhraním pro publikování/odběr ve frontě.
SYSTEM.QPUBSUB.SUBPOINT.NAMELIST	Seznam objektů témat používaných rozhraním publikování/odběru zařazeným ve frontě k přiřazení objektů témat k bodům odběru.

Tabulka 51. Systémové a výchozí objekty: procesy

Název objektu	Popis
SYSTEM.DEFAULT.PROCESS	Výchozí definice procesu.

Tabulka 52. Systémové a výchozí objekty: služby

Název objektu	Popis
SYSTEM.AMQP.SERVICE	MQ Light Služba rozhraní API. Všimněte si, že objekt je definován, ale služba není podporována.
SYSTEM.DEFAULT.SERVICE	Výchozí služba.

SYSTEM.BASE.TOPIC

Základní téma pro rozlišení ASPARENT . Pokud konkrétní téma nemá žádné nadřazené objekty administrativních témat nebo tyto nadřazené objekty mají také ASPARENT, všechny zbývající atributy ASPARENT se zdědí od tohoto objektu.

Tabulka 53. Výchozí hodnoty SYSTEM.BASE.TOPIC

Parametr	Hodnota
TOPICSTR	"
CAPEXPY	NOLIMIT
CLROUTE	DIRECT
CLUSTER	Výchozí hodnota je prázdný řetězec.
COMMINFO	SYSTEM.DEFAULT.COMMINFO.MULTICAST
DEFPRESP	SYNC
DEFPRTY	0
DEFPSIST	NO
DESCR	'Základní téma pro vyřešení atributů'
DURSUB	YES
MCAST	DISABLED
MDURMDL	SYSTEM.DURABLE.MODEL.QUEUE
MNDURMDL	SYSTEM.NDURABLE.MODEL.QUEUE
NPMSGDLV	ALLAVAIL
PMSGDLV	ALLDUR
PROXYSUB	FIRSTUSE
PUB	ENABLED
PUBSCOPE	ALL
QSGDISP (pouze platforma z/OS)	QMGR
SUB	ENABLED
SUBSCOPE	ALL
USEDLQ	YES
WILDCARD	PASSTHRU

Pokud tento objekt neexistuje, jeho výchozí hodnoty jsou stále používány produktem IBM MQ pro atributy ASPARENT, které nejsou vyřešeny nadřizenými tématy ve stromu témat.

Nastavení atributů PUB nebo SUB produktu SYSTEM.BASE.TOPIC na hodnotu DISABLED zabrání aplikacím v publikování nebo odběru témat ve stromu témat se dvěma výjimkami:

1. Všechny objekty témat ve stromu témat, které mají explicitně nastavenou hodnotu PUB nebo SUB na hodnotu ENABLE. Aplikace mohou publikovat nebo odebírat tato témata a jejich podřazené položky.
2. Publikování a odběr produktu SYSTEM.BROKER.ADMIN.STREAM není zakázáno nastavením atributů PUB nebo SUB SYSTEM.BASE.TOPIC na hodnotu DISABLED.

Viz také Speciální zacházení pro parametr PUB.

Informace o sekci konfiguračních souborů

Následující informace vám pomohou nakonfigurovat informace v sekcích a vypíše obsah souborů `mqs.ini`, `qm.inia` a `mqclient.ini`.

Konfigurace sekcí

Použijte odkazy, které vám pomohou nakonfigurovat systém nebo systémy ve vašem podniku:

- Sekce a atributy souboru `mqs.ini` vám pomohou nakonfigurovat:
 - `AllQueueSprávci`
 - `DefaultQueueSprávce`
 - `ExitProperties` sekce
 - `LogDefaults` sekce
 - Sekce `Zabezpečení` v souboru `qm.ini`
- Sekce a atributy souboru `qm.ini` vám pomohou nakonfigurovat:
 -  `AccessMode` sekce (pouze Windows)
 - Sekce `Služba` - pro instalovatelné služby
 - Sekce `Protokol`
 -   `RestrictedMode` sekce (pouze systémy AIX and Linux)
 - `XAResourceManager` sekce
 - Sekce `TCP, LU62a NETBIOS`
 - `ExitPath` sekce
 - `QMErrorLog` sekce
 - Sekce `SSL`
 - `ExitPropertiesLokální` sekce
- Konfigurace služeb a komponent vám pomůže nakonfigurovat:
 - Sekce `Služba`
 - `ServiceComponent` sekcea obsahuje odkazy na způsob jejich použití pro různé služby na platformách AIX, Linux, and Windows.
- Konfigurace uživatelských procedur rozhraní API vám pomůže nakonfigurovat:
 - `AllActivityAllActivity`
 - `ApplicationTrace` oddíl
- Konfigurace chování trasování aktivity vám pomůže nakonfigurovat:
 - `ApiExitCommon`
 - `ApiExitŠablona` sekce
 - `ApiExitLokální` sekce
- IBM MQ MQI client konfigurační soubor, `mqclient.ini` vám pomůže nakonfigurovat:
 - Sekce `CHANNELS`
 - `ClientExitCesta`
 -  `LU62, NETBIOS` a sekce `SPX` (pouze Windows)
 - `MessageBuffer` sekce

- Sekce *SSL*
- Sekce *TCP*
- **V 9.3.3** Sekce *Trace* (používá se pouze pro IBM MQ .NET a XMS .NET).
- Produkt “Sekce konfiguračního souboru pro distribuované fronty” na stránce 85 vám pomůže nakonfigurovat:
 - Sekce *CHANNELS*
 - Sekce *TCP*
 - *LU62* sekce
 - *NETBIOS*
 - *ExitPath* sekce
- Nastavení atributů zpráv publikování/odběru ve frontě vám pomůže nakonfigurovat:
 - Atribut *PersistentPublishOpakovat*
 - *NonPersistentPublishRetry* atribut
 - atribut *PublishBatchVelikost*
 - Atribut *PublishRetryInterval*
 v sekci *Zprostředkovatel* .



Upozornění: Pokud potřebujete sekci *Zprostředkovatel* , musíte ji vytvořit.

- Použití automatické konfigurace vám pomůže nakonfigurovat:
 - Sekce *AutoConfig*
 - Sekce *AutoCluster*
 - Sekce proměnných

Konfigurační soubory

Viz:

- [mqc.ini](#) soubor
- [qm.ini](#) soubor
- [mqclient.ini](#) soubor

pro seznam možných sekcí v každém konfiguračním souboru.

Linux

AIX

Soubor *mqc.ini*

Příklad konfiguračního souboru IBM MQ pro systémy AIX and Linux zobrazuje ukázkový soubor *mqc.ini* .

Soubor *mqc.ini* může obsahovat následující sekce:

- [AllQueueAllQueue](#)
- [DefaultQueueSprávce](#)
- [ExitProperties](#)
- [LogDefaults](#)

Kromě toho existuje jedna sekce *QueueManager* pro každého správce front.

Soubor *qm.ini*

Příklad konfiguračního souboru správce front pro IBM MQ for AIX or Linux systémy ukazuje ukázkový soubor *qm.ini* .

Soubor *qm.ini* může obsahovat následující sekce:

- [ExitPath](#)
- [Protokol](#)
- [QMErrorLog](#)
- [QueueManager](#)
- [Zabezpečení](#)
- [ServiceComponent](#)

 Chcete-li konfigurovat [InstallableServices](#) , použijte sekce *Služba* a *ServiceComponent* .



- *Připojení* pro [DefaultBindTyp](#)



Upozornění: Musíte vytvořit sekci *Připojení* , pokud ji potřebujete.

- [SSL a TLS](#)
- [TCP, LU62a NETBIOS](#)
- [XAResourceManager](#)

Kromě toho můžete změnit:

-  *AccessMode* (pouzeWindows)
-  *RestrictedMode* (pouze systémyAIX and Linux)

pomocí příkazu [crtmqm](#) .

Soubor `mqclient.ini`

Soubor `mqclient.ini` může obsahovat následující sekce:

- [KANÁLY](#)
- [ClientExitCesta](#)
- [LU62, NETBIOSa SPX](#)
- [MessageBuffer](#)
- [SSL](#)
- [TCP](#)

Kromě toho budete možná potřebovat sekci [PreConnect](#) , abyste nakonfigurovali uživatelskou proceduru předběžného připojení.

Sekce konfiguračního souboru pro distribuované fronty

Popis sekcí konfiguračního souboru správce front `qm.inis` souvisejících s distribuovaným řazením do front.

V tomto tématu jsou uvedeny sekce v konfiguračním souboru správce front, které se týkají distribuovaného řazení do front. Týká se konfiguračního souboru správce front pro produkt IBM MQ for Multiplatforms. Soubor se nazývá `qm.ini` na všech platformách.

Sekce, které se vztahují k distribuovaným frontám, jsou:

- kanály
- TCP
- LU62
- NETBIOS
- EXITPATH

Obrázek 6 na stránce 86 zobrazuje hodnoty, které můžete nastavit pomocí těchto sekcí. Když definujete jednu z těchto sekcí, nemusíte spouštět každou položku na novém řádku. K označení komentáře můžete použít buď středník (;), nebo znak křížku (#).

```

CHANNELS:
MAXCHANNELS=n           ; Maximum number of channels allowed, the
                        ; default value is 100.
MAXACTIVECHANNELS=n    ; Maximum number of channels allowed to be active at
                        ; any time, the default is the value of MaxChannels.
MAXINITIATORS=n        ; Maximum number of initiators allowed, the default
                        ; and maximum value is 3.
MQIBINDTYPE=type       ; Whether the binding for applications is to be
                        ; "fastpath" or "standard".
                        ; The default is "standard".
PIPELINELENGTH=n      ; The maximum number of concurrent threads a channel will use.
                        ; The default is 1. Any value greater than 1 is treated as 2.
ADOPTNEWMCA=chlname   ; Stops previous process if channel fails to start.
                        ; The default is "NO".
ADOPTNEWMCATIMEOUT=n  ; Specifies the amount of time that the new
                        ; process should wait for the old process to end.
                        ; The default is 60.
ADOPTNEWMCACHECHECK= ; Specifies the type checking required.
typecheck              ; The default is "NAME", "ADDRESS", and "QM".
CHLAUTHEARLYADOPT=Y/N ; The order in which connection authentication and channel
authentication rules are ; processed. If not present in the qm.ini file the default is "N".
From MQ9.0.4 all
PASSWORDPROTECTION=   ; queue managers are created with a default of "Y"
than using TLS.       ; From MQ8.0, set protected passwords in the MQCSP structure, rather
options              ; The options are "compatible", "always", "optional" and "warn"
                    ; The default is "compatible".
IGNORESEQNUMBERMISMATCH ; How the queue manager handles a sequence number mismatch during
channel startup.     ;
                    =Y/N ; The options are "Y" and "N" with the default being "N".
CHLAUTHIGNOREUSERCASE ; Enables a queue manager to make username matching within CHLAUTH
rules case-insensitive.
                    =Y/N ; The options are "Y" and "N" with the default being "N".
CHLAUTHISSUEWARN=Y   ; If you want message AMQ9787 to be generated when you set theWARN=YES
attribute
TCP:
PORT=n               ; TCP entries
KEEPALIVE=Yes       ; Port number, the default is 1414
                    ; Switch TCP/IP KeepAlive on
LU62:
LIBRARY2=DLLName2   ; Used if code is in two libraries
EXITPATH:1          ; Location of user exits
EXITPATHS=          ; String of directory paths.

```

Obrázek 6. Sekce qm.ini pro distribuované řazení do front


Notes:

1. EXITPATH se vztahuje pouze na následující platformy:

-  AIX
-  Windows

Související úlohy

[Konfigurace](#)

 [Konfigurace produktu z/OS](#)

[Změna informací o konfiguraci produktu IBM MQ na platformě Multiplatforms](#)

Atributy kanálu

Tato sekce popisuje atributy kanálu, které jsou uloženy v definicích kanálu.

Atributy kanálu můžete zvolit tak, aby byly optimální pro konkrétní sadu okolností pro každý kanál. Avšak, když je kanál spuštěn, skutečné hodnoty se mohly změnit během vyjednávání spuštění. Viz [Příprava kanálů](#).


Mnoho atributů má výchozí hodnoty a tyto hodnoty můžete použít pro většinu kanálů. Avšak za těch okolností, kdy výchozí hodnoty nejsou optimální, viz tato část, kde naleznete pokyny pro výběr správných hodnot.

Poznámka: V produktu IBM MQ for IBM ilze většinu atributů zadat jako *SYSDFTCHL, což znamená, že hodnota je převzata z výchozího kanálu systému ve vašem systému.

Typy kanálů pro atributy kanálu IBM MQ jsou uvedeny v následující tabulce v pořadí parametrů příkazu MQSC.

Poznámka: V případě kanálů klastru (sloupce CLUSSDR a CLUSRCVR v tabulce) platí, že pokud lze atribut nastavit u obou kanálů, nastavte ho na obou a ujistěte se, že je jeho nastavení identické. Pokud se toto nastavení liší, bude se pravděpodobněji používat to, které jste zadali u kanálu CLUSRCVR. Toto chování je vysvětleno v tématu [Kanály klastru](#).

Tabulka 54. Atributy kanálu pro typy kanálů

Pole atributu	Parametr příkazu MQSC	SDR	SVR	RCV R	RQST R	CLNT-CONN	SVR-CONN	CLUS-SDR	CLUS-RCVR	AMQP
Afinita připojení	AFFINITY					Ano				
Změna data	ALTDATE	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Čas změny	ALTTIME	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
 AMQP-udržení aktivity	AMQPKA									Ano
Interval synchronizace dávek	BATCHHB	Ano	Ano					Ano	Ano	
Interval dávek	BATCHINT	Ano	Ano					Ano	Ano	
Omezení dávky	BATCHLIM	Ano	Ano					Ano	Ano	
batch siye, velikost dávky	BATCHSZ	Ano	Ano	Ano	Ano			Ano	Ano	
Popisek certifikátu	CERTLABL	Ano	Ano	Ano	Ano	Ano	Ano	Ano ¹ na stránce 91	Ano	Ano
Název kanálu	CHANNEL	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Typ kanálu	CHLTYPE	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Váha kanálu klienta	CLNTWGH T					Ano				
Seznam názvů klastru	CLUSNL							Ano	Ano	
Klastr	CLUSTER							Ano	Ano	
Priorita pracovní zátěže klastru	CLWLPRT Y							Ano	Ano	
Ohodnocení důležitosti pracovní zátěže klastru	CLWLRAN K							Ano	Ano	
Váha pracovní zátěže klastru	CLWLWGH T							Ano	Ano	


Tabulka 54. Atributy kanálu pro typy kanálů (pokračování)

Pole atributu	Parametr příkazu MQSC	SDR	SVR	RCV R	RQST R	CLNT-CONN	SVR-CONN	CLUS-SDR	CLUS-RCVR	AM QP
<u>Kompresa záhlaví</u>	COMPHDR	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Kompresa dat</u>	COMPMSG	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Název připojení</u>	CONNNAME	Ano	Ano		Ano	Ano		Ano	Ano	
<u>Konvertovat zprávu</u>	CONVERT	Ano	Ano					Ano	Ano	
<u>Výchozí opětovné připojení</u>	DEFRECON					Ano				
<u>Popis</u>	DESCR	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
<u>Interval odpojení</u>	DISCINT	Ano	Ano				Ano ^{"2"} na stránce 91	Ano	Ano	
<u>Interval synchronizace</u>	HBINT	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Interval udržení aktivity</u>	KAINT	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Lokální adresa</u>	LOCLADDR	Ano	Ano		Ano	Ano		Ano	Ano	Ano
<u>Počet dlouhých opakování</u>	LONGRTY	Ano	Ano					Ano	Ano	
<u>Interval dlouhých opakování</u>	LONGTMR	Ano	Ano					Ano	Ano	
<u>Maximální počet instancí</u>	MAXINST						Ano			Ano
<u>Maximální počet instancí na klienta</u>	MAXINSTC						Ano			
<u>Maximální délka zprávy</u>	MAXMSGL	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
<u>Název agenta kanálu zpráv</u>	MCANAME	Ano	Ano		Ano			Ano	Ano	
<u>Typ agenta oznamovacího kanálu</u>	MCATYPE	Ano	Ano		Ano			Ano	Ano	
<u>Uživatel agenta kanálu zpráv</u>	MCAUSER	Ano	Ano	Ano	Ano		Ano	Ano	Ano	Ano
<u>Název režimu LU 6.2</u>	MODENAME	Ano	Ano		Ano	Ano		Ano	Ano	
<u>Monitorování</u>	MONCHL	Ano	Ano	Ano	Ano		Ano	Ano	Ano	

Tabulka 54. Atributy kanálu pro typy kanálů (pokračování)

Pole atributu	Parametr příkazu MQSC	SDR	SVR	RCV R	RQST R	CLNT-CONN	SVR-CONN	CLUS-SDR	CLUS-RCVR	AM QP
<u>Uživatelská data uživatelské procedury pro opakování zpráv</u>	MRDATA			Ano	Ano				Ano	
<u>Název uživatelské procedury pro opakování zpráv</u>	MREXIT			Ano	Ano				Ano	
<u>Počet opakování zprávy</u>	MRRTY			Ano	Ano				Ano	
<u>Interval opakování zprávy</u>	MRTMR			Ano	Ano				Ano	
<u>Data uživatelské procedury pro zpracování zprávy</u>	MSGDATA	Ano	Ano	Ano	Ano			Ano	Ano	
<u>Název uživatelské procedury pro zpracování zprávy</u>	MSGEXIT	Ano	Ano	Ano	Ano			Ano	Ano	
<u>Priorita síťového připojení</u>	NETPRTY								Ano	
<u>Rychlost přechodných zpráv</u>	NPMSPEED	Ano	Ano	Ano	Ano			Ano	Ano	
<u>Password</u>	PASSWORD	Ano	Ano		Ano	Ano		Ano		
<u>Číslo portu</u>	PORT									Ano
PROPCTL volby kanálu pro MQGMO	PROPCTL	Ano	Ano					Ano	Ano	
<u>Oprávnění pro operaci vložení (Put)</u>	PUTAUT			Ano	Ano		Ano ^{"2"} na stránce 91		Ano	
<u>Název správce front</u>	QMNAME					Ano				
<u>Odebrání "2" na stránce 91</u>	QSGDISP	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Data uživatelské procedury pro přijetí zprávy</u>	RCVDATA	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	


Tabulka 54. Atributy kanálu pro typy kanálů (pokračování)

Pole atributu	Parametr příkazu MQSC	SDR	SVR	RCV R	RQST R	CLNT-CONN	SVR-CONN	CLUS-SDR	CLUS-RCVR	AM QP
<u>Jméno uživatele uživatelské procedury pro příjem</u>	RCVEXIT	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Data uživatelské procedury zabezpečení zprávy</u>	SCYDATA	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Název uživatelské procedury zabezpečení zprávy</u>	SCYEXIT	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Data uživatelské procedury pro odeslání zprávy</u>	SENDDAT A	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Název uživatelské procedury pro odeslání zprávy</u>	SENDEXIT	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Nejvyšší pořadové číslo</u>	SEQWRAP	Ano	Ano	Ano	Ano			Ano	Ano	
<u>Sdílená připojení</u>	SHARECN V					Ano	Ano			
<u>Počet krátkých opakování</u>	SHORTRT Y	Ano	Ano					Ano	Ano	
<u>Interval krátkých opakování</u>	SHORTTM R	Ano	Ano					Ano	Ano	
 <u>Ochrana zásad zabezpečení "2" na stránce 91</u>	SPLPROT	Ano	Ano	Ano	Ano					
<u>Ověření klienta pomocí SSL</u>	SSLCAUTH		Ano	Ano	Ano		Ano		Ano	Ano
<u>Specifikace šifrování zabezpečení SSL</u>	SSLCIPH	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
<u>Partner SSL</u>	SSLPEER	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
<u>Channel Statistics, Statistika kanálů</u>	STATCHL	Ano	Ano	Ano	Ano			Ano	Ano	
<u>LU 6.2 název transakčního programu</u>	TPNAME	Ano	Ano		Ano	Ano		Ano	Ano	
<u>Kořen tématu</u>	TPROOT									Ano

Tabulka 54. Atributy kanálu pro typy kanálů (pokračování)

Pole atributu	Parametr příkazu MQSC	SDR	SVR	RCV R	RQST R	CLNT-CONN	SVR-CONN	CLUS-SDR	CLUS-RCVR	AM QP
<u>Typ transportu</u>	TRPTYPE	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	
<u>Použit ID klienta</u>	USECLTID									Ano
<u>Použit frontu nedoručených zpráv</u>	USEDLQ	Ano	Ano	Ano	Ano			Ano	Ano	
<u>ID uživatele</u>	USERID	Ano	Ano		Ano	Ano		Ano		
<u>Jméno přenosové fronty</u>	XMITQ	Ano	Ano							

Notes:

1. Žádné z administrativních rozhraní nedovoluje, aby byl tento atribut zjišťován nebo nastaven pro kanály CLUSSDR. Obdržíte zprávu MQRCCF_WRONG_CHANNEL_TYPE . Atribut je však přítomen v objektech kanálu CLUSSDR (včetně struktur MQCD) a uživatelská procedura CHAD jej může v případě potřeby programově nastavit.
2.  Platí pouze na systému z/OS .

Produkt IBM MQ nemusí na některých platformách implementovat všechny atributy zobrazené v této sekci. Výjimky a rozdíly mezi platformami jsou uvedeny v popisech jednotlivých atributů, kde je to relevantní.

Název každého atributu je uveden v hranatých závorkách.

Atributy jsou uspořádány v abecedním pořadí ve skupinách.

Související odkazy

[Příkazy MQSC](#)

[POZMĚNIT KANÁL](#)

[Definovat kanál](#)

Atributy kanálu pro klíčová slova MQSC (A-B)

Abecední seznam atributů kanálu pro klíčová slova MQSC začínající písmenem A nebo B.

AFFINITY (afinita připojení)

Tento atribut určuje, zda klientské aplikace, které se připojují vícekrát pomocí stejného názvu správce front, používají stejný kanál klienta.

Tento atribut (MQIACH_CONNECTION_AFFINITY) použijte v případě, že je k dispozici více použitelných definic kanálů.

Možné hodnoty jsou:

Preferovaný

První připojení v procesu, které čte tabulku CCDT (Client Channel Definition Table), vytvoří seznam použitelných definic v závislosti na váze kanálu klienta, přičemž případné definice s vahou 0 jsou uvedeny jako první v abecedním pořadí. Každé připojení v procesu se pokusí připojit pomocí první definice v seznamu. Pokud se navázání připojení nezdaří, je použita další definice. Neúspěšné definice s vahou klienta jinou než 0 jsou přesunuty na konec seznamu. Definice s vahou klienta rovnou nule zůstávají na začátku seznamu a jsou pro každé připojení zkušeny jako první.

Každý proces klienta se stejným názvem hostitele vždy vytvoří stejný seznam.

V případě klientských aplikací napsaných v jazyce C, C++ nebo v programovacím rámci .NET (včetně plně spravovaných .NET) a v případě aplikací, které používají IBM MQ classes for Java a IBM MQ classes for JMS, je seznam aktualizován, pokud byla tabulka CCDT od vytvoření seznamu změněna.

Tato hodnota je výchozí a má hodnotu 1.

ŽÁDNÉ

První připojení v procesu, které čte tabulku CCDT, vytvoří seznam použitelných definic. Všechna připojení v procesu vyberou použitelnou definici v závislosti na váze kanálu klienta, přičemž případné definice s vahou 0 jsou vybrány jako první v abecedním pořadí.

V případě klientských aplikací napsaných v jazyce C, C++ nebo v programovacím rámci .NET (včetně plně spravovaných .NET) a v případě aplikací, které používají IBM MQ classes for Java a IBM MQ classes for JMS, je seznam aktualizován, pokud byla tabulka CCDT od vytvoření seznamu změněna.

Tento atribut je platný pouze pro typ kanálu připojení klienta.

ALTDATA (změna data)

Tento atribut je datum poslední změny definice ve formátu yyyy-mm-dd a je platný pro všechny typy kanálů.

ALTTIME (změna času)

Tento atribut je časem poslední změny definice ve formátu hh.mm.ss a je platný pro všechny typy kanálů.

AMQPKA (AMQP udržení aktivity)



Použijte atribut **AMQPKA** k uvedení doby trvání platnosti pro připojení klienta AMQP. Pokud klient AMQP neodeslal žádné rámce v intervalu udržení aktivity, pak je připojení uzavřeno.

Atribut **AMQPKA** určuje hodnotu atributu idle-timeout odeslanou z produktu IBM MQ klientovi AMQP. Atribut je časové období v milisekundách.

Je-li parametr **AMQPKA** nastaven na hodnotu > 0, bude hodnota IBM MQ téci polovinu této hodnoty jako atribut časového limitu nečinnosti. Například hodnota 10000 způsobí, že správce front odešle hodnotu časového limitu nečinnosti 5000. Klient by se měl ujistit, že jsou data odeslána do IBM MQ alespoň každých 10000 milisekund. Pokud v této době produkt IBM MQ nepřijme data, produkt IBM MQ předpokládá, že klient ztratil připojení a vynuceně uzavře připojení s chybovým stavem `amqp:resource-limit-exceeded`.

Hodnota AUTO nebo 0 znamená, že IBM MQ neproudí atribut časového limitu nečinnosti do klienta AMQP.

Klient AMQP může stále vlastní hodnotu časového limitu nečinnosti. Pokud ano, produkt IBM MQ protéká data (nebo prázdný rámec AMQP) alespoň tak často, aby informoval klienta, že je k dispozici.

BATCHHB (Interval synchronizace dávek)

jeho atribut umožňuje odesílajícímu kanálu ověřit, zda je přijímací kanál stále aktivní těsně před potvrzením dávky zpráv.

Interval prezenčního signálu dávky tedy umožňuje, aby byla dávka vrácena zpět, místo aby se stala nejistou, pokud přijímací kanál není aktivní. Zálohováním dávky zůstanou zprávy k dispozici pro zpracování, aby mohly být například přesměrovány na jiný kanál.

Pokud odesílací kanál měl komunikaci z přijímacího kanálu v rámci intervalu prezenčního signálu dávky, předpokládá se, že přijímací kanál je stále aktivní, jinak je přijímací kanál odeslán ke kontrole. Odesílací kanál čeká na odezvu přijímací strany kanálu pro interval, který vychází z počtu sekund uvedeného v atributu Interval prezenčního signálu (HBINT) kanálu.

Hodnota je v milisekundách a musí být v rozsahu od 0 do 999999. Hodnota nula označuje, že se nepoužívá tepová frekvence dávky.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Odesílatel klastru
- Příjemce klastru

BATCHINT (dávkový interval)

Tento atribut je období v milisekundách, během kterého kanál udržuje dávku otevřenou, i když v přenosové frontě nejsou žádné zprávy.

Můžete zadat libovolný počet milisekund, od nuly do 999 999 999 999. Výchozí hodnota je 0.

Pokud neuvedete interval dávky, dávka se zavře, když je splněna jedna z následujících podmínek:

- Počet zpráv uvedených v BATCHSZ byl odeslán.
- Počet bajtů uvedených v BATCLIM byl odeslán.
- Přenosová fronta je prázdná.

U kanálů s lehkým zatížením, kde se přenosová fronta často stává prázdnou, může být efektivní velikost dávky mnohem menší než BATCHSZ.

Atribut BATCHINT můžete použít k zefektivnění kanálů tím, že snížíte počet krátkých dávek. Mějte však na paměti, že dobu odezvy můžete zpomalit, protože dávky trvají déle a zprávy zůstávají déle nepotvrzené.

Zadáte-li BATCHINT, dávky se uzavírají pouze v případě, že je splněna jedna z následujících podmínek:

- Počet zpráv uvedených v BATCHSZ byl odeslán.
- Počet bajtů uvedených v BATCLIM byl odeslán.
- V přenosové frontě nejsou žádné další zprávy a při čekání na zprávy (od načtení první zprávy dávky) uplynul časový interval BATCHINT.

Poznámka: BATCHINT uvádí celkový čas strávený čekáním na zprávy. Nezahrnuje čas strávený načítáním zpráv, které jsou již k dispozici v přenosové frontě, ani čas strávený přenosem zpráv.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Odesílatel klastru
- Příjemce klastru

BATCLIM (limit dávky)

Tento atribut je limitem množství dat v kilobajtech, které lze odeslat prostřednictvím kanálu před vytvořením synchronizačního bodu.

Bod synchronizace se provede po zprávě, která způsobí dosažení limitu zpráv proteklých kanálem.

Hodnota musí být v rozsahu 0-999999. Výchozí hodnota je 5000.

Hodnota nula v tomto atributu znamená, že se na dávky v tomto kanálu nepoužije žádný datový limit.

Dávka se ukončí při splnění jedné z následujících podmínek:

- Byly odeslány zprávy BATCHSZ.
- Bylo odesláno BATCLIM bajtů.
- Přenosová fronta je prázdná a BATCHINT byl překročen.

Tento atribut je platný pro typy kanálů:

- Odesílatel

- Server
- Odesílatel klastru
- Příjemce klastru

BATCHSZ (Velikost dávky)

Tento atribut představuje maximální počet zpráv, které mají být odeslány před převzetím bodu synchronizace.

Velikost dávky nemá vliv na způsob, jakým kanál přenáší zprávy; zprávy jsou vždy přenášeny jednotlivě, ale jsou potvrzeny nebo vráceny jako dávka.

Chcete-li zlepšit výkon, můžete nastavit velikost dávky tak, aby definovala maximální počet zpráv, které mají být přeneseny mezi dvěma *synchronizačním bodem*. Velikost dávky, která se má použít, se vyjedná při spuštění kanálu a použije se nižší z obou definic kanálu. V některých implementacích je velikost dávky vypočtena na základě nejnižších ze dvou definic kanálu a dvou hodnot MAXUMSGS správce front. Skutečná velikost dávky může být menší; například dávka se dokončí, když v přenosové frontě nezbývají žádné zprávy nebo vyprší interval dávky.

Velká hodnota pro velikost dávky zvyšuje propustnost, ale časy obnovy se zvyšují, protože existuje více zpráv, které se mají vrátit zpět a znovu odeslat. Výchozí hodnota BATCHSZ je 50 a doporučuje se nejprve tuto hodnotu vyzkoušet. Můžete zvolit nižší hodnotu pro BATCHSZ, pokud je vaše komunikace nespolehlivá, což povede k větší pravděpodobnosti obnovy.

Procedura synchronizačního bodu potřebuje jedinečný logický identifikátor pracovní jednotky, který bude vyměňován v rámci propojení při každém synchronizačním bodu, aby bylo možné koordinovat procedury dávkového potvrzování.

Pokud je synchronizovaná procedura dávkového potvrzování přerušena, může se vyskytnout situace *nejistá*. Neověřené situace jsou vyřešeny automaticky při spuštění kanálu zpráv. Není-li toto řešení úspěšné, může být nutný ruční zásah pomocí příkazu RESOLVE.

Některé aspekty při výběru čísla pro velikost dávky:

- Je-li číslo příliš velké, velikost prostoru ve frontě zabraného na obou koncích odkazu bude příliš velká. Zprávy zabírají místo ve frontě, když nejsou potvrzeny, a nemohou být odebrány z front, dokud nejsou potvrzeny.
- Je-li pravděpodobné, že dojde k trvalému toku zpráv, můžete zvýšit výkon kanálu zvýšením velikosti dávky, protože k přenosu stejného množství bajtů je zapotřebí méně potvrzujících toků.
- Pokud charakteristika toku zpráv označuje, že zprávy přicházejí přerušovaně, může velikost dávky 1 s relativně velkým časovým intervalem odpojení poskytnout lepší výkon.
- Číslo může být v rozsahu 1 až 9999.
- I když přechodné zprávy v rychlém kanálu nečekají na synchronizační bod, přispívají k počtu dávek.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Příjemce
- Žadatel
- Odesílatel klastru
- Příjemce klastru

Atributy kanálu pro klíčová slova MQSC (C)

Abecední seznam atributů kanálu pro klíčová slova MQSC začínající písmenem C.

CERTLABL (popisek certifikátu)

Tento atribut určuje popisek certifikátu definice kanálu.

Popisek identifikuje, který osobní certifikát v úložišti klíčů je odeslán vzdálenému partnerovi. Certifikát je definován tak, jak je popsáno v tématu [Popisky digitálních certifikátů](#).

Příchozí kanály (včetně kanálů RCVR, RQSTR, CLUSRCVR, unqualified SERVER a SVRCONN) odešlou nakonfigurovaný certifikát pouze v případě, že verze IBM MQ vzdáleného partnera plně podporuje konfiguraci popisku certifikátu a kanál používá protokol TLS CipherSpec.

Pokud tomu tak není, atribut **CERTLABL** správce front určí odeslaný certifikát. Toto omezení je způsobeno tím, že mechanismus výběru popisků certifikátů pro příchozí kanály závisí na rozšíření protokolu TLS, které není ve všech případech podporováno. Zejména klienti Java a JMS nepodporují požadované rozšíření protokolu a vždy obdrží pouze certifikát nakonfigurovaný atributem správce front **CERTLABL**, bez ohledu na nastavení popisku specifického pro kanál.

Nekvalifikovaný kanál serveru je kanál, který nemá nastaveno pole CONNAME.

Žádné z administrativních rozhraní nedovoluje, aby byl tento atribut zjišťován nebo nastaven pro kanály CLUSSDR. Obdržíte zprávu MQRCCF_WRONG_CHANNEL_TYPE. Atribut je však přítomen v objektech kanálu CLUSSDR (včetně struktur MQCD) a uživatelská procedura CHAD jej může v případě potřeby programově nastavit.

Další informace o tom, co může popisek certifikátu obsahovat, naleznete v tématu [Popisky digitálních certifikátů s porozuměním požadavkům](#).

Tento atribut je platný pro všechny typy kanálů.

Poznámka: Pro SSL/TLS musí být CERTLABL definován v definici QMGR. Volitelně můžete nastavit CERTLABL na definici CHANNEL.

Správce front CERTLABL je zkontrolován a musí se jednat o platný osobní certifikát, a to i v případě, že nastavujete CERTLABL v definici CHANNEL.

CHANNEL (název kanálu)

Tento atribut určuje název definice kanálu.

Název může obsahovat až 20 znaků, ačkoli oba konce kanálu zpráv musí mít stejný název a jiné implementace mohou mít omezení velikosti, skutečný počet znaků může být menší.

Pokud je to možné, názvy kanálů jsou jedinečné pro jeden kanál mezi libovolnými dvěma správci front v síti propojených správců front.

Název musí obsahovat znaky z následujícího seznamu:

Abecední	(A-Z, a-z; Všimněte si, že velká a malá písmena jsou významná)
Číslice	(0-9)
Období	(.)
Dopředné lomítko	(/)
Podtržítka	(_)
Znak procentní části	(%)

Poznámka:

1. Vložené mezery nejsou povoleny a úvodní mezery jsou ignorovány.
2. V systémech používajících EBCDIC Katakana nelze používat malá písmena.

Tento atribut je platný pro všechny typy kanálů.

CHLTYPE (Typ kanálu)

Tento atribut určuje typ kanálu, který je definován.

Možné typy kanálů jsou:

Typy kanálů zpráv:

- Odesílatel
- Server
- Příjemce
- Žadatel
- Odesílatel klastru
- Příjemce klastru

Typy kanálů MQI:

- Připojení klienta (pouze AIX, Linux, and Windows)

Poznámka: Kanály připojení klienta lze také definovat v systému z/OS pro použití na jiných platformách.

- Připojení serveru
- AMQP

Oba konce kanálu musí mít stejný název a kompatibilní typy:

- Odesílatel s příjemcem
- Žadatel se serverem
- Žadatel s odesílatelem (pro zpětné volání)
- Server s přijímačem (server se používá jako odesílatel)
- Připojení klienta k serveru-připojení
- Odesílatel klastru s příjemcem klastru
- AMQP s AMQP

CLNTWGHT (váha kanálu klienta)

Tento atribut určuje váhu, která má ovlivnit, která definice kanálu připojení klienta je použita.

Díky použití atributu váhy kanálu klienta lze v případě, že je k dispozici více než jedna definice, náhodně vybrat definice kanálu připojení klienta v závislosti na jejich váze.

Pokud klient zadá požadavek MQCONN na připojení ke skupině správců front zadáním názvu správce front začínajícím hvězdičkou, který umožňuje vyrovnávání váhy klienta v několika správcích front, a v tabulce CCDT (Client Channel Definition Table) je k dispozici více než jedna vhodná definice kanálu, bude definice, která má být použita, náhodně vybrána na základě váhy, přičemž všechny příslušné definice CLNTWGHT (0) budou vybrány jako první v abecedním pořadí.

Poznámka: Při použití JSON CCDT je možné mít více kanálů se stejným názvem. Pokud existuje více kanálů se stejným názvem a mají CLNTWGHT (0), budou kanály vybrány v pořadí, v jakém jsou definovány v tabulce JSON CCDT.

Zadejte hodnotu v rozsahu 0 - 99. Výchozí hodnota je 0.

Hodnota 0 znamená, že není prováděno žádné vyvažování zátěže a dostupné definice jsou vybírány v abecedním pořadí. Chcete-li povolit vyvažování zátěže, vyberte hodnotu v rozsahu 1 až 99, přičemž hodnota 1 znamená nejnižší a hodnota 99 nejvyšší váhu. Rozdělení spojení mezi dva nebo více kanálů s nenulovými váhami je úměrné poměru těchto vah. Například tři kanály s hodnotami CLNTWGHT 2, 4 a 14 jsou vybrány přibližně 10%, 20% a 70% času. Tato distribuce není zaručena. Pokud je atribut AFFINITY připojení nastaven na hodnotu PREFERRED, první připojení zvolí definici kanálu podle vah klienta a následná připojení budou nadále používat stejnou definici kanálu.

Tento atribut je platný pouze pro typ kanálu připojení klienta.

CLUSNL (seznam názvů klastru)

Tento atribut je názvem seznamu názvů, který určuje seznam klastrů, ke kterým kanál patří.

Až jedna z výsledných hodnot CLUSTER nebo CLUSNL může být neprázdná. Pokud je jedna z hodnot neprázdná, druhá musí být prázdná.

Tento atribut je platný pro typy kanálů:

- Odesílatel klastru
- Příjemce klastru

Klastr (CLUSTER)

Tento atribut je název klastru, ke kterému kanál náleží.

Maximální délka je 48 znaků v souladu s pravidly pro pojmenování objektů IBM MQ .

Až jedna z výsledných hodnot CLUSTER nebo CLUSNL může být neprázdná. Pokud jedna z hodnot není prázdná, druhá musí být prázdná.

Tento atribut je platný pouze pro typy kanálů:

- Odesílatel klastru
- Příjemce klastru

CLWLPRTY (priorita pracovní zátěže klastru)

Atribut kanálu CLWLPRTY určuje pořadí priorit pro kanály pro distribuci pracovní zátěže klastru. Hodnota musí být v rozsahu 0-9, kde 0 je nejnižší priorita a 9 je nejvyšší.

Pomocí atributu kanálu CLWLPRTY můžete nastavit pořadí priorit pro dostupná místa určení klastru. Produkt IBM MQ vybere cíle s nejvyšší prioritou před výběrem cílů s nejnižší prioritou cíle klastru. Pokud existuje více míst určení se stejnou prioritou, vybere nejméně nedávno použité místo určení.

Pokud existují dva možné cíle, můžete pomocí tohoto atributu povolit překonání selhání. Zprávy se odesílají do správce front s kanálem s nejvyšší prioritou. Pokud nebude k dispozici, přejdou zprávy na dalšího správce front s nejvyšší prioritou. Správci front s nižší prioritou vystupují jako rezervy.

Produkt IBM MQ kontroluje stav kanálu před stanovením priority kanálů. Kandidáty na výběr jsou pouze dostupní správci front.

Notes:

- Určete tento atribut v přijímacím kanálu klastru v cílovém správci front. Jakékoli vyvážení, které zadáte v odpovídajícím odesílacím kanálu klastru, bude pravděpodobně ignorováno. Viz [Kanály klastru](#).
- Dostupnost vzdáleného správce front je založena na stavu kanálu pro daného správce front. Při spuštění kanálů se jejich stav několikrát změní, přičemž některé ze stavů mají nižší prioritu než algoritmus správy pracovní zátěže klastru. V praxi to znamená, že lze vybrat cíle s nižší prioritou (záložní), zatímco se začínají kanály s cíli s vyšší prioritou (primární).
- Potřebujete-li se ujistit, že do cíle zálohování nepřejdou žádné zprávy, nepoužívejte příkaz CLWLPRTY. Zvažte použití oddělených front nebo CLWLRANK s ručním přepínáním z primárního k zálohování.

CLWLRANK (rank pracovní zátěže klastru)

Atribut kanálu **CLWLRANK** určuje pořadí kanálů pro distribuci pracovní zátěže klastru. Hodnota musí být v rozsahu 0-9, kde 0 je nejnižší a 9 je nejvyšší.

Atribut kanálu **CLWLRANK** použijte v případě, že chcete řídit konečné místo určení pro zprávy odeslané správci front v jiném klastru. Výběr konečného místa určení můžete řídit nastavením pořadí kanálů, které připojují správce front ke správcům front brány v průniku klastrů.

Nastavíte-li parametr **CLWLRANK**, zprávy budou mít určenou trasu přes propojené klastry směrem k cíli s vyšším hodnocením. Zprávy například přicházejí do správce front brány, který je může odeslat jednomu ze dvou správců front s použitím kanálů s hodnocením 1 a 2. Jsou automaticky odesílány do správce front připojeného kanálem s nejvyšší hodnotou, v tomto případě kanál do správce front s hodnocením 2.

Produkt IBM MQ získá ohodnocení důležitosti kanálů před kontrolou stavu kanálu. Získání hodnoty před kontrolou stavu kanálu znamená, že pro výběr jsou k dispozici i nepřístupné kanály. Umožňuje směřování zpráv po síti i v případě, že konečný cíl není k dispozici.

Notes:

- Určete tento atribut v přijímacím kanálu klastru v cílovém správci front. Jakékoli vyvážení, které zadáte v odpovídajícím odesílacím kanálu klastru, bude pravděpodobně ignorováno. Viz [Kanály klastru](#).
- Pokud jste také použili atribut priority **CLWLPRTY**, produkt IBM MQ provede výběr mezi dostupnými cíli. Pokud není kanál k dispozici pro místo určení s nejvyšším hodnocením, je zpráva zadržena v přenosové frontě. Je uvolněn, když je kanál k dispozici. Zpráva se neodešle na další dostupný cíl v pořadí podle důležitosti.

CLWLWGHT (váha pracovní zátěže klastru)

Atribut kanálu CLWLWGHT určuje váhu použitou pro kanály CLUSSDR a CLUSRCVR pro distribuci pracovní zátěže klastru. Hodnota musí být v rozsahu 1-99, kde 1 je nejnižší váha a 99 je nejvyšší.

Použijte CLWLWGHT k odeslání serverů s větším výkonem zpracování více zpráv. Čím vyšší je váha kanálu, tím více zpráv je odesláno přes tento kanál.

Notes:

- Určete tento atribut v přijímacím kanálu klastru v cílovém správci front. Jakékoli vyvážení, které zadáte v odpovídajícím odesílacím kanálu klastru, bude pravděpodobně ignorováno. Viz [Kanály klastru](#).
- Je-li funkce CLWLWGHT upravena z výchozí hodnoty 50 na libovolném kanálu, bude vyrovňování pracovní zátěže záviset na celkovém počtu případů, kdy byl každý kanál vybrán pro zprávu odeslanou do libovolné klastrované fronty. Další informace viz téma [“Algoritmus správy pracovní zátěže klastru” na stránce 142](#).

COMPHDR (komprese záhlaví)

Tento atribut je seznam technik komprese dat záhlaví podporovaných kanálem.

Pro kanály odesilatele, serveru, odesilatele klastru, příjemce klastru a připojení klienta jsou zadané hodnoty v pořadí podle předvolby s první technikou komprese podporovanou vzdáleným koncem používaného kanálu. Vzájemně podporované techniky komprese kanálů jsou předány uživatelské proceduře pro zprávy vysílajícího kanálu, kde lze použitou techniku komprese změnit na základě jednotlivých zpráv. Komprese změní data předaná k odeslání a přijetí uživatelských procedur.

Možné hodnoty jsou:

ŽÁDNÉ

Neprovádí se žádná komprese dat hlavičky. Tato hodnota je výchozí hodnota.

SYSTÉM

Provádí se komprese dat hlavičky.

Tento atribut je platný pro všechny typy kanálů.

COMPMSG (komprese dat)

Tento atribut je seznam technik komprese dat zpráv podporovaných kanálem.

Pro kanály odesilatele, serveru, odesilatele klastru, příjemce klastru a připojení klienta jsou zadané hodnoty v pořadí podle předvolby. Použije se první technika komprese podporovaná vzdáleným koncem kanálu. Vzájemně podporované techniky komprese kanálů jsou předány uživatelské proceduře pro zprávy vysílajícího kanálu, kde lze použitou techniku komprese změnit na základě jednotlivých zpráv. Komprese

změní data předaná k odeslání a přijetí uživatelských procedur. Kompresi záhlaví zprávy viz [“COMPHDR \(komprese záhlaví\)”](#) na stránce 98 .

Možné hodnoty jsou:

ŽÁDNÉ

Neprovádí se žádná komprese dat zprávy. Tato hodnota je výchozí hodnota.

RLE

Komprese dat zprávy se provádí pomocí kódování délky spuštění.

ZLIBFAST

Komprese dat zprávy se provádí pomocí techniky komprese zlib. Preferuje se rychlá komprese.

ZLIBFAST lze volitelně odlehčovat do prostředí zEnterprise Data Compression. Další informace viz [zEDC Express facility](#) .

ZLIBHIGH

Komprese dat zprávy se provádí pomocí techniky komprese zlib. Preferuje se vysoká úroveň komprese.

ANY

Umožňuje kanálu podporovat libovolnou techniku komprese podporovanou správcem front. Podporováno pouze pro kanály Receiver, Requester a Server-Connection.

Tento atribut je platný pro všechny typy kanálů.

AIX V systému IBM MQ 9.3.0 mohou techniky ZLIBFAST a ZLIBHIGH používat knihovnu zlibNX s hardwarovou akcelerací v systému IBM MQ for AIX , pokud je nainstalována. Knihovna zlibNX je rozšířenou verzí knihovny komprese zlib, která podporuje hardwarově akcelerovanou kompresi a dekompresi dat pomocí koprocesorů s názvem NX (Nest accelerators) na serverech založených na procesorech IBM POWER9 . Knihovna zlibNX je k dispozici v produktu IBM AIX 7.2 s balíkem Technology Level 4 Expansion Pack a novějším. Vysoce komprimovatelné zprávy, jejichž velikost přesahuje 2KB , s největší pravděpodobností využijí volbu použití knihovny zlibNX , a to snížením využití procesoru. Chcete-li povolit, aby agent kanálu zpráv (MCA) používal knihovnu zlibNX , nastavte proměnnou prostředí AMQ_USE_ZLIBNX.

CONNNAME (Název připojení)

Tento atribut je identifikátor komunikačního připojení. Určuje konkrétní komunikační linky, které má tento kanál používat.

Pro kanály serveru je volitelné, pokud není spuštěn kanál serveru. V takovém případě musí být zadán název připojení.

Zadejte **CONNNAME** jako seznam názvů počítačů pro uvedené **TRPTYPE** oddělených čárkami. Obvykle se vyžaduje pouze jeden název počítače. Můžete zadat více názvů počítačů a nakonfigurovat více připojení se stejnými vlastnostmi. Tato připojení se obvykle zkouší v tom pořadí, ve kterém jsou uvedeny v seznamu připojení, dokud nedojde k úspěšnému navázání připojení. Pořadí je pro klienty upraveno, je-li zadán atribut **CLNTWGT**. Pokud nebylo žádné připojení úspěšné, kanál se pokusí o připojení znovu, jak určují atributy kanálu. Spolu s kanály klienta je seznam připojení alternativou při konfiguraci více připojení ke skupinám správců front. Spolu s kanály zpráv se seznam připojení používá ke konfiguraci připojení k alternativním adresám správce front s více instancemi.

Multi V [Multiplatforms](#) je parametr názvu připojení TCP/IP přijímacího kanálu klastru nepovinný. Pokud ponecháte název připojení prázdný, vygeneruje IBM MQ název připojení za vás a bude předpokládat výchozí port a bude používat aktuální adresu IP systému. Výchozí číslo portu můžete přepsat, ale i nadále se bude používat aktuální adresa IP systému. Pro každý název připojení ponechte název IP prázdný a zadejte číslo portu do závorek. Např.:

(1415)

Vygenerovaný řetězec **CONNNAME** je vždy ve formátu desítkových čísel oddělených tečkami (IPv4) nebo v hexadecimálním formátu (IPv6) a nikoli ve tvaru alfanumerického názvu hostitele DNS.

Maximální délka názvu závisí na platformě:

- ▶ **Multi** 264 znaků.
- ▶ **z/OS** 48 znaků (viz poznámka 1).

Je-li typ přenosu TCP

CONNNAME je buď název hostitele, nebo síťová adresa vzdáleného počítače (nebo lokální počítač pro přijímací kanály klastru). Například (ABC.EXAMPLE.COM), (2001:DB8:0:0:0:0:0:0) nebo (127.0.0.1). Může obsahovat číslo portu, například (MACHINE(123)).

▶ **z/OS** Může zahrnovat název IP dynamické skupiny DNS nebo vstupní port Network Dispatcher.

Pokud použijete adresu IPv6 v síti, která podporuje pouze produkt IPv4, název připojení se nevyřeší. V síti, která používá jak IPv4, tak IPv6, název připojení interaktivně spolupracuje s lokální adresou k určení, který zásobník IP se používá. Další informace viz [“LOCLADDR \(lokální adresa\)”](#) na stránce 104.

Je-li typ přenosu LU 6.2

▶ **Multi** Jsou-li zadány hodnoty TPNAME a MODENAME, zadejte plně kvalifikované jméno partnerské LU. Pokud jsou TPNAME a MODENAME prázdné, uveďte název objektu informací na straně CPI-C pro vaši specifickou platformu.

▶ **z/OS** Existují dva způsoby, jak zadat hodnotu:

- Název logické jednotky

Informace o logické jednotce pro správce front obsahující název logické jednotky, název TP a volitelný název režimu. Tento název lze zadat v jedné ze tří forem:

Formát	Příklad
luname	IGY12355
luname/TPname	IGY12345/APING
luname/TPname/modename	IGY12345/APINGD/#INTER

Pro první formulář musí být uveden název TP a název režimu pro atributy TPNAME a MODENAME; jinak musí být tyto atributy prázdné. Pro kanály připojení klienta je povolen pouze první formulář.

- Symbolický název

Symbolický název místa určení pro informace o logické jednotce pro správce front, jak je definován v datové sadě informací o straně. Atributy TPNAME a MODENAME musí být prázdné. Všimněte si, že v případě přijímacích kanálů klastru se informace o straně nacházejí v ostatních správcích front v klastru. V tomto případě se může jednat o název, který může uživatelská procedura automatické definice kanálu interpretovat jako příslušné informace o logické jednotce pro lokálního správce front.

Zadané nebo odvozené jméno LU může být názvem skupiny generických prostředků VTAM.

Je-li přenosový protokol NetBIOS

CONNNAME je název NetBIOS definovaný na vzdáleném počítači.

Pokud je přenosový protokol SPX

CONNNAME je adresa ve stylu SPX, která se skládá ze 4bajtové síťové adresy, 6bajtové adresy uzlu a 2bajtového čísla soketu. Zadejte tyto hodnoty v hexadecimální soustavě s adresami sítě a uzlu oddělenými tečkou a číslem soketu v hranatých závorkách. Příklad:

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

Pokud je číslo soketu vynecháno, použije se výchozí IBM MQ SPX číslo soketu. Výchozí hodnota je X'5E86'.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server

Pro kanály serveru je volitelné, pokud není spuštěn kanál serveru. V takovém případě musí být zadán název připojení.

- Žadatel
- Připojení klienta
- Odesílatel klastru
- Příjemce klastru

Poznámka:

1. U délek názvů můžete limit 48 znaků obejít jedním z následujících způsobů:

- Nastavte servery DNS tak, aby používaly například název hostitele "myserver" namísto "myserver.location.company.com", čímž zajistíte, že budete moci použít krátký název hostitele.
- Použít adresy IP.

2. Definice přenosového protokolu je obsažena v souboru [TRPTYPE](#).

CONVERT (Převést zprávu)

Tento atribut uvádí, že zpráva musí být před přenosem převedena do formátu požadovaného přijímajícím systémem.

Data zprávy aplikace jsou obvykle převedena přijímající aplikací. Pokud se však vzdálený správce front nachází na platformě, která nepodporuje převod dat, použijte tento atribut kanálu k určení, že zpráva musí být převedena do formátu vyžadovaného přijímajícím systémem **před** přenosem.

Možné hodnoty jsou yes a no. Pokud zadáte hodnotu yes, data aplikace ve zprávě se před odesláním převedou, pokud jste zadali jeden z názvů vestavěného formátu, nebo pokud je uživatelská procedura pro převod dat k dispozici pro formát definovaný uživatelem (viz [Zápis uživatelských procedur pro převod dat](#)). Zadáte-li no, data aplikace ve zprávě se před odesláním nepřevodou.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Odesílatel klastru
- Příjemce klastru

Atributy kanálu pro klíčová slova MQSC (D-L)

Abecední seznam atributů kanálu pro klíčová slova MQSC začínající písmeny D až L.

DEFRECON (výchozí opětovné připojení)

Určuje, zda připojení klienta automaticky znovu připojí klientskou aplikaci v případě přerušení připojení.

Možné hodnoty jsou:

NO (výchozí)

Pokud není přepsáno **MQCONN**, 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

Opětovné připojení je zakázáno, a to i v případě, že to vyžaduje klientský program pomocí volání **MQCONNX MQI**.

Tento atribut je platný pouze pro kanály připojení klienta.

DESCR (Popis)

Tento atribut popisuje definici kanálu a obsahuje až 64 bajtů textu.

Poznámka: Pokud systém používá dvoubajtovou znakovou sadu (DBCS), bude maximální počet znaků zredukován.

Použijte znaky ze znakové sady identifikované identifikátorem kódované znakové sady (CCSID) pro správce front, abyste se ujistili, že je text správně přeložen, pokud je odeslán jinému správci front.

Tento atribut je platný pro všechny typy kanálů.

DISCINT (Interval odpojení)

Tento atribut je doba, po které se kanál zavře, pokud během tohoto období nedorazí žádná zpráva.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Připojení k serveru pouze pomocí protokolu TCP
- Odesílatel klastru
- Příjemce klastru

Tento atribut je časový limit, uvedený v sekundách.

Pro kanály zpráv typu server-server (typ serveru, odesílací kanál klastru, odesílací kanál a přijímací kanál klastru) je interval měřen od bodu, ve kterém končí dávka, tj. po dosažení velikosti dávky nebo po vypršení intervalu dávky a vyprázdnění přenosové fronty. Pokud během uvedeného časového intervalu do přenosové fronty nedorazí žádné zprávy, kanál se zavře. (Čas je přibližný.)

Závěrečná výměna řídicích dat mezi dvěma konci kanálu zpráv server-server obsahuje informaci o příčině uzavření. Tím se zajistí, že odpovídající konec kanálu zůstane k dispozici pro opětovné spuštění.

Můžete zadat libovolný počet sekund od nuly do 999 999, kde hodnota nula znamená žádné odpojení; čekat nekonečně dlouho.

Výchozí hodnota je 6000 sekund (100 minut) pro kanály zpráv typu server-server a 0 (bez časového limitu) pro kanály připojení serveru. Můžete změnit výchozí hodnotu, která se používá pro nové kanály, které vytváříte, změnou výchozích objektů kanálu. Změňte například atribut DISCINT v systému SYSTEM.DEF.SENDER nastaví novou výchozí hodnotu pro nové odesílací kanály, které definujete.

Pro kanály připojení serveru používající protokol TCP představuje interval hodnotu odpojení neaktivity klienta určenou v sekundách. Pokud program kanálu připojení serveru nepřijal po tuto dobu žádnou komunikaci od svého partnerského klienta, ukončí připojení.

Interval nečinnosti připojení serveru se používá mezi voláními rozhraní API IBM MQ z klienta.

Poznámka: Potenciálně přerušitelný příkaz MQGET s voláním wait není klasifikován jako nečinnost, a proto nikdy neuplyne časový limit v důsledku vypršení DISCINT.



Upozornění: Výkon je ovlivněn hodnotou uvedenou pro interval odpojení.

Nízká hodnota (například několik sekund) může negativně ovlivňovat výkon systému tím, že se kanál neustále zastavuje a znovu spouští. Velká hodnota (více než hodinu) může znamenat, že jsou systémové prostředky spotřebovány bez přínosu. Můžete také určit interval prezenčního signálu, takže pokud v přenosové frontě nejsou žádné zprávy, odesílající agent MCA odešle tok prezenčního signálu přijímajícímu adaptéru MCA, čímž dává přijímajícímu adaptéru MCA možnost uvést kanál do klidového stavu bez čekání na vypršení intervalu odpojení. Aby tyto dvě hodnoty fungovaly efektivně, musí být hodnota intervalu prezenčního signálu výrazně nižší než hodnota intervalu odpojení.

Výchozí hodnota DISCINT pro kanály zpráv server-server je 6000 sekund (100 minut). Hodnota několika minut je však často rozumnou hodnotou, kterou lze použít bez dopadu na výkon nebo ponechání kanálů spuštěných zbytečně dlouhou dobu. Je-li to vhodné pro vaše prostředí, můžete tuto hodnotu změnit buď na každém jednotlivém kanálu, nebo změnou atributu DISCINT ve výchozích definicích kanálu (například SYSTEM.DEF.SENDER pro odesílací kanály) před vytvořením vlastních kanálů.

Další informace naleznete v tématu [Zastavení a uvedení kanálů do klidového stavu](#).

HBINT (interval prezenčního signálu)

Tento atribut určuje přibližnou dobu mezi toky synchronizačních signálů, které mají být předány od agenta MCA (odeslání kanálu zpráv) v případě, že v přenosové frontě nejsou žádné zprávy.

Toky synchronizace odblokují přijímajícího agenta MCA, který čeká na vložení zpráv nebo na vypršení intervalu odpojení. Je-li přijímající agent MCA odblokován, může kanál odpojit bez čekání na vypršení intervalu odpojení. Synchronizační toky také uvolní všechny vyrovnávací paměti, které byly přiděleny pro velké zprávy, a zavřou všechny fronty, které zůstaly otevřené na přijímacím konci kanálu.

Hodnota je v sekundách a musí být v rozsahu 0-999 999 999. Hodnota nula znamená, že se neodešlou žádné toky prezenčního signálu. Výchozí hodnota je 300. Aby byla hodnota nejužitečnější, musí být výrazně nižší než hodnota intervalu odpojení.

U aplikací, které používají rozhraní API IBM MQ classes for Java, JMS nebo .NET, je hodnota HBINT určena jedním z následujících způsobů:

- Buď hodnotou v kanálu SVRCONN používanou aplikací.
- Nebo hodnotou kanálu CLNTCONN, pokud byla aplikace konfigurována pro použití tabulky CCDT.

Pro kanály připojení serveru a připojení klienta mohou prezenční signály proudit nezávisle na straně serveru i na straně klienta. Pokud pro interval prezenčního signálu nebyla v kanálu přenesena žádná data, agent MQI připojení klienta odešle tok prezenčního signálu a agent MQI připojení serveru na něj odpoví jiným tokem prezenčního signálu. K tomu dochází bez ohledu na stav kanálu, například bez ohledu na to, zda je při volání rozhraní API neaktivní, nebo zda je neaktivní při čekání na uživatelský vstup klienta. Agent MQI připojení serveru je také schopen iniciovat prezenční signál klientovi znovu bez ohledu na stav kanálu. Aby se zabránilo vzájemnému tlukotu agentů MQI pro připojení serveru a připojení klienta současně, je synchronizační signál serveru přenášen poté, co v kanálu nebyla přenesena žádná data pro interval prezenčního signálu plus 5 sekund.

Pro kanály připojení serveru a připojení klienta pracující v režimu kanálu před produktem IBM WebSphere MQ 7.0 probíhá synchronizační signály pouze v případě, že agent MCA serveru čeká na příkaz MQGET se zadanou volbou WAIT, kterou vydal jménem klientské aplikace.

Další informace o práci kanálů MQI ve dvou režimech naleznete v tématu [SharingConversations \(MQLONG\)](#).

KAINT (interval udržení aktivity)

Tento atribut se používá k určení hodnoty časového limitu pro kanál.

Atribut Interval udržení aktivity je hodnota předaná do komunikačního zásobníku uvádějící časování udržení aktivity pro kanál. Umožňuje určit jinou hodnotu udržení aktivity pro každý kanál.

Pro jednotlivé kanály můžete nastavit atribut Interval udržení aktivity (KAIN T).

Multi V systému Multiplatforms můžete přistupovat k parametru a upravovat jej, ale je pouze uložen a postoupen; neexistuje žádná funkční implementace parametru. Potřebujete-li funkčnost poskytovanou parametrem KAIN T, použijte parametr Interval prezenčního signálu (HBINT), jak je popsáno v tématu “HBINT (interval prezenčního signálu)” na stránce 103.

Aby měl tento atribut nějaký účinek, musí být povoleno udržení aktivity TCP/IP.

- **z/OS** V systému z/OS povolíte udržení aktivity zadáním příkazu ALTER QMGR TCPKEEP (YES) MQSC.
- **Multi** V systému Multiplatforms se vyskytne, když je uveden parametr KEEPALIVE=YES v sekci TCP v konfiguračním souboru distribuovaných front, qm .ini, nebo prostřednictvím IBM MQ Explorer.

Udržení aktivity musí být také povoleno v rámci samotného TCP/IP, pomocí datové sady konfigurace profilu TCP.

Hodnota označuje čas v sekundách a musí být v rozsahu 0-99999. Hodnota intervalu udržení aktivity 0 označuje, že pro kanál není povoleno udržení aktivity specifické pro kanál a je použita pouze hodnota pro udržení aktivity nastavená v rámci celého systému v protokolu TCP/IP. Můžete také nastavit KAIN T na hodnotu AUTO (tato hodnota je výchozí). Je-li hodnota KAIN T nastavena na AUTO, bude hodnota Keepalive založena na hodnotě vyjednaného intervalu prezenčního signálu (HBINT):

Vyjednaný HBINT	KAIN T
>0	Vyjednané HBINT + 60 sekund
0	0

Tento atribut je platný pro všechny typy kanálů.

Hodnota je ignorována pro všechny kanály s jiným typem TransportType (TRPTYPE) než TCP nebo SPX.

LOCLADDR (lokální adresa)

Tento atribut určuje lokální komunikační adresu kanálu.

Poznámka: Kanály AMQP nepodporují stejný formát LOCLADDR jako ostatní kanály IBM MQ . Další informace viz téma “#unique_51/unique_51_Connect_42_locladdr_amqp” na stránce 106.

LOCLADDR pro všechny kanály kromě kanálů AMQP

Tento atribut se používá pouze v případě, že typ přenosu (TRPTYPE) je TCP/IP. Pro všechny ostatní typy přenosu se ignoruje.

Je-li zadána hodnota LOCLADDR , bude kanál, který je zastaven a poté restartován, nadále používat adresu TCP/IP uvedenou v souboru LOCLADDR. Ve scénářích obnovy může být tento atribut užitečný, když kanál komunikuje přes bránu firewall. Je to užitečné, protože odstraňuje problémy způsobené restartováním kanálu s adresou IP zásobníku TCP/IP, ke kterému je připojen. Produkt LOCLADDR může také vynutit, aby kanál používal zásobník IPv4 nebo IPv6 v duálním systému, nebo zásobník v duálním režimu v jednom systému zásobníku.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Žadatel
- Připojení klienta
- Odesílatel klastru

- Příjemce klastru

Pokud produkt LOCLADDR obsahuje síťovou adresu, musí se jednat o síťové adresy náležející k síťovému rozhraní v systému, v němž je kanál spuštěn. Například při definování odesílacího kanálu ve správci front ALPHA pro správce front BETA pomocí následujícího příkazu MSQC:

```
DEFINE CHANNEL(TO.BETA) CHLTYPE(SDR) CONNAME(192.0.2.0) XMITQ(BETA) LOCLADDR(192.0.2.1)
```

Adresa LOCLADDR je IPv4 adresa 192.0.2.1. Tento kanál odesílatele je spuštěn v systému správce front ALPHA, takže adresa IPv4 musí patřit k jednomu ze síťových rozhraní jeho systému.

Hodnotou je volitelná adresa IP, volitelný port nebo rozsah portů, které se budou používat pro odchozí komunikaci TCP/IP. Formát této informace je následující:

```
LOCLADDR([ip-addr][(low-port[,high-port])][,[ip-addr][(low-port[,high-port])]])
```

Maximální délka pole **LOCLADDR**, včetně více adres, je MQ_LOCAL_ADDRESS_LENGTH.

Vynecháte-li **LOCLADDR**, automaticky se alokuje lokální adresa.

Všimněte si, že můžete nastavit **LOCLADDR** pro klienta jazyka C pomocí tabulky definic kanálů klienta (CCDT).

Všechny parametry jsou volitelné. Vynechání části adresy ip-addr umožní nakonfigurovat pevné číslo portu pro brány firewall IP. Vynechání čísla portu umožní výběr určitého síťového adaptéru, aniž byste museli identifikovat jedinečné číslo lokálního portu. Sada protokolu TCP/IP vygeneruje jedinečné číslo portu.

Uveďte [, [ip-addr][(low-port[,high-port])]] vícekrát, pro každou další lokální adresu. Více lokálních adres použijte v případě, že chcete zadat specifickou podmnožinu lokálních síťových adaptérů. Můžete také použít produkt [, [ip-addr][(low-port[,high-port])]] k reprezentaci konkrétní lokální síťové adresy na různých serverech, které jsou součástí konfigurace správce front s více instancemi.

ip-addr

ip-addr se uvádí v jednom z těchto tří formátů:

tečková dekadická notace IPv4

Například: 192.0.2.1

hexadecimální notace IPv6

Například: 2001:DB8:0:0:0:0:0:0

alfanumerický název hostitele

Například: WWW.EXAMPLE.COM

low-port and high-port

low-port a high-port jsou čísla portů uzavřená do závorek.

Následující tabulka ukazuje, jak lze použít parametr **LOCLADDR**:

<i>Tabulka 57. Příklady způsobu použití parametru LOCLADDR</i>	
LOCLADDR	Význam
9.20.4.98	Kanál se spojí s touto adresou lokálně.
9.20.4.98, 9.20.4.99	Kanál se spojí s některou z uvedených adres IP. Těmito adresami mohou být dva síťové adaptéry na jednom serveru, nebo různé síťové adaptéry na dvou různých serverech v konfiguraci s více instancemi.
9.20.4.98(1000)	Kanál se spojí s touto adresou a portem 1000 lokálně.
9.20.4.98(1000,2000)	Kanál se lokálně spojí s touto adresou a použije port v rozsahu 1000 - 2000.
(1000)	Kanál se lokálně spojí s portem 1000.

Tabulka 57. Příklady způsobu použití parametru **LOCLADDR** (pokračování)

LOCLADDR	Význam
(1000,2000)	Kanál se lokálně spojí s portem z rozsahu 1000 - 2000.

Při spuštění kanálu hodnoty uvedené pro název připojení (CONNAME) a lokální adresu (LOCLADDR) určují, který zásobník IP se použije pro komunikaci. Použitý zásobník IP je určen takto:

- Pokud má systém nakonfigurován pouze zásobník IPv4 , vždy se použije zásobník IPv4 . Pokud je lokální adresa (LOCLADDR) nebo název připojení (CONNAME) uveden jako síťová adresa IPv6 , vygeneruje se chyba a kanál se nespustí.
- Pokud má systém nakonfigurován pouze zásobník IPv6 , vždy se použije zásobník IPv6 . Je-li lokální adresa (LOCLADDR) uvedena jako síťová adresa IPv4 , vygeneruje se chyba a kanál se nespustí. Je-li na platformách podporujících mapované adresování systému IPv6 zadán název připojení (CONNAME) jako síťová adresa systému IPv4 , je tato adresa mapována na adresu systému IPv6 . Například xxx . xxx . xxx . xxx je mapován na : : ffff : xxx . xxx . xxx . xxx. Použití mapovaných adres může vyžadovat překladače protokolu. Pokud je to možné, vyvarujte se použití mapovaných adres.
- Pokud je lokální adresa (LOCLADDR) uvedena jako adresa IP pro kanál, použije se zásobník pro tuto adresu IP. Pokud je lokální adresa (LOCLADDR) uvedena jako název hostitele, který se interpretuje na adresy IPv4 i IPv6 , název připojení (CONNAME) určuje, který ze zásobníků se používá. Pokud jsou lokální adresa (LOCLADDR) i název připojení (CONNAME) zadány jako názvy hostitelů, které se interpretují na adresy IPv4 i IPv6 , je použitý zásobník určen atributem správce front IPADDRV.
- Pokud má systém nakonfigurované duální zásobníky IPv4 a IPv6 a lokální adresa (LOCLADDR) není uvedena pro kanál, název připojení (CONNAME) uvedený pro kanál určuje, který zásobník IP se má použít. Pokud je název připojení (CONNAME) zadán jako název hostitele, který se interpretuje na adresy IPv4 i IPv6 , je použitý zásobník určen atributem správce front IPADDRV.

Multi V systému Multiplatformsmůžete nastavit výchozí hodnotu lokální adresy, která se použije pro všechny odesílací kanály, které nemají definovanou lokální adresu. Výchozí hodnota je definována nastavením proměnné prostředí MQ_LCLADDR před spuštěním správce front. Formát hodnoty odpovídá formátu atributu MQSC LOCLADDR.

Lokální adresy s odesílacími kanály klastru

Odesílací kanály klastru vždy dědí konfiguraci odpovídajícího přijímacího kanálu klastru, jak je definováno v cílovém správci front. To platí i v případě, že existuje lokálně definovaný odesílací kanál klastru se stejným názvem. V takovém případě se ruční definice používá pouze pro počáteční komunikaci.

Z tohoto důvodu není možné záviset na parametru LOCLADDR definovaném v přijímacím kanálu klastru, protože je pravděpodobné, že adresa IP není vlastněna systémem, kde jsou vytvořeni odesílatelé klastru. Z tohoto důvodu by neměl být parametr LOCLADDR na přijímači klastru použit, pokud není důvod omezit pouze porty, ale ne adresu IP pro všechny potenciální odesílatele klastru, a je známo, že tyto porty jsou k dispozici na všech systémech, kde může být vytvořen odesílací kanál klastru.

Pokud musí klastr použít příkaz LOCLADDR k získání odchozích komunikačních kanálů pro vytvoření vazby na specifickou adresu IP, použijte buď uživatelskou proceduru automatické definice kanálu, nebo použijte výchozí parametr LOCLADDR pro správce front, je-li to možné. Při použití výstupu kanálu vynutí hodnotu LOCLADDR z výstupu do libovolného automaticky definovaného kanálu CLUSSDR.

Používáte-li pro odesílací kanály klastru jinou než výchozí hodnotu LOCLADDR prostřednictvím uživatelské procedury nebo výchozí hodnoty, musí mít každý odpovídající ručně definovaný odesílací kanál klastru, například pro správce front úplného úložiště, také nastavenou hodnotu LOCLADDR, která umožní počáteční komunikaci prostřednictvím kanálu.

Poznámka: Pokud operační systém vrátí chybu vazby pro port dodaný v produktu LOCLADDR (nebo všechny porty, pokud je zadán rozsah portů), kanál se nespustí; systém vydá chybovou zprávu.

LOCLADDR pro kanály AMQP

Kanály AMQP podporují jiný formát LOCLADDR než jiné kanály IBM MQ :

LOCLADDR (*ip-addr*)

LOCLADDR je lokální komunikační adresa kanálu. Tento parametr použijte, chcete-li vynutit, aby klient používal konkrétní adresu IP. LOCLADDR je také užitečné vynutit, aby kanál používal adresu IPv4 nebo IPv6 , je-li k dispozici volba, nebo použít konkrétní síťový adaptér v systému s více síťovými adaptéry.

Maximální délka LOCLADDR je MQ_LOCAL_ADDRESS_LENGTH.

Vynecháte-li LOCLADDR, automaticky se alokuje lokální adresa.

ip-addr

ip-addr je jedna síťová adresa uvedená v jednom ze tří formátů:

tečková dekadická notace IPv4

Například: 192 . 0 . 2 . 1

hexadecimální notace IPv6

Například: 2001 : DB8 : 0 : 0 : 0 : 0 : 0 : 0

alfanumerický název hostitele

Například: WWW . EXAMPLE . COM

Je-li zadána adresa IP, bude ověřen pouze formát adresy. Samotná adresa IP není ověřena.

Další informace viz [Práce s automaticky definovanými odesílacími kanály klastru](#) .

LONGRTY (Počet dlouhých opakování)

Tento atribut určuje maximální počet pokusů kanálu o přidělení relace svému partnerovi.

Atribut **long retry count** lze nastavit od nuly do 999 999 999 999.

Tento atribut je platný pro následující typy kanálů:

- Odesílatel
- Server
- Odesílatel klastru
- Příjemce klastru

Pokud se počáteční pokus o alokaci nezdaří, počet *krátkých opakování* se sníží a kanál zopakuje zbývající počet pokusů. Pokud se stále nezdaří, zopakuje *počet dlouhých opakování* s intervalem *intervalu dlouhých opakování* mezi jednotlivými pokusy. Pokud je stále neúspěšný, kanál se zavře. Kanál pak musí být restartován pomocí příkazu; není automaticky spuštěn inicializátorem kanálu.

z/OS V systému z/OSnemůže kanál zadat opakování, pokud byl překročen maximální počet kanálů (**MAXCHL**).

Multi V systému [Multiplatforms](#) musí být spuštěn inicializátor kanálu, aby bylo možné pokus zopakovat. Inicializátor kanálu musí monitorovat inicializační frontu určenou v definici přenosové fronty, kterou kanál používá.

Je-li inicializátor kanálu (v systému z/OS) nebo kanál (v systému [Multiplatforms](#)) zastaven při opakovaném pokusu kanálu, jsou *počet krátkých opakování* a *počet dlouhých opakování* resetovány při restartování inicializátoru kanálu nebo kanálu nebo při úspěšném vložení zprávy do kanálu odesílatele. Avšak, pokud inicializátor kanálu (na z/OS) nebo správce front (na platformě [Multiplatforms](#)) je vypnutý a restartovaný, *počet krátkých opakování* a *počet dlouhých opakování* nejsou resetovány. Kanál zachová hodnoty počtu opakování, které měl před restartováním správce front nebo před vložení zprávy.

Multi V systému [Multiplatforms](#):

1. Když kanál přejde ze stavu RETRYING do stavu RUNNING, *počet krátkých opakování* a *počet dlouhých opakování* nejsou okamžitě resetovány. Jsou resetovány pouze v případě, že první zpráva úspěšně

protéká kanálem po přechodu kanálu do stavu SPUŠTĚNO, tj. když lokální kanál potvrdí počet zpráv odeslaných na druhý konec.

2. Počet krátkých opakování a počet dlouhých opakování jsou resetovány při restartování kanálu.

LONGTMR (Interval dlouhých opakování)

Tento atribut představuje přibližný interval v sekundách, po který má kanál čekat před opětovným pokusem o navázání připojení během režimu dlouhého opakování.

Interval mezi opakovanými pokusy lze prodloužit, pokud má kanál čekat na aktivaci.

Počet pokusů kanálu o připojení *long retry* v tomto dlouhém intervalu po počtu pokusů o *počet krátkých opakování* v intervalu krátkých opakování.

Tento atribut lze nastavit od nuly do 999 999.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Odesílatel klastru
- Příjemce klastru

Atributy kanálu pro klíčová slova MQSC (M)

Abecední seznam atributů kanálu pro klíčová slova MQSC začínající písmenem *M*.

MAXINST (Maximální počet instancí)

Tento atribut určuje maximální počet souběžných instancí kanálu připojení serveru nebo kanálu AMQP, které lze spustit.

Maximální počet instancí připojení kanálu připojení serveru

Pro kanál připojení serveru tento atribut určuje maximální počet souběžných instancí kanálu připojení serveru, které lze spustit.

Tento atribut lze nastavit od nuly do 999 999 999 999. Nulová hodnota označuje, že v tomto kanálu nejsou povolena žádná připojení klienta. Výchozí hodnota je 999 999 999.

Je-li hodnota snížena tak, že je menší než počet instancí kanálu připojení serveru, které jsou aktuálně spuštěny, nebudou spuštěné kanály ovlivněny. Nové instance však nelze spustit, dokud nepřestane běžet dostatečný počet existujících instancí.

Maximální počet instancí připojení kanálu AMQP

Pro kanál AMQP tento atribut uvádí maximální počet souběžných instancí kanálu AMQP, které lze spustit.

Tento atribut lze nastavit od nuly do 999 999 999 999. Nulová hodnota označuje, že v tomto kanálu nejsou povolena žádná připojení klienta. Výchozí hodnota je 999 999 999.

Pokud se klient pokusí o připojení a počet připojených klientů dosáhl hodnoty MAXINST, kanál uzavře připojení s uzavřeným rámcem. Rámec zavření obsahuje následující zprávu:

```
amqp:resource-limit-exceeded
```

Pokud se klient připojí s ID, které je již připojeno (tj. provádí převzetí klienta), bude převzetí úspěšné bez ohledu na to, zda počet připojených klientů dosáhl hodnoty MAXINST.

Další informace viz [Omezení kanálu připojení serveru](#) .

MAXINSTC (Maximální počet instancí na klienta)

Tento atribut určuje maximální počet souběžných instancí kanálu připojení serveru, které lze spustit z jednoho klienta.

Tento atribut lze nastavit od nuly do 999 999 999 999. Nulová hodnota označuje, že v tomto kanálu nejsou povolena žádná připojení klienta. Výchozí hodnota je 999 999 999.

Pokud je hodnota snížena tak, že je menší než počet instancí kanálu připojení serveru, které jsou aktuálně spuštěny z jednotlivých klientů, nebudou spuštěné kanály ovlivněny. Nové instance z těchto klientů však nelze spustit, dokud nepřestane běžet dostatečný počet existujících instancí.

Tento atribut je platný pouze pro kanály připojení serveru.

Další informace viz [Omezení kanálu připojení serveru](#).

MAXMSGL (Maximální délka zprávy)

Tento atribut určuje maximální délku zprávy, kterou lze přenést kanálem.

Multi V systému Multiplatformszadejte hodnotu větší nebo rovnou nule a menší nebo rovnou maximální délce zprávy pro správce front. Další informace viz parametr MAXMSGL příkazu ALTER QMGR v [ALTER QMGR](#).

z/OS V systému IBM MQ for z/OSzadejte hodnotu větší nebo rovnou nule a menší nebo rovnou 104 857 600 bajtů (tj. 100 MB).

Protože různé implementace systémů IBM MQ existují na různých platformách, velikost dostupná pro zpracování zpráv může být v některých aplikacích omezena. Toto číslo musí odrážet velikost, kterou váš systém zvládne bez stresu. Při spuštění kanálu se vezme nižší ze dvou čísel na obou koncích kanálu.

Poznámka: Pro kanál můžete použít maximální velikost zprávy 0, což znamená, že velikost má být nastavena na maximální hodnotu lokálního správce front.

Přidáním digitálního podpisu a klíče ke zprávě produkt [Advanced Message Security](#) zvýší délku zprávy.

Tento atribut je platný pro všechny typy kanálů.

MCANAME (název agenta kanálu zpráv)

Tento atribut je vyhrazený, pokud je uveden, musí být nastaven pouze na mezery a maximální délka je 20 znaků.

MCATYPE (typ agenta kanálu zpráv)

Tento atribut může určovat agenta kanálu zpráv jako proces nebo podproces.

Mezi výhody spuštění jako procesu patří:

- Izolace pro každý kanál poskytující větší integritu
- Oprávnění úlohy specifické pro každý kanál
- Řízení plánování úloh

Mezi výhody vláken patří:

- Mnohem nižší využití úložiště
- Snadnější konfigurace zadáním na příkazový řádek
- Rychlejší provedení-spuštění podprocesu je rychlejší než instruování operačního systému ke spuštění procesu.

Poznámka: Pro typy kanálů odesílatel, server a žadatel je výchozí hodnota process. Pro typy kanálů odesílatel klastru a příjemce klastru je výchozí hodnota podproces. Tato výchozí nastavení se mohou během instalace změnit.

Zadáte-li v definici kanálu proces , spustí se proces RUNMQCHL. Zadáte-li podproces, spustí se agent MCA na podprocesu procesu AMQRMPPA nebo na podprocesu RUNMQCHI, pokud je zadán parametr **MQNOREMPOOL** . V počítači, který přijímá příchozí přidělení, je agent MCA spuštěn jako podproces, pokud používáte **RUNMQLSR**. Pokud používáte **inetd**, spustí se jako proces.

z/OS V systému IBM MQ for z/OS je tento atribut podporován pouze pro kanály s typem kanálu příjemce klastru.

Multi Na jiných platformách je tento atribut platný pro typy kanálů:

- Odesílatel
- Server
- Žadatel
- Odesílatel klastru
- Příjemce klastru

MCAUSER (Identifikátor uživatele agenta kanálu zpráv)

Tento atribut je identifikátor uživatele (řetězec), který má být použit agentem MCA pro autorizaci pro přístup k prostředkům IBM MQ .

Poznámka: Alternativním způsobem, jak poskytnout ID uživatele pro kanál, pod kterým se má spustit, je použít záznamy ověření kanálu. U záznamů ověřování kanálu mohou různá připojení používat stejný kanál při použití různých pověření. Pokud je v kanálu nastaven atribut MCAUSER a pro stejný kanál jsou použity záznamy ověřování kanálu, mají přednost záznamy ověřování kanálu. Atribut MCAUSER v definici kanálu se používá pouze v případě, že záznam ověřování kanálu používá hodnotu USERSRC (CHANNEL).

Toto oprávnění zahrnuje (je-li oprávnění PUT DEF) vložení zprávy do cílové fronty pro kanály příjemce nebo žadatele.

V systému IBM MQ for Windows může být identifikátor uživatele kvalifikovaný doménou pomocí formátu `user@domain`, kde `domain` musí být buď doména systému Windows lokálního systému, nebo důvěryhodná doména.

Je-li tento atribut prázdný, použije agent MCA svůj výchozí identifikátor uživatele. Další informace viz [DEFINE CHANNEL](#).

Tento atribut je platný pro typy kanálů:

- Příjemce
- Žadatel
- Připojení serveru
- Příjemce klastru

MODENAME (LU 6.2 název režimu)

Tento atribut je určen pro použití s připojeními LU 6.2. Poskytuje další definici charakteristik relace připojení, když se provádí alokace komunikační relace.

Při použití informací o straně pro komunikace SNA je název režimu definován v objektu CPI-C Communications Side Object nebo v informacích o straně APPC a tento atribut musí být ponechán prázdný; jinak musí být nastaven na název režimu SNA.

Název musí být dlouhý jeden až osm alfanumerických znaků.

Tento atribut je platný pouze pro typy kanálů:

- Odesílatel
- Server
- Žadatel

- Připojení klienta
- Odesílatel klastru
- Příjemce klastru

MONCHL (monitorování)

Tento atribut řídí shromažďování online dat monitorování.

Možné hodnoty jsou:

QMGR

Kolekce dat monitorování online je zděděna z nastavení atributu MONCHL v objektu správce front. Tato hodnota je výchozí hodnota.

VYP

Shromažďování dat monitorování online pro tento kanál je zakázáno.

NÍZKÁ

Nízký poměr shromažďování dat s minimálním dopadem na výkon. Zobrazené výsledky monitorování však nemusí být aktuální.

STŘEDNÍ

Střední poměr shromažďování dat s omezeným dopadem na výkon systému.

VYSOKÁ

Vysoký poměr sběru dat s možností ovlivnit výkon. Zobrazené výsledky monitorování jsou však nejaktuálnější.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Příjemce
- Žadatel
- Připojení serveru
- Odesílatel klastru
- Příjemce klastru

Další informace o datech monitorování viz [Zobrazení dat monitorování fronty a kanálu](#).

MRDATA (uživatelská data ukončení opakování zprávy)

Jeho atribut určuje data předaná uživatelské proceduře pro opakování zpráv kanálu při volání.

Tento atribut je platný pro typy kanálů:

- Příjemce
- Žadatel
- Příjemce klastru

MREXIT (název uživatelské procedury opakování zprávy)

Tento atribut uvádí název uživatelského programu, který se má spustit uživatelskou procedurou pro opakování zpráv.

Ponechte prázdné, pokud není v platnosti žádný uživatelský program opakování zprávy.

Formát a maximální délka názvu závisí na platformě, jako pro [“RCVEXIT \(Název uživatelské procedury pro příjem\)”](#) na stránce 116. Můžete však zadat pouze jednu uživatelskou proceduru opakování zprávy.

Tento atribut je platný pro typy kanálů:

- Příjemce

- Žadatel
- Příjemce klastru

MRRTY (Počet opakování zpráv)

Tento atribut určuje, kolikrát se kanál pokusí zprávu znovu doručit.

Tento atribut řídí akci agenta MCA pouze v případě, že je název uživatelské procedury opakování zprávy prázdný. Není-li název uživatelské procedury prázdný, hodnota MRRTY je předána uživatelské proceduře, ale počet provedených pokusů (pokud existují) je řízen uživatelskou procedurou, a ne tímto atributem.

Hodnota musí být v rozsahu 0-999 999 999 999. Hodnota nula znamená, že se neprovedou žádné další pokusy. Výchozí hodnota je 10.

Tento atribut je platný pro typy kanálů:

- Příjemce
- Žadatel
- Příjemce klastru

MRTMR (Interval opakování zpráv)

Tento atribut určuje minimální časový interval v milisekundách, který musí uplynout, aby mohl kanál zopakovat operaci MQPUT.

Tento atribut řídí akci agenta MCA pouze v případě, že je název uživatelské procedury opakování zprávy prázdný. Není-li název uživatelské procedury prázdný, hodnota MRTMR je předána uživatelské proceduře pro použití uživatelskou procedurou, ale interval opakování je řízen uživatelskou procedurou a ne tímto atributem.

Hodnota musí být v rozsahu 0-999 999 999 999. Hodnota nula znamená, že opakování se provede co nejdříve (pokud je hodnota MRRTY větší než nula). Výchozí hodnotou je hodnota 1000.

Tento atribut je platný pro následující typy kanálů:

- Příjemce
- Žadatel
- Příjemce klastru

MSGDATA (Uživatelská data uživatelské procedury zprávy)

Tento atribut určuje uživatelská data, která se předávají uživatelským procedur zpráv kanálu.

Můžete spustit posloupnost uživatelských procedur zpráv. Omezení délky uživatelských dat a příklad, jak uvést MSGDATA pro více než jednu uživatelskou proceduru, jsou zobrazena pro RCVDATA. Viz [“RCVDATA \(Přijmout uživatelská data uživatelské procedury\)”](#) na stránce 116.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Příjemce
- Žadatel
- Odesílatel klastru
- Příjemce klastru

MSGEXIT (Název uživatelské procedury zprávy)

Tento atribut určuje název programu uživatelské procedury, který má být spuštěn uživatelskou procedurou pro zprávy kanálu.

Tento atribut může být seznam názvů programů, které mají být spuštěny v posloupnosti. Ponechte prázdné, pokud není v platnosti žádná uživatelská procedura pro zprávy kanálu.

Formát a maximální délka tohoto atributu závisí na platformě, jako pro [“RCVEXIT \(Název uživatelské procedury pro příjem\)”](#) na stránce 116.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Příjemce
- Žadatel
- Odesílatel klastru
- Příjemce klastru

Atributy kanálu pro klíčová slova MQSC (N-R)

Abecední seznam atributů kanálu pro klíčová slova MQSC začínající písmeny N až R.

NETPRTY (priorita síťového připojení)

Atribut kanálu NETPRTY určuje prioritu kanálu CLUSRCVR . Hodnota musí být v rozsahu 0-9, kde 0 je nejnižší priorita a 9 je nejvyšší.

Pomocí atributu NETPRTY nastavte jednu síť jako primární síť a jinou síť jako záložní síť. Je-li k dispozici sada kanálů se stejným hodnocením, klastrování zvolí cestu s nejvyšší prioritou, je-li k dispozici více cest.

Typickým příkladem použití atributu kanálu NETPRTY je rozlišení mezi sítěmi, které mají různé náklady nebo rychlosti, a připojení stejných cílů.

Poznámka: Určete tento atribut v přijímacím kanálu klastru v cílovém správci front. Jakékoli vyvážení, které zadáte v odpovídajícím odesílacím kanálu klastru, bude pravděpodobně ignorováno. Viz [Kanály klastru](#).

NPMSPEED (Rychlost přechodných zpráv)

Tento atribut určuje rychlost odesílání dočasných zpráv.

Možné hodnoty jsou:

NORMÁLNÍ

Přechodné zprávy kanálu jsou přenášeny v rámci transakcí.

FAST

Přechodné zprávy kanálu nejsou přenášeny v rámci transakcí.

Předvolba je FAST. Výhodou je, že přechodné zprávy budou k dispozici pro rychlejší načtení. Nevýhodou je, že vzhledem k tomu, že nejsou součástí transakce, mohou být zprávy ztraceny v případě selhání přenosu nebo v případě, že se kanál zastaví při přenosu zpráv. Viz [Bezpečnost zpráv](#).

Notes:

1. Pokud aktivní protokoly pro zotavení produktu IBM MQ for z/OS přepínají a archivují častěji, než se očekávalo, vzhledem k tomu, že zprávy odesílané prostřednictvím kanálu jsou dočasné, nastavení parametru NPMSPEED (FAST) na odesílající i přijímající straně kanálu může minimalizovat SYSTEM.CHANNEL.SYNCQ .
2. Pokud vidíte vysoké využití procesoru související s aktualizacemi systému SYSTEM.CHANNEL.SYNCQ, nastavení NPMSPEED (FAST) může výrazně snížit využití procesoru.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server

- Příjemce
- Žadatel
- Odesílatel klastru
- Příjemce klastru

PASSWORD (Heslo)

Tento atribut určuje heslo, které může agent MCA použít při pokusu o zahájení zabezpečené relace LU 6.2 se vzdáleným agentem MCA.

Můžete zadat heslo o maximální délce 12 znaků, i když se použije pouze prvních 10 znaků.

z/OS V systému IBM MQ for z/OS je tento atribut platný pouze pro kanály připojení klienta.

Multi Na jiných platformách je tento atribut platný pro typy kanálů:

- Odesílatel
- Server
- Žadatel
- Připojení klienta
- Odesílatel klastru

PORT (číslo portu)

Uveďte číslo portu, které se používá pro připojení klienta AMQP.

Výchozí port pro připojení AMQP 1.0 je 5672. Pokud již port 5672 používáte, zadejte jiný port.

PUTAUT (Oprávnění PUT)

Tento atribut určuje typ zpracování zabezpečení, které má provádět agent MCA.

Tento atribut použijte k výběru typu zpracování zabezpečení, které má agent MCA provést při provádění:

- příkaz MQPUT do cílové fronty (pro kanály zpráv), nebo
- Volání MQI (pro kanály MQI).

z/OS V systému z/OS závisí ID uživatelů, která jsou kontrolována, a počet ID uživatelů, kteří jsou kontrolováni, na nastavení profilu MQADMIN RACF class hlq.RESLEVEL. V závislosti na úrovni přístupu, kterou má ID uživatele inicializátoru kanálu k hodnotě hlq.RESLEVEL, se kontroluje nula, jedno nebo dvě ID uživatele. Chcete-li zjistit, kolik ID uživatelů je zkontrolováno, prohlédněte si téma [RESLEVEL a připojení inicializátoru kanálu](#). Další informace o tom, která ID uživatelů jsou kontrolována, naleznete v tématu [ID uživatelů používaná inicializátorem kanálu](#).

Můžete si vybrat jednu z následujících možností:

Zabezpečení procesu, nazývané také výchozí oprávnění (DEF)

Použije se výchozí ID uživatele.

Multi Na jiných platformách než z/OS je ID uživatele použité ke kontrole otevřeného oprávnění ve frontě ID uživatele procesu nebo uživatele, který spustil agenta MCA na přijímacím konci kanálu zpráv.

z/OS V systému z/OS lze použít ID uživatele přijaté ze sítě i ID uživatele odvozené od [MCAUSER](#) v závislosti na počtu ID uživatelů, která se mají zkontrolovat.

Fronty jsou otevřeny s tímto ID uživatele a volbou otevření MQOO_SET_ALL_CONTEXT.

Zabezpečení kontextu (CTX)

ID uživatele z informací o kontextu přidružených ke zprávě se použije jako alternativní ID uživatele.

Soubor *UserIdentifier* v deskriptoru zprávy se přesune do pole *AlternateUserId* v deskriptoru objektu. Fronta je otevřena s volbami otevření MQOOO_SET_ALL_CONTEXT a MQOO_ALTERNATE_USER_AUTHORITY.

Multi Na jiných platformách než z/OS je ID uživatele použité ke kontrole otevřeného oprávnění ve frontě pro MQOOO_SET_ALL_CONTEXT a MQOO_ALTERNATE_USER_AUTHORITY použito pro proces nebo uživatele, který spustil agenta MCA na přijímacím konci kanálu zpráv. ID uživatele použité ke kontrole otevřeného oprávnění ve frontě pro MQOO_OUTPUT je *UserIdentifier* v deskriptoru zprávy.

z/OS V systému z/OS lze použít ID uživatele přijaté ze sítě nebo odvozené od MCAUSER a také ID uživatele z informací o kontextu v deskriptoru zprávy v závislosti na počtu ID uživatelů, která mají být zkontrolována.

Zabezpečení kontextu (CTX) není podporováno na kanálech připojení serveru.

z/OS Pouze zabezpečení agenta kanálu zpráv (ONLYMCA)

Použije se ID uživatele odvozené od MCAUSER.

Fronty se otevírají s volbou otevření MQOOO_SET_ALL_CONTEXT.

Tato hodnota platí pouze pro z/OS.

z/OS Zabezpečení agenta alternativního kanálu zpráv (ALTMCA)

Lze použít ID uživatele z informací o kontextu (pole *UserIdentifier*) v deskriptoru zprávy, stejně jako ID uživatele odvozené od MCAUSER, v závislosti na počtu ID uživatelů, která se mají zkontrolovat.

Tato hodnota platí pouze pro z/OS.

Další podrobnosti o polích kontextu a otevřených volbách naleznete v části Řízení informací o kontextu.

Více informací o zabezpečení naleznete zde:

- [Zabezpečení](#)
- **ALW** [Nastavení zabezpečení na systému AIX, Linux, and Windows](#)
- **IBM i** [Nastavení zabezpečení na systému IBM i](#)
- **z/OS** [Nastavení zabezpečení na systému z/OS](#)

Tento atribut je platný pro typy kanálů:

- Příjemce
- Žadatel
- **z/OS** Připojení k serveru (pouze z/OS)
- Příjemce klastru

QMNAME (název správce front)

jeho atribut určuje název správce front nebo skupiny správců front, ke kterému může aplikace IBM MQ MQI client požadovat připojení.

Tento atribut je platný pro typy kanálů:

- Připojení klienta

QSGDISP (odebrání)

z/OS

Tento atribut určuje dispozici kanálu ve skupině sdílení front. Platí pouze na systému z/OS.

Hodnoty jsou:

QMGR

Kanál je definován v sadě stránek správce front, který provádí příkaz. Tato hodnota je výchozí.

SKUPINA

Kanál je definován ve sdíleném úložišti. Tato hodnota je povolena pouze v případě, že existuje sdílené prostředí správce front. Když je kanál definován s QSGDISP (GROUP), příkaz DEFINE CHANNEL (name) NOREPLACE QSGDISP (COPY) je generován automaticky a odeslán všem aktivním správcům front, aby vytvořili lokální kopie na sadě stránek 0. Pro správce front, kteří nejsou aktivní nebo se ke skupině sdílení front připojí později, je příkaz generován při spuštění správce front.

COPY

Kanál je definován v sadě stránek správce front, který příkaz spouští, a kopíruje jeho definici z kanálu QSGDISP (GROUP) se stejným názvem. Tato hodnota je povolena pouze v případě, že existuje sdílené prostředí správce front.

Tento atribut je platný pro všechny typy kanálů.

RCVDATA (Přijmout uživatelská data uživatelské procedury)

Tento atribut určuje uživatelská data, která jsou předána uživatelské proceduře pro příjem.

Můžete spustit posloupnost uživatelských procedur příjmu. Řetězec uživatelských dat pro řadu uživatelských procedur musí být oddělen čárkou, mezerami nebo obojím. Příklad:

```
RCVDATA(exit1_data exit2_data)
MSGDATA(exit1_data,exit2_data)
SENDDATA(exit1_data, exit2_data)
```

ALW V systémech IBM MQ for UNIX a Windows je délka řetězce názvů uživatelských procedur a řetězců uživatelských dat omezena na 500 znaků.

IBM i V produktu IBM MQ for IBM i můžete zadat až 10 názvů ukončení a délka uživatelských dat pro každý z nich je omezena na 32 znaků.

z/OS V produktu IBM MQ for z/OS můžete zadat až osm řetězců uživatelských dat o délce 32 znaků.

Tento atribut je platný pro všechny typy kanálů.

RCVEXIT (Název uživatelské procedury pro příjem)

Tento atribut určuje název uživatelského programu, který má být spuštěn uživatelskou procedurou pro příjem kanálu.

Tento atribut může být seznam názvů programů, které mají být spuštěny v posloupnosti. Ponechte toto pole prázdné, pokud není v platnosti žádná uživatelská procedura pro příjem kanálu.

Formát a maximální délka tohoto atributu závisí na platformě:

- z/OS** V systému z/OS se jedná o název zaváděcího modulu, maximální délka je 8 znaků, s výjimkou kanálů připojení klienta, kde maximální délka je 128 znaků.
- IBM i** Na systému IBM i je ve tvaru:

```
libname/progname
```

je-li uvedeno v CL příkazech.

Je-li uveden v příkazu IBM MQ (MQSC), má tvar:

```
progrname libname
```

kde *progrname* zabírá prvních 10 znaků a *libname* dalších 10 znaků (v případě potřeby obě prázdné znaky napravo). Maximální délka řetězce je 20 znaků.

- ▶ Linux ▶ AIX Na systému AIX and Linux je ve tvaru:

```
libraryname(functionname)
```

Maximální délka řetězce je 40 znaků.

- ▶ Windows Na systému Windows je ve tvaru:

```
dllname(functionname)
```

kde *dllname* je uvedeno bez přípony .DLL. Maximální délka řetězce je 40 znaků.

- ▶ z/OS Během automatické definice kanálu odesilatele klastru v systému z/OS jsou názvy uživatelských procedur kanálu převedeny na formát z/OS. Chcete-li řídit způsob převodu názvů uživatelských procedur, můžete napsat uživatelskou proceduru automatické definice kanálu. Další informace naleznete v tématu [Uživatelský program automatické definice kanálu](#).

Můžete uvést seznam názvů programů pro příjem, odeslání nebo ukončení zpráv. Názvy musí být odděleny čárkou, mezerou nebo obojím. Příklad:

```
RCVEXIT(exit1 exit2)  
MSGEXIT(exit1,exit2)  
SENDEXIT(exit1, exit2)
```

Celková délka řetězce názvů ukončení a řetězců uživatelských dat pro konkrétní typ ukončení je omezena na 500 znaků.

- ▶ IBM i V systému IBM MQ for IBM i můžete vypsát až 10 názvů ukončení.
- ▶ z/OS V systému IBM MQ for z/OS můžete vypsát až osm názvů ukončení.

Tento atribut je platný pro všechny typy kanálů.

Atributy kanálu pro klíčová slova MQSC (S)

Abecední seznam atributů kanálu pro klíčová slova MQSC začínající písmenem S.

SCYDATA (Uživatelská data uživatelské procedury zabezpečení)

Tento atribut určuje uživatelská data, která jsou předána uživatelské proceduře pro zabezpečení zprávy.

Maximální délka je 32 znaků.

Tento atribut je platný pro všechny typy kanálů.

SCYEXIT (Název uživatelské procedury zabezpečení)

Tento atribut určuje název uživatelského programu, který má být spuštěn uživatelskou procedurou pro zabezpečení zprávy kanálu.

Ponechte prázdné, pokud není v platnosti žádná uživatelská procedura zabezpečení kanálu.

Formát a maximální délka názvu závisí na platformě, jako pro [RCVEXIT](#). Můžete však zadat pouze jednu uživatelskou proceduru zabezpečení.

Další informace o uživatelských procedurách zabezpečení naleznete v tématu [Programy uživatelských procedur zabezpečení kanálu](#).

Tento atribut je platný pro všechny typy kanálů.

SENDDATA (Odeslat uživatelská data uživatelské procedury)

Tento atribut uvádí uživatelská data, která jsou předána uživatelské proceduře pro odeslání.

Můžete spustit posloupnost uživatelských procedur odeslání. Omezení délky uživatelských dat a příklad, jak uvést SENDDATA pro více než jednu uživatelskou proceduru, jsou uvedeny pro RCVDATA. Viz [RCVDATA](#).

Tento atribut je platný pro všechny typy kanálů.

SENDEXIT (Název uživatelské procedury odeslání)

Tento atribut určuje název uživatelského programu, který má být spuštěn uživatelskou procedurou pro odeslání kanálu.

Tento atribut může být seznam názvů programů, které se mají spustit v posloupnosti. Ponechte prázdné, pokud není v platnosti žádná uživatelská procedura odeslání kanálu.

Formát a maximální délka tohoto atributu závisí na platformě, jako pro [RCVEXIT](#).

Tento atribut je platný pro všechny typy kanálů.

SEQWRAP (zalomení pořadového čísla)

Tento atribut uvádí nejvyšší číslo, které pořadové číslo zprávy dosáhne před restartováním v 1.

Hodnota čísla musí být dostatečně vysoká, aby se zabránilo opětovnému zadání čísla, zatímco je stále používáno dřívější zprávou. Oba konce kanálu musí mít při spuštění kanálu stejnou hodnotu obtékání pořadového čísla; jinak dojde k chybě.

Hodnotu lze nastavit od 100 do 999 999 999 999.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Příjemce
- Žadatel
- Odesílatel klastru
- Příjemce klastru

SHORTRTY (počet krátkých opakování)

Tento atribut určuje maximální počet pokusů kanálu o přidělení relace svému partnerovi.

Atribut SHORTRTY lze nastavit od nuly do 999 999 999 999.

Pokud bylo v rámci kanálu definováno více adres IP a je nutné znovu navázat spojení, produkt IBM MQ vyhodnotí definici kanálu a pokusí se připojit ke každé adrese IP v pořadí, v jakém je definována, dokud nebude vytvořeno úspěšné připojení nebo dokud nebudou provedeny všechny adresy.

V tomto případě se parametr SHORTRTY vztahuje k celkovému počtu pokusů o opětovné připojení kanálu, nikoli k jednotlivým adresám IP.

Pokud se počáteční pokus o alokaci nezdaří, sníží se *počet krátkých opakování* a kanál se mezi každým pokusem zopakuje se zbývajícím počtem pokusů s intervalem definovaným v atributu **short retry interval**. Pokud se stále nezdaří, zopakuje *počet dlouhých opakování* s intervalem *intervalu dlouhých opakování* mezi jednotlivými pokusy. Pokud je stále neúspěšný, kanál se zavře.

z/OS V systému z/OSnemůže kanál zadat opakování, pokud byl překročen maximální počet kanálů (**MAXCHL**).

Multi V systému Multiplatforms musí být spuštěn inicializátor kanálu, aby bylo možné pokus zopakovat. Inicializátor kanálu musí monitorovat inicializační frontu určenou v definici přenosové fronty, kterou kanál používá.

Pokud je inicializátor kanálu (na z/OS) nebo je kanál (v systému Multiplatforms) zastaven při opakovaném pokusu kanálu, *počet krátkých opakování* a *počet dlouhých opakování* jsou resetovány při restartování inicializátoru kanálu nebo kanálu nebo při úspěšném vložení zprávy do kanálu odesílatele. Avšak, pokud inicializátor kanálu (na z/OS) nebo správce front (na platformě Multiplatforms) je vypnutý a restartovaný, *počet krátkých opakování* a *počet dlouhých opakování* nejsou resetovány. Kanál zachová hodnoty počtu opakování, které měl před restartováním správce front nebo před vložением zprávy.

Multi V systému Multiplatforms:

1. Když kanál přejde ze stavu RETRYING do stavu RUNNING, *počet krátkých opakování* a *počet dlouhých opakování* nejsou okamžitě resetovány. Jsou resetovány pouze v případě, že první zpráva úspěšně protéká kanálem po přechodu kanálu do stavu SPUŠTĚNO, tj. když lokální kanál potvrdí počet zpráv odeslaných na druhý konec.
2. *Počet krátkých opakování* a *počet dlouhých opakování* jsou resetovány při restartování kanálu.

Tento atribut je platný pro následující typy kanálů:

- Odesílatel
- Server
- Odesílatel klastru
- Příjemce klastru

SHORTTMR (Interval krátkých opakování)

Tento atribut určuje přibližný interval v sekundách, po který má kanál čekat před opětovným pokusem o navázání připojení během režimu krátkých opakování.

Interval mezi opakovanými pokusy může být prodloužen, pokud má kanál čekat na aktivaci.

Tento atribut lze nastavit od nuly do 999 999.

Pokud bylo v rámci kanálu definováno více adres IP a je nutné znovu navázat spojení, produkt IBM MQ vyhodnotí definici kanálu a pokusí se připojit ke každé adrese IP v pořadí, v jakém je definována, dokud nebude vytvořeno úspěšné připojení nebo dokud nebudou provedeny všechny adresy.

V tomto případě se parametr SHORTTMR vztahuje k době, po kterou celkový kanál čeká na restartování procesu připojení, nikoli k jednotlivým adresám IP.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Odesílatel klastru
- Příjemce klastru

SPLPROT (Ochrana zásad zabezpečení)

z/OS

Tento atribut uvádí, jak by měl agent kanálu zpráv server-server pracovat s ochranou zpráv, když je AMS aktivní a existuje použitelná zásada.

Tento atribut lze nastavit na:

PASSTHRU

Na kanálech odesílatele, serveru, příjemce a žadatele

REMOVE

Na kanálech odesílatele a serveru

ASPOLICY

Na přijímacích a žadatelových kanálech

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Příjemce
- Žadatel

SSLCAUTH (ověření klienta SSL)

Atribut **SSLCAUTH** uvádí, zda kanál potřebuje přijmout a ověřit certifikát TLS od klienta TLS.

SSLCAUTH je volitelný atribut. Možné hodnoty tohoto atributu jsou:

Volitelný

Pokud klient TLS typu peer odešle certifikát, je certifikát zpracován jako normální, ale ověření neselže, pokud není odeslán žádný certifikát.

POVINNÉ

Pokud klient TLS neodešle certifikát, ověření se nezdaří.

Výchozí hodnota je REQUIRED.

Můžete uvést hodnotu pro **SSLCAUTH** v definici kanálu jiného než TLS. To znamená, že v definici kanálu chybí atribut [SSLCIPH](#) nebo je prázdný.

Další informace o SSLCAUTH viz [DEFINE CHANNEL \(MQTT\)](#) a [Zabezpečení](#).

Atribut **SSLCAUTH** je platný pro všechny typy kanálů, které mohou přijímat tok inicializace kanálu, s výjimkou odesílacích kanálů. Tento atribut je platný pro typy kanálů:

- Server
- Příjemce
- Žadatel
- Připojení serveru
- Příjemce klastru

SSLCIPH (specifikace šifrování SSL)



Atribut **SSLCIPH** určuje alias nebo jednu pojmenovanou položku CipherSpec pro připojení TLS.

Každá definice kanálu IBM MQ obsahuje atribut **SSLCIPH**. Hodnota je řetězec s maximální délkou 32 znaků.

Atribut **SSLCIPH** je platný pouze pro kanály s typem přenosu (**TRPTYPE**) TCP. Pokud **TRPTYPE** není TCP, data se ignorují a nevydává se žádná chybová zpráva.

Notes:

- Atribut **SSLCIPH** může obsahovat prázdnou hodnotu, což znamená, že nepoužíváte TLS. Pokud má jeden konec kanálu prázdný atribut **SSLCIPH**, druhý konec kanálu musí mít také prázdný atribut SSLCIPH.

  Je-li povolena volba [SecureCommsOnly](#), komunikace v prostém textu není podporována a kanál se nespustí.

- Případně, pokud **SSLCIPH** obsahuje neprázdnou hodnotu, hodnota může být buď alias, nebo pojmenovaná CipherSpec. Kanály vyjednávají nejsilnější CipherSpec podporovanou oběma konci kanálu.
- Plně spravovaný klient .NET může uvést speciální hodnotu *NEGOTIATION. Tato volba umožňuje kanálu vybrat nejnovější verzi protokolu podporovanou rámcem .NET a vyjednat CipherSpec, kterou server podporuje.

Atribut **SSLCIPH** je platný pouze pro kanály s typem přenosu (**TRPTYPE**) TCP. Pokud **TRPTYPE** není TCP, data se ignorují a nevydává se žádná chybová zpráva.

Další informace o produktu **SSLCIPH** naleznete v části [DEFINE CHANNEL](#) a [Určení CipherSpecs](#).

SSLPEER (rovnocenný partner SSL)

Atribut **SSLPEER** se používá ke kontrole rozlišujícího názvu (DN) certifikátu ze správce front typu peer nebo klienta na druhém konci kanálu IBM MQ.

Poznámka: Alternativním způsobem, jak omezit připojení do kanálů porovnáním s rozlišujícím názvem subjektu TLS, je použít záznamy ověřování kanálu. U záznamů ověřování kanálu lze pro stejný kanál použít různé vzory rozlišujícího názvu subjektu TLS. Pokud se pro použití na stejný kanál používá **SSLPEER** na kanálu i záznam ověření kanálu, přichází certifikát se musí shodovat s oběma vzory, aby se mohl připojit.

Pokud DN přijaté od partnera neodpovídá hodnotě **SSLPEER**, kanál se nespustí.

SSLPEER je volitelný atribut. Není-li hodnota uvedena, DN partnera se při spuštění kanálu nekontroluje.

Maximální délka atributu **SSLPEER** závisí na platformě:

- **z/OS** V systému z/OS je maximální délka atributu 256 bajtů.
- **Multi** Na všech ostatních platformách je to 1024 bajtů.

Záznamy ověřování kanálu poskytují větší flexibilitu při používání produktu **SSLPEER** a podporují maximální délku 1024 bajtů na všech platformách.

Kontrola hodnot atributu **SSLPEER** také závisí na platformě:

- **z/OS** V systému z/OS se hodnoty atributů, které se používají, nekontrolují. Zadáte-li nesprávné hodnoty, kanál při spuštění selže a chybové zprávy se zapíší do protokolu chyb na obou koncích kanálu. Na obou koncích kanálu je také generována chybová událost SSL kanálu.
- **Multi** Na jiných platformách než z/OS, které podporují **SSLPEER**, je platnost řetězce kontrolována při prvním zadání.

Můžete zadat hodnotu parametru **SSLPEER** v jiné definici kanálu než TLS, v níž chybí atribut **SSLCIPH** nebo je prázdný. Pomocí této volby můžete dočasně zakázat protokol TLS pro ladění bez nutnosti vymazat a později znovu zadat parametry protokolu TLS.

Atribut **SSLPEER** je platný pro všechny typy kanálů.

Další informace o použití **SSLPEER** viz [SET CHLAUTH](#), [Zabezpečení Záznamy ověření kanálu](#).

STATCHL (statistika kanálů)

Tento atribut řídí shromažďování statistických dat pro kanály.

Možné hodnoty jsou:

QMGR

Shromažďování statistických dat pro tento kanál je založeno na nastavení atributu STATCHL správce front. Tato hodnota je výchozí hodnota.

VYP

Shromažďování statistických dat pro tento kanál je zakázáno.

NÍZKÁ

Shromažďování statistických dat pro tento kanál je povoleno s nízkým poměrem shromažďování dat.


STŘEDNÍ

Shromažďování statistických dat pro tento kanál je povoleno se středním poměrem shromažďování dat.

VYSOKÁ

Shromažďování statistických dat pro tento kanál je povoleno s vysokým poměrem shromažďování dat.

Další informace o statistice kanálu viz [Odkaz na monitorování](#).

 Na systémech z/OS povolení tohoto parametru jednoduše zapne shromažďování statistických dat bez ohledu na vybranou hodnotu. Zadáním LOW, MEDIUM nebo HIGH nezpůsobíte ve výsledcích žádný změnu. Tento parametr musí být povolen, aby bylo možné shromažďovat účtovací záznamy kanálu.

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Příjemce
- Žadatel
- Odesílatel klastru
- Příjemce klastru

Atributy kanálu pro klíčová slova MQSC (T-Z)

Abecední seznam atributů kanálu pro klíčová slova MQSC začínající písmeny T až Z.

TPNAME (název transakčního programu LU 6.2)

Tento atribut je určen pro použití s připojeními LU 6.2. Jedná se o název nebo generický název transakčního programu (MCA), který má být spuštěn na vzdáleném konci propojení.

Při použití informací o straně pro komunikace SNA je název transakčního programu definován v objektu CPI-C Communications Side Object nebo v informacích o straně APPC a tento atribut musí být ponechán prázdný. Jinak je toto jméno vyžadováno kanály odesílatele a kanály žadatele.

Název může mít délku až 64 znaků.

Název musí být nastaven na název transakčního programu SNA, pokud CONNAME neobsahuje název postranního objektu, v takovém případě musí být nastaven na mezery. Skutečný název je místo toho převzat z objektu CPI-C Communications Side Object nebo z datové sady informací na straně APPC.

Tyto informace jsou nastaveny různými způsoby na různých platformách. Další informace o nastavení komunikace pro vaši platformu naleznete v tématu [Konfigurace distribuovaných front](#).

Tento atribut je platný pro typy kanálů:

- Odesílatel
- Server
- Žadatel
- Připojení klienta
- Odesílatel klastru
- Příjemce klastru

TPROOT (kořen tématu)

Tento atribut určuje kořen tématu pro kanál AMQP.

Pomocí atributu TPROOT můžete určit kořen tématu pro kanál AMQP. Použití tohoto atributu zajišťuje, že aplikace MQ Light při implementaci do správce front nepublikuje zprávy do oblastí stromu témat, které jsou používány jinými aplikacemi, ani se k těmto zprávám nepřihlašuje.

Výchozí hodnota pro TPROOT je SYSTEM.BASE.TOPIC. Při použití této hodnoty nemá řetězec tématu, který klient AMQP používá k publikování nebo odběru, žádnou předponu a klient si může vyměňovat zprávy s jinými aplikacemi publikování/odběru produktu MQ. Chcete-li nechat klienty AMQP publikovat a odebírat pod předponou tématu, nejprve vytvořte objekt tématu MQ s řetězcem tématu nastaveným na požadovanou předponu a poté změňte hodnotu atributu TPROOT kanálu AMQP na název vámi vytvořeného objektu tématu MQ. Následující příklad ukazuje kořen tématu, který je nastaven na APPGROUP1.BASE.TOPIC pro kanál AMQP MYAMQP:

```
DEFINE CHANNEL(MYAMQP) CHLTYPE(AMQP) TPROOT(APPGROUP1.BASE.TOPIC) PORT(5673)
```

Poznámka: Pokud se změní hodnota atributu TPROOT nebo řetězec tématu, který ji tvoří, existující témata AMQP a jejich zprávy mohou být osiřelé.

TRPTYPE (Typ přenosu)

Tento atribut určuje typ přenosu, který se má použít.

Možné hodnoty jsou:

<i>Tabulka 58. Volby typu přenosu</i>	
Hodnota	Typ přenosu
LU62	LU 6.2
TCP	TCP/IP
NETBIOS	NetBIOS “1” na stránce 123
SPX	SPX “1” na stránce 123

Notes:

1. Pro použití na Windows. Lze také použít v systému z/OS pro definování kanálů připojení klienta pro použití v systému Windows.

Tento atribut je platný pro všechny typy kanálů, ale je ignorován odpovědnými agenty kanálů zpráv.

USECLTID (Použit ID klienta)

Uveďte, zda se ID klienta používá pro připojení ke kanálu AMQP. Nastavte na hodnotu Yes nebo No.

USEDLQ (Použit frontu nedoručených zpráv)

Tento atribut určuje, zda se použije fronta nedoručených zpráv (nebo nedoručená fronta zpráv), když kanály nemohou doručovat zprávy.

Možné hodnoty jsou:

NO

Zprávy, které nelze doručit prostřednictvím kanálu, jsou považovány za selhání. Kanál tyto zprávy buď vyřadí, nebo skončí v souladu s nastavením NPMSPEED.

YES (výchozí)

Pokud atribut DEADQ správce front poskytuje název fronty nedoručených zpráv, použije se, jinak je chování stejné jako pro NO.


USERID (ID uživatele)

Tento atribut určuje ID uživatele, které má agent MCA použít při pokusu o zahájení zabezpečené relace SNA se vzdáleným agentem MCA.

Můžete zadat identifikátor uživatele úlohy o délce 20 znaků.

Pokud jsou hesla na přijímacím konci uchovávána v šifrovaném formátu a software LU 6.2 používá jinou metodu šifrování, pokus o spuštění kanálu selže s neplatnými podrobnostmi zabezpečení. Tomuto selhání se můžete vyhnout úpravou přijímací konfigurace SNA na některou z následujících možností:

- Vypněte substituci hesla, nebo
- Definujte ID a heslo uživatele zabezpečení.

 V systému IBM MQ for z/OS je tento atribut platný pouze pro kanály připojení klienta.

 Na jiných platformách je tento atribut platný pro typy kanálů:

- Odesílatel
- Server
- Žadatel
- Připojení klienta
- Odesílatel klastru

XMITQ (název přenosové fronty)

Tento atribut uvádí název přenosové fronty, ze které se načítají zprávy.

Zadejte název přenosové fronty, která má být přidružena k tomuto odesílacímu kanálu nebo kanálu serveru, který odpovídá správci front na vzdálené straně kanálu. Přenosové frontě můžete dát stejný název jako správci front na vzdáleném konci.



Tento atribut je povinný pro kanály typu odesílatel nebo server a není platný pro jiné typy kanálů.

Příkazy a atributy klastru IBM MQ

Existují příkazy klastru MQSC a PCF, které lze použít k aktualizaci nebo resetování klastru nebo k zobrazení, obnovení či pozastavení správce front klastru. Kromě toho mají příkazy MQSC a PCF, které definují kanály, fronty a správce front, atributy, které se vztahují na klastry. Některé z těchto atributů jsou používány algoritmem správy pracovní zátěže klastru.

Příkazy MQSC

Příkazy MQSC jsou zobrazeny tak, jak by je zadal administrátor systému na příkazové konzole. Nezapomeňte, že tímto způsobem nemusíte zadávat příkazy. Existuje řada dalších metod, v závislosti na vaší platformě; například:

-  V systému IBM MQ for IBM i použijte příkazy MQSC interaktivně z volby 26 souboru **WRKMQM**. Můžete také použít CL příkazy nebo uložit příkazy MQSC do souboru a použít CL příkaz **STRMQMMQSC**.
-  V systému z/OS můžete použít funkci COMMAND obslužného programu **CSQUTIL**, operace a ovládací panely nebo konzolu z/OS.
- Na všech ostatních platformách můžete příkazy uložit do souboru a použít funkci **runmqsc**.

V příkazu MQSC může být název klastru zadaný pomocí atributu CLUSTER dlouhý až 48 znaků.

Seznam názvů klastrů, který je uveden pomocí atributu CLUSNL, může obsahovat až 256 názvů. Chcete-li vytvořit seznam názvů klastru, použijte příkaz **DEFINE NAMELIST**.

IBM MQ Explorer

Grafické uživatelské rozhraní produktu IBM MQ Explorer může provádět administraci klastru se správcí front úložiště v systému IBM WebSphere MQ for z/OS 6.0 nebo novějším. Nemusíte nominovat další úložiště na samostatném systému. Pro starší verze produktu IBM MQ for z/OS nemůže produkt IBM MQ Explorer provádět administraci klastru se správcí front úložiště. Proto musíte navrhnout další úložiště v systému, které může produkt IBM MQ Explorer spravovat.

V systémech IBM MQ for Windows a IBM MQ for Linux můžete také použít produkt IBM MQ Explorer pro práci s klastry. Můžete také použít samostatného klienta IBM MQ Explorer .

Pomocí konzoly IBM MQ Explorer můžete zobrazit fronty klastru a dotazovat se na stav odesílacích kanálů klastru a přijímacích kanálů klastru. Produkt IBM MQ Explorer obsahuje dva průvodce, které můžete použít k provedení následujících úloh:

- Vytvořit klastr
- Připojit nezávislého správce front ke klastru

Ekvivalenty PCF příkazů MQSC specificky pro práci s klastry

Příkaz MQSC	Ekvivalentní příkaz PCF
DISPLAY CLUSQMGR	MQCMD_INQUIRE_CLUSTER_Q_MGR
REFRESH CLUSTER	MQCMD_REFRESH_CLUSTER
RESET CLUSTER	MQCMD_RESET_CLUSTER
RESUME QMGR	MQCMD_RESUME_Q_MGR_CLUSTER
SUSPEND QMGR	MQCMD_SUSPEND_Q_MGR_CLUSTER

Související informace

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

Atributy klastru dostupné v příkazech definice kanálu

Atributy klastru, které lze zadat v příkazech definice kanálu.

Příkazy DEFINE CHANNEL, ALTER CHANNEL a DISPLAY CHANNEL mají dva specifické parametry CHLTYPE pro klastry: CLUSRCVR a CLUSSDR. Chcete-li definovat přijímací kanál klastru, použijte příkaz DEFINE CHANNEL s uvedením CHLTYPE (CLUSRCVR). Mnoho atributů v definici přijímacího kanálu klastru je stejných jako atributy v definici příjemce nebo odesílacího kanálu. Chcete-li definovat odesílací kanál klastru, použijte příkaz DEFINE CHANNEL se zadáním parametru CHLTYPE (CLUSSDR) a mnoha stejných atributů, které používáte k definování odesílacího kanálu.

Při definování odesílacího kanálu klastru již není nutné zadávat název správce front úplného úložiště. Znáte-li konvenci pojmenování používanou pro kanály v klastru, můžete vytvořit definici CLUSSDR pomocí konstrukce +QMNAME+. Konstrukce +QMNAME+ není v systému z/OS podporována. Po připojení produkt IBM MQ změní název kanálu a nahradí správný název správce front úplného úložiště názvem +QMNAME+. Výsledný název kanálu je zkrácen na 20 znaků.

Další informace o konvencích pojmenování naleznete v tématu Konvence pojmenování klastru.

Tato technika funguje pouze v případě, že vaše konvence pojmenování kanálů obsahuje název správce front. Definujete například správce front úplného úložiště s názvem QM1 v klastru s názvem CLUSTER1 s přijímacím kanálem klastru s názvem CLUSTER1.QM1.ALPHA. Každý jiný správce front může definovat odesílací kanál klastru pro tohoto správce front s použitím názvu kanálu CLUSTER1.+QMNAME+.ALPHA.

Pokud pro všechny kanály použijete stejnou konvenci pojmenování, mějte na paměti, že v daném okamžiku může existovat pouze jedna definice +QMNAME+.

Následující atributy v příkazech DEFINE CHANNEL a ALTER CHANNEL jsou specifické pro kanály klastru:

CLUSTER

Atribut CLUSTER určuje název klastru, ke kterému je tento kanál přidružen. Případně použijte atribut CLUSNL .

CLUSNL

Atribut CLUSNL uvádí seznam názvů klastrů.

NETPRTY

Pouze přijímače klastru.

Atribut NETPRTY určuje prioritu sítě pro kanál. NETPRTY pomáhá rutinám správy pracovní zátěže. Pokud existuje více než jedna možná trasa k místu určení, rutina správy pracovní zátěže vybere tu s nejvyšší prioritou.

CLWLPRTY

Parametr CLWLPRTY používá faktor priority pro kanály ve stejném místě určení pro účely správy pracovní zátěže. Tento parametr určuje prioritu kanálu pro účely distribuce pracovní zátěže klastru. Hodnota musí být v rozsahu od nuly do 9, kde nula je nejnižší priorita a 9 je nejvyšší.

CLWLRANK

Parametr CLWLRANK používá faktor hodnocení důležitosti pro kanál pro účely správy pracovní zátěže. Tento parametr určuje pořadí kanálu pro účely rozdělení pracovní zátěže klastru. Hodnota musí být v rozsahu od nuly do 9, kde nula je nejnižší ohodnocení a 9 je nejvyšší.

CLWLWGHT

Parametr CLWLWGHT používá faktor váhy pro kanál pro účely správy pracovní zátěže. CLWLWGHT váží kanál tak, aby bylo možné řídit proporce zpráv odesílaných tímto kanálem. Algoritmus pracovní zátěže klastru používá funkci CLWLWGHT k předpětí volby místa určení, aby bylo možné prostřednictvím konkrétního kanálu odeslat více zpráv. Standardně mají všechny atributy váhy kanálu stejnou výchozí hodnotu. Atribut váhy vám umožňuje přidělit kanálu na výkonném počítači se systémem UNIX větší váhu než jiný kanál na malém stolním počítači. Větší váha znamená, že algoritmus pracovní zátěže klastru vybírá počítač UNIX častěji než PC jako místo určení pro zprávy.

CONNAME

Hodnota CONNAME uvedená v definici přijímacího kanálu klastru se používá v celém klastru k identifikaci síťové adresy správce front. Dávejte pozor, abyste vybrali hodnotu pro parametr CONNAME , která se interpretuje v celém klastru IBM MQ . Nepoužívejte generický název. Nezapomeňte, že hodnota zadaná v přijímacím kanálu klastru má přednost před libovolnou hodnotou zadanou v odpovídajícím odesílacím kanálu klastru.

Tyto atributy příkazu DEFINE CHANNEL a příkazu ALTER CHANNEL se také vztahují na příkaz DISPLAY CHANNEL .

Poznámka: Automaticky definované odesílací kanály klastru přebírá své atributy z odpovídající definice přijímacího kanálu klastru v přijímajícím správci front. I v případě, že existuje ručně definovaný odesílací kanál klastru, jsou jeho atributy automaticky upraveny tak, aby se shodovaly s atributy v odpovídající definici příjemce klastru. Mějte na paměti, že můžete například definovat CLUSRCVR bez zadání čísla portu v parametru CONNAME , zatímco ručně definujete CLUSSDR , který uvádí číslo portu. Když automaticky definovaný CLUSSDR nahradí ručně definovaný port, číslo portu (převzato z CLUSRCVR) se stane nevyplněnou. Použije se výchozí číslo portu a kanál se nezdaří.

Poznámka: Příkaz DISPLAY CHANNEL nezobrazuje automaticky definované kanály. Pomocí příkazu DISPLAY CLUSQMgr však můžete zkontrolovat atributy automaticky definovaných odesílacích kanálů klastru.

Pomocí příkazu DISPLAY CHSTATUS můžete zobrazit stav kanálu odesílatele klastru nebo kanálu příjemce klastru. Tento příkaz uvádí stav jak ručně definovaných kanálů, tak automaticky definovaných kanálů.

Ekvivalentní PCF jsou MQCMD_CHANGE_CHANNEL, MQCMD_COPY_CHANNEL, MQCMD_CREATE_CHANNEL a MQCMD_INQUIRE_CHANNEL.

Vynechání hodnoty CONNAME v definici CLUSRCVR

V některých případech můžete vynechat hodnotu CONNAME v definici CLUSRCVR . Nesmíte vynechat hodnotu CONNAME na z/OS.

Multi

V Multiplatforms je parametr názvu připojení TCP/IP přijímacího kanálu klastru nepovinný. Pokud ponecháte název připojení prázdný, vygeneruje IBM MQ název připojení za vás a bude předpokládat výchozí port a bude používat aktuální adresu IP systému. Výchozí číslo portu můžete přepsat, ale i nadále se bude používat aktuální adresa IP systému. Pro každý název připojení ponechte název IP prázdný a zadejte číslo portu do závorek. Např.:

(1415)

Vygenerovaný řetězec **CONNAME** je vždy ve formátu desítkových čísel oddělených tečkami (IPv4) nebo v hexadecimálním formátu (IPv6) a nikoli ve tvaru alfanumerického názvu hostitele DNS.

Tento prostředek je užitečný, pokud máte počítače používající protokol DHCP (Dynamic Host Configuration Protocol). Pokud nezádáte hodnotu pro CONNAME v kanálu CLUSRCVR , nemusíte měnit definici CLUSRCVR . DHCP vám přidělí novou IP adresu.

Pokud zadáte mezeru pro CONNAME v definici CLUSRCVR , IBM MQ vygeneruje CONNAME z adresy IP systému. V úložištích je uložen pouze vygenerovaný soubor CONNAME . Jiní správci front v klastru nevědí, že hodnota CONNAME byla původně prázdná.

Zadáte-li příkaz `DISPLAY CLUSQMGR` , zobrazí se vygenerovaný příkaz CONNAME. Pokud však zadáte příkaz `DISPLAY CHANNEL` z lokálního správce front, uvidíte, že CONNAME je prázdné.

Pokud je správce front zastaven a restartován s jinou adresou IP, produkt IBM MQ kvůli protokolu DHCP znovu vygeneruje název CONNAME a odpovídajícím způsobem aktualizuje úložiště.

Související pojmy

Vyrovňování pracovní zátěže v klastrech

Pokud klastř obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směrována. K určení nejlepšího správce front, který má být použit, používá algoritmus správy pracovní zátěže klastru a řadu atributů specifických pro pracovní zátěž klastru.

z/OS

Asynchronní chování příkazů CLUSTER v systému z/OS

Vydavatel příkazu klastru v systému z/OS obdrží potvrzení, že byl příkaz odeslán, ale ne že byl úspěšně dokončen.

Související odkazy

Atributy klastru dostupné v příkazech definice fronty

Atributy klastru, které lze zadat v příkazech definice fronty.

Atributy klastru dostupné v příkazech definice správce front

Atributy klastru, které lze zadat v příkazech definice správce front.

DISPLAY CLUSQMGR

Pomocí příkazu `DISPLAY CLUSQMGR` můžete zobrazit informace o klastrech správců front v klastru.

Aktualizovat klastř

Zadejte příkaz `REFRESH CLUSTER` ze správce front, abyste vyřadili všechny lokálně uchovávané informace o klastru. Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

RESET CLUSTER: Vynucené odebrání správce front z klastru

Příkaz **RESET CLUSTER** se používá k vynucovému odebrání správce front z klastru za výjimečných okolností.

SUSPEND QMGR, RESUME QMGR a klastry

Pomocí příkazů `SUSPEND QMGR` a `RESUME QMGR` můžete dočasně snížit aktivitu příchozího klastru pro tohoto správce front, například před provedením údržby tohoto správce front, a poté jej znovu uvést do původního stavu.

Atributy klastru dostupné v příkazech definice fronty

Atributy klastru, které lze zadat v příkazech definice fronty.

Příkazy **DEFINE QLOCAL**, **DEFINE QREMOTE** a **DEFINE QALIAS**

Atributy klastru v příkazech **DEFINE QLOCAL**, **DEFINE QREMOTE** a **DEFINE QALIAS** a tři ekvivalentní příkazy **ALTER**:

CLUSTER

Určuje název klastru, ke kterému fronta náleží.

CLUSNL

Určuje seznam názvů klastrů.

DEFBIND

Určuje vazbu, která má být použita v případě, že aplikace určuje hodnotu **MQOO_BIND_AS_Q_DEF** ve volání **MQOPEN**. Volby pro tento atribut jsou:

- Zadejte **DEFBIND(OPEN)**, chcete-li při otevření fronty svázat manipulátor fronty se specifickou instancí fronty klastru. **DEFBIND(OPEN)** je předvolba pro tento atribut.
- Zadejte hodnotu **DEFBIND(NOTFIXED)**, aby popisovač fronty nebyl svázán s žádnou instancí fronty klastru.
- Zadejte **DEFBIND(GROUP)**, chcete-li povolit aplikaci požadovat, aby skupina zpráv byla přidělena ke stejné cílové instanci.

Je-li v klastru správců front uvedeno více front se stejným názvem, mohou aplikace zvolit, zda mají být všechny zprávy z této aplikace odesílány do jedné instance (**MQOO_BIND_ON_OPEN**), povolit algoritmu správy pracovní zátěže výběr nejhodnějšího místa určení pro jednotlivé zprávy (**MQOO_BIND_NOT_FIXED**) nebo povolit aplikaci požadovat, aby byla "skupina" zpráv přidělena stejné cílové instanci (**MQOO_BIND_ON_GROUP**). Vyrovnávání pracovní zátěže je znovu řízeno mezi skupinami zpráv (bez požadavku na **MQCLOSE** a **MQOPEN** fronty).

Zadáte-li v definici fronty hodnotu **DEFBIND**, bude fronta definována s jedním z atributů **MQBND_BIND_ON_OPEN**, **MQBND_BIND_NOT_FIXED** nebo **MQBND_BIND_ON_GROUP**. Při použití skupin s klastru musí být zadána hodnota **MQBND_BIND_ON_OPEN** nebo **MQBND_BIND_ON_GROUP**.

Atribut **DEFBIND** byste měli nastavit na stejnou hodnotu ve všech instancích stejné fronty klastru.

CLWLRANK

Použije faktor hodnocení pro frontu pro účely správy pracovní zátěže. Parametr **CLWLRANK** není podporován v modelových frontách. Algoritmus pracovní zátěže klastru vybere cílovou frontu s nejvyšším hodnocením. Standardně je volba **CLWLRANK** pro všechny fronty nastavena na nulu.

Je-li konečným cílem správce front v jiném klastru, můžete nastavit ohodnocení důležitosti všech intermediačních správců front brány v průniku sousedních klastrů. Při ohodnocení pořadí intermediačních správců front algoritmus pracovní zátěže klastru správně vybere cílového správce front, který je blíže konečnému místu určení.

Stejná logika platí pro alias fronty. Výběr skupiny disků rank je proveden před kontrolou stavu kanálu, a proto jsou pro výběr k dispozici i nepřístupní správci front. To má za následek, že zpráva může být směrována přes síť, spíše než aby byla vybrána mezi dvěma možnými cíli (jako prioritou). Pokud tedy není kanál spuštěn na místo, kde je uvedena pozice, nebude zpráva směrována na další nejvyšší pozici, ale bude čekat, až bude kanál k dispozici pro dané místo určení (zpráva je zadržena ve vysílací frontě).

CLWLPRTY

Použije faktor priority na frontu pro účely správy pracovní zátěže. Algoritmus pracovní zátěže klastru vybere cílovou frontu s nejvyšší prioritou. Standardně je prioritou pro všechny fronty nastavena na nulu.

Pokud existují dvě možné cílové fronty, můžete pomocí tohoto atributu provést překonání selhání jednoho místa určení do druhého místa určení. Výběr priority se provede po kontrole stavu kanálu.

Všechny zprávy jsou odesílány do fronty s nejvyšší prioritou, pokud stav kanálu pro dané místo určení není tak příznivý jako stav kanálů pro jiná místa určení. To znamená, že pro výběr jsou k dispozici pouze ty nejdostupnější cíle. To má za následek stanovení priorit mezi více cíli, které jsou všechny k dispozici.

CLWLUSEQ

Určuje chování operace MQPUT pro frontu. Tento parametr určuje chování operace MQPUT, když má cílová fronta lokální instanci a alespoň jednu instanci vzdáleného klastru (kromě případů, kdy MQPUT pochází z kanálu klastru). Tento parametr je platný pouze pro lokální fronty.

Možné hodnoty jsou: QMGR (chování je určeno parametrem CLWLUSEQ definice správce front), ANY (správce front považuje lokální frontu za jinou instanci fronty klastru pro účely distribuce pracovní zátěže), LOCAL (lokální fronta je jediným cílem operace MQPUT za předpokladu, že je lokální fronta vložena). Chování MQPUT závisí na [algoritmu správy pracovní zátěže klastru](#).

Příkazy DISPLAY QUEUE a DISPLAY QCLUSTER

Atributy v příkazech DEFINE QLOCAL, DEFINE QREMOTE a DEFINE QALIAS platí také pro příkaz DISPLAY QUEUE.

Chcete-li zobrazit informace o frontách klastru, zadejte typ fronty QCLUSTER nebo klíčové slovo CLUSINFO v příkazu DISPLAY QUEUE nebo použijte příkaz DISPLAY QCLUSTER.

Příkaz DISPLAY QUEUE nebo DISPLAY QCLUSTER vrátí název správce front, který je hostitelem fronty (nebo názvy všech správců front, pokud existuje více než jedna instance fronty). Dále vrátí název systému pro každého správce front, který je hostitelem fronty, reprezentovaný typ fronty a datum a čas, kdy byla definice zpřístupněna lokálnímu správci front. Tyto informace jsou vráceny pomocí atributů CLUSQMGR, QMID, CLUSQT, CLUSDATE a CLUSTIME.

Název systému pro správce front (QMID) je jedinečný, systémem generovaný název správce front.

Můžete definovat frontu klastru, která je také sdílenou frontou. Například, v systému z/OS můžete definovat:


```
DEFINE QLOCAL(MYQUEUE) CLUSTER(MYCLUSTER) QSGDISP(SHARED) CFSTRUCT(STRUCTURE)
```

Ekvivalentní PCF jsou MQCMD_CHANGE_Q, MQCMD_COPY_Q, MQCMD_CREATE_Q a MQCMD_INQUIRE_Q.

Související pojmy

[Vyrovnávání pracovní zátěže v klastrech](#)

Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směrována. K určení nejlepšího správce front, který má být použit, používá algoritmus správy pracovní zátěže klastru a řadu atributů specifických pro pracovní zátěž klastru.

 [Asynchronní chování příkazů CLUSTER v systému z/OS](#)

Vydavatel příkazu klastru v systému z/OS obdrží potvrzení, že byl příkaz odeslán, ale ne že byl úspěšně dokončen.

Související odkazy

[Atributy klastru dostupné v příkazech definice kanálu](#)

[Atributy klastru, které lze zadat v příkazech definice kanálu.](#)

[Atributy klastru dostupné v příkazech definice správce front](#)

[Atributy klastru, které lze zadat v příkazech definice správce front.](#)

[DISPLAY CLUSQMGR](#)

Pomocí příkazu DISPLAY CLUSQMGR můžete zobrazit informace o klastrech správců front v klastru.

[Aktualizovat klastr](#)

Zadejte příkaz REFRESH CLUSTER ze správce front, abyste vyřadili všechny lokálně uchovávané informace o klastru. Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

[RESET CLUSTER: Vynucené odebrání správce front z klastru](#)

Příkaz **RESET CLUSTER** se používá k vynucovému odebrání správce front z klastru za výjimečných okolností.

SUSPEND QMGR, RESUME QMGR a klastry

Pomocí příkazů **SUSPEND QMGR** a **RESUME QMGR** můžete dočasně snížit aktivitu příchozího klastru pro tohoto správce front, například před provedením údržby tohoto správce front, a poté jej znovu uvést do původního stavu.

“Atributy vyrovnávání pracovní zátěže klastru-fronta” na stránce 139

Abecední seznam atributů fronty používaných při vyrovnávání pracovní zátěže klastru.

Atributy klastru dostupné v příkazech definice správce front

Atributy klastru, které lze zadat v příkazech definice správce front.

Chcete-li určit, že správce front uchovává úplné úložiště pro klastr, použijte příkaz **ALTER QMGR** určující atribut **REPOS(*clustername*)**. Chcete-li zadat seznam několika názvů klastrů, definujte seznam názvů klastrů a poté zadejte atribut **REPOSNL(*namelist*)** v příkazu **ALTER QMGR** :

```
DEFINE NAMELIST(CLUSTERLIST)
      DESCR('List of clusters whose repositories I host')
      NAMES(CLUS1, CLUS2, CLUS3)
ALTER QMGR REPOSNL(CLUSTERLIST)
```

V příkazu **ALTER QMGR** můžete zadat další atributy klastru.

CLWLEXIT(*name*)

Určuje název uživatelské procedury, která má být volána při vložení zprávy do fronty klastru.

CLWLDATA(*data*)

Určuje data, která mají být předána uživatelské proceduře pracovní zátěže klastru.

CLWLLEN(*length*)

Určuje maximální množství dat zprávy, která mají být předána uživatelské proceduře pracovní zátěže klastru.

CLWLMRUC(*channels*)

Určuje maximální počet odchozích kanálů klastru.

CLWLMRUC je atribut lokálního správce front, který není šířen kolem klastru. Je k dispozici pro uživatelské procedury pracovní zátěže klastru a algoritmus pracovní zátěže klastru, který vybírá místo určení pro zprávy.

CLWLUSEQ(LOCAL|ANY)

Určuje chování produktu MQPUT v případě, že cílová fronta obsahuje lokální instanci i alespoň jednu vzdálenou instanci klastru. Tento atribut se nepoužije v případě, že je zdrojem operace vložení kanál klastru. Parametr **CLWLUSEQ** lze zadat jako atribut fronty i jako atribut správce front.

Pokud uvedete **ANY**, lokální fronta i vzdálené fronty jsou možné cíle MQPUT.

Pokud uvedete **LOCAL**, lokální fronta je jediným cílem MQPUT.

Ekvivalentní PCF jsou MQCMD_CHANGE_Q_MGR a MQCMD_INQUIRE_Q_MGR.

Související pojmy

Vyrovňování pracovní zátěže v klastrech

Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směrována. K určení nejlepšího správce front, který má být použit, používá algoritmus správy pracovní zátěže klastru a řadu atributů specifických pro pracovní zátěž klastru.

Asynchronní chování příkazů CLUSTER v systému z/OS

Vydavatel příkazu klastru v systému z/OS obdrží potvrzení, že byl příkaz odeslán, ale ne že byl úspěšně dokončen.

Související odkazy

Atributy klastru dostupné v příkazech definice kanálu

Atributy klastru, které lze zadat v příkazech definice kanálu.

Atributy klastru dostupné v příkazech definice fronty

Atributy klastru, které lze zadat v příkazech definice fronty.

DISPLAY CLUSQMGR

Pomocí příkazu `DISPLAY CLUSQMGR` můžete zobrazit informace o klastrech správců front v klastru.

Aktualizovat klastr

Zadejte příkaz `REFRESH CLUSTER` ze správce front, abyste vyřadili všechny lokálně uchovávané informace o klastru. Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

RESET CLUSTER: Vynucené odebrání správce front z klastru

Příkaz **RESET CLUSTER** se používá k vynucovému odebrání správce front z klastru za výjimečných okolností.

SUSPEND QMGR, RESUME QMGR a klastry

Pomocí příkazů `SUSPEND QMGR` a `RESUME QMGR` můžete dočasně snížit aktivitu příchozího klastru pro tohoto správce front, například před provedením údržby tohoto správce front, a poté jej znovu uvést do původního stavu.

“Vyrovnávání pracovní zátěže klastru-atributy správce front” na stránce 141

Abecední seznam atributů správce front používaných při vyrovnávání pracovní zátěže klastru.

DISPLAY CLUSQMGR

Pomocí příkazu `DISPLAY CLUSQMGR` můžete zobrazit informace o klastrech správců front v klastru.

Pokud tento příkaz zadáte ze správce front s úplným úložištěm, budou vrácené informace platit pro každého správce front v klastru. Jinak budou vrácené informace platit pouze pro správce front, kterých se to týká. To znamená každého správce front, na něhož byl učiněn pokus o odeslání zprávy, a každého správce front, který má úplné úložiště.

Informace zahrnují většinu atributů kanálu, které se vztahují na odesílací a přijímací kanály klastru. Kromě toho lze zobrazit následující atributy:

CHANNEL

Název přijímacího kanálu klastru pro správce front.

CLUSDATE

Datum, kdy byla definice zpřístupněna lokálnímu správci front.

CLUSTER

V jakých klastrech se nachází správce front.

CLUSTIME

Čas, kdy byla definice zpřístupněna lokálnímu správci front.

DEFTYPE

Jak byl správce front definován. `DEFTYPE` může být jedna z následujících hodnot:

CLUSSDR

Kanál odesilatele klastru byl administrativně definován v lokálním správci front, ale dosud nebyl rozpoznán cílovým správcem front. Chcete-li se nacházet v tomto stavu, lokální správce front definoval ruční odesílací kanál klastru, ale přijímací správce front nepřijal informace o klastru. Příčinou může být skutečnost, že kanál nebyl nikdy vytvořen kvůli dostupnosti nebo chybě v konfiguraci odesilatele klastru, například neshoda ve vlastnosti `CLUSTER` mezi definicemi odesilatele a příjemce. Jedná se o přechodný stav nebo chybový stav a je třeba jej vyšetřit.

CLUSSDRA

Tato hodnota představuje automaticky zjištěného správce front klastru, žádný odesílací kanál klastru není definován lokálně. Jedná se o typ `DEFTYPE` pro správce front klastru, pro které lokální správce front nemá žádnou lokální konfiguraci, ale byl o tom informován. Například:

- Pokud je lokálním správcem front správce front správce front s úplným úložištěm, měla by se jednat o hodnotu `DEFTYPE` pro všechny správce front s částečným úložištěm v klastru.

- Pokud je lokální správce front částečným úložištěm, může se jednat o hostitele fronty klastru, která je používána z tohoto lokálního správce front, nebo z druhého správce front úplného úložiště, se kterým byl tento správce front informován o práci.

Je-li hodnota DEFTYPE CLUSSDRA a oba lokální a vzdálení správci front jsou úplnými úložišti pro uvedený klastr, konfigurace není správná, protože musí být definován lokálně definovaný odesílací kanál klastru, aby se převedl na DEFTYPE CLUSDRB.

CLUSDRB

Kanál odesílatele klastru byl administrativně definován v lokálním správci front a byl přijat cílovým správcem front jako platný kanál klastru. Jedná se o očekávaný typ DEFTYPE ručně konfigurovaného správce front úplného úložiště pro správce front dílčího úložiště. Mělo by to být také DEFTYPE libovolného CLUSQMGR z jednoho úplného úložiště do jiného úplného úložiště v klastru. Odesílací kanály ručního klastru by neměly být konfigurovány na dílčí úložiště nebo ze správce front dílčího úložiště na více než jedno úplné úložiště. Pokud je DEFTYPE CLUSSDRB viděn v jedné z těchto situací, měl by být vyšetřen a opraven.

CLUSRCVR

Administrativně definovaný jako přijímací kanál klastru v lokálním správci front. Toto představuje lokálního správce front v klastru.

Poznámka: Chcete-li identifikovat, kteří CLUSQMGRs jsou správci front úplného úložiště pro klastr, prohlédněte si vlastnost QMTYPE .

Další informace o definování kanálů klastru naleznete v tématu Kanály klastru.

QMTYPE

Zda obsahuje úplné úložiště, nebo pouze dílčí úložiště.

STATUS

Stav odesílacího kanálu klastru pro tohoto správce front.

SUSPEND

Zda je správce front pozastaven.

verze

Verze instalace produktu IBM MQ , ke které je přidružen správce front klastru.

Verze je ve formátu VVRRMMFF:

- VV: Verze
- RR: Vydání
- MM: Úroveň údržby
- FF: Úroveň opravy

XMITQ


Přenosová fronta klastru používaná správcem front.

Viz také příkaz `DISPLAY QCLUSTER` . To je stručně popsáno v části `DISPLAY QUEUE` a v části "Atributy klastru dostupné v příkazech definice fronty" na stránce 128 `DISPLAY QUEUE` a `DISPLAY QCLUSTER` příkazy . Chcete-li získat příklady použití produktu `DISPLAY QCLUSTER`, vyhledejte v sadě informací "DISPLAY QCLUSTER" a "DIS QCLUSTER".

Související pojmy

Vyrovňávání pracovní zátěže v klastrech

Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směrována. K určení nejlepšího správce front, který má být použit, používá algoritmus správy pracovní zátěže klastru a řadu atributů specifických pro pracovní zátěž klastru.

 Asynchronní chování příkazů CLUSTER v systému z/OS

Vydavatel příkazu klastru v systému z/OS obdrží potvrzení, že byl příkaz odeslán, ale ne že byl úspěšně dokončen.

Související odkazy

Atributy klastru dostupné v příkazech definice kanálu

Atributy klastru, které lze zadat v příkazech definice kanálu.

Atributy klastru dostupné v příkazech definice fronty

Atributy klastru, které lze zadat v příkazech definice fronty.

Atributy klastru dostupné v příkazech definice správce front

Atributy klastru, které lze zadat v příkazech definice správce front.

Aktualizovat klastr

Zadejte příkaz REFRESH CLUSTER ze správce front, abyste vyřadili všechny lokálně uchovávané informace o klastru. Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

RESET CLUSTER: Vynucené odebrání správce front z klastru

Příkaz **RESET CLUSTER** se používá k vynucovému odebrání správce front z klastru za výjimečných okolností.

SUSPEND QMGR, RESUME QMGR a klastry

Pomocí příkazů SUSPEND QMGR a RESUME QMGR můžete dočasně snížit aktivitu příchozího klastru pro tohoto správce front, například před provedením údržby tohoto správce front, a poté jej znovu uvést do původního stavu.

Příkaz MQSC DISPLAY CLUSQMGR

Aktualizovat klastr

Zadejte příkaz REFRESH CLUSTER ze správce front, abyste vyřadili všechny lokálně uchovávané informace o klastru. Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

Existují tři formy tohoto příkazu:

REFRESH CLUSTER(cclustername) REPOS(NO)

Výchozí hodnota Správce front si uchovává informace o všech lokálně definovaných frontách front klastru a front klastru a všech správcích front klastru, kteří jsou úplnými úložišti. Kromě toho, pokud je správce front úplným úložištěm pro klastr, uchová si také informace o ostatních správcích front klastru v klastru. Vše ostatní je odebráno z lokální kopie úložiště a znovu sestaveno z ostatních úplných úložišť v klastru. Kanály klastru se nezastaví, pokud se použije REPOS(NO). Úplné úložiště používá své kanály CLUSSDR, aby informovalo zbytek klastru, že dokončil svou aktualizaci.

REFRESH CLUSTER(cclustername) REPOS(YES)

Kromě výchozího chování jsou aktualizovány také objekty představující správce front klastru s úplným úložištěm. Použití této volby není platné, pokud je správce front úplným úložištěm. Pokud je použit, příkaz selže s chybou AMQ9406/CSQX406E. Pokud se jedná o úplné úložiště, musíte je nejprve změnit tak, aby nebylo úplným úložištěm pro daný klastr. Úplné umístění úložiště je obnoveno z ručně definovaných definic CLUSSDR. Po vydání aktualizace pomocí produktu REPOS(YES) lze správce front změnit tak, aby se v případě potřeby znovu stal úplným úložištěm.

REFRESH CLUSTER(*)

Aktualizuje správce front ve všech klastrech, jejichž je členem. Pokud se používá s produktem REPOS(YES) REFRESH CLUSTER(*), má další vliv na to, aby správce front restartoval své hledání úplných úložišť z informací v lokálních definicích CLUSSDR. Vyhledávání proběhne i v případě, že kanál CLUSSDR připojí správce front k několika klastrům.

Poznámka: Použití příkazu **REFRESH CLUSTER** může narušit provoz velkých klastrů, a to jak při spuštění, tak později v 27denních intervalech, kdy objekty klastru automaticky rozesílají aktualizace stavu všem zainteresovaným správcům front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.

Související pojmy

Vyrovňování pracovní zátěže v klastrech

Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směrována. K určení nejlepšího správce front, který má být použit, používá algoritmus správy pracovní zátěže klastru a řadu atributů specifických pro pracovní zátěž klastru.

Vydavatel příkazu klastru v systému z/OS obdrží potvrzení, že byl příkaz odeslán, ale ne že byl úspěšně dokončen.

Související odkazy

[Atributy klastru dostupné v příkazech definice kanálu](#)

Atributy klastru, které lze zadat v příkazech definice kanálu.

[Atributy klastru dostupné v příkazech definice fronty](#)

Atributy klastru, které lze zadat v příkazech definice fronty.

[Atributy klastru dostupné v příkazech definice správce front](#)

Atributy klastru, které lze zadat v příkazech definice správce front.

DISPLAY CLUSQMGR

Pomocí příkazu DISPLAY CLUSQMGR můžete zobrazit informace o klastrech správců front v klastru.

[RESET CLUSTER: Vynucené odebrání správce front z klastru](#)

Příkaz **RESET CLUSTER** se používá k vynucovému odebrání správce front z klastru za výjimečných okolností.

[SUSPEND QMGR, RESUME QMGR a klastry](#)

Pomocí příkazů SUSPEND QMGR a RESUME QMGR můžete dočasně snížit aktivitu příchozího klastru pro tohoto správce front, například před provedením údržby tohoto správce front, a poté jej znovu uvést do původního stavu.

Související informace

[Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER](#)

RESET CLUSTER: Vynucené odebrání správce front z klastru

Příkaz **RESET CLUSTER** se používá k vynucovému odebrání správce front z klastru za výjimečných okolností.

Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

Příkaz **RESET CLUSTER** můžete zadat pouze ze správců front úplného úložiště. Příkaz má dvě formy v závislosti na tom, zda odkazujete na správce front podle názvu nebo identifikátoru.

1.

```
RESET CLUSTER( clustername
) QMNAME( qmname ) ACTION(FORCEREMOVE) QUEUES(NO)
```
2.

```
RESET CLUSTER( clustername
) QMID( qmids ) ACTION(FORCEREMOVE) QUEUES(NO)
```

Nelze současně zadat QMNAME a QMID. Pokud použijete QMNAMEa v klastru s tímto názvem je více než jeden správce front, příkaz se nespustí. Použijte QMID místo QMNAME , abyste se ujistili, že je spuštěn příkaz **RESET CLUSTER** .

Určení QUEUES(NO) v příkazu **RESET CLUSTER** je výchozí. Zadáním parametru QUEUES(YES) odeberete odkazy na fronty klastru vlastněné správcem front z klastru. Kromě odebrání správce front ze samotného klastru jsou odkazy odebrány.

Odkazy jsou odebrány i v případě, že správce front klastru není v klastru viditelný; možná proto, že byl dříve vynuceně odebrán, bez volby QUEUES .

Příkaz **RESET CLUSTER** můžete použít například v případě, že byl odstraněn správce front, ale pro klastr jsou stále definovány přijímací kanály klastru. Místo čekání na odebrání těchto definic produktem IBM MQ (což se provádí automaticky) můžete zadat příkaz **RESET CLUSTER** , který se dříve upraví. Všichni ostatní správci front v klastru jsou poté informováni o tom, že daný správce front již není k dispozici.

Dojde-li k dočasnému poškození správce front, může být vhodné informovat ostatní správce front v klastru před tím, než se pokusí odeslat zprávy. Produkt **RESET CLUSTER** odebere poškozeného správce

front. Později, když poškozený správce front znovu pracuje, použijte příkaz **REFRESH CLUSTER**, abyste obrátili účinek produktu **RESET CLUSTER** a vrátili správce front do klastru. Je-li správce front v klastru publikování/odběru, musíte znovu nastavit všechny požadované proxy odběry. Viz [Aspekty REFRESH CLUSTER pro klastry publikování/odběru](#).

Poznámka: Použití příkazu **REFRESH CLUSTER** může narušit provoz velkých klastrů, a to jak při spuštění, tak později v 27denních intervalech, kdy objekty klastru automaticky rozesílají aktualizace stavu všem zainteresovaným správcům front. Viz téma [Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost](#).

Použití příkazu **RESET CLUSTER** je jediný způsob, jak odstranit automaticky definované odesílací kanály klastru.

Důležité: Je-li automaticky definovaný kanál, který má být odebrán, nejistý, produkt **RESET CLUSTER** tento kanál okamžitě neodebere. V této situaci musíte zadat příkaz [RESOLVE CHANNEL](#) před příkazem **RESET CLUSTER**.

Za normálních okolností není pravděpodobné, že byste tento příkaz potřebovali. Podpora IBM vám může doporučit, abyste zadali příkaz k uklizení informací o klastru, které drží správci front klastru. Tento příkaz nepoužívejte jako zkratku pro odebrání správce front z klastru. Správný způsob odebrání správce front z klastru je popsán v tématu [Odebrání správce front z klastru](#).

Vzhledem k tomu, že úložiště uchovávají informace pouze po dobu 90 dnů, může se po uplynutí této doby správce front, který byl vynuceně odebrán, znovu připojit ke klastru. Automaticky se znovu připojí, pokud nebyl odstraněn. Chcete-li zabránit opětovnému připojení správce front ke klastru, je třeba provést příslušná bezpečnostní opatření.

Všechny příkazy klastru s výjimkou **DISPLAY CLUSQMgr** pracují asynchronně. Příkazy, které mění atributy objektů zahrnující klastrování, aktualizují objekt a odešlou požadavek na procesor úložiště. Příkazy pro práci s klastry jsou kontrolovány na syntaxi a požadavek je odeslán do procesoru úložiště.

Požadavky odeslané do procesoru úložiště jsou zpracovány asynchronně spolu s požadavky klastru přijatými od ostatních členů klastru. Zpracování může trvat delší dobu, pokud se musí šířit po celém klastru, aby se zjistilo, zda jsou úspěšné nebo ne.

Související pojmy

[Vyrovnávání pracovní zátěže v klastrech](#)

Pokud klaster obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směrována. K určení nejlepšího správce front, který má být použit, používá algoritmus správy pracovní zátěže klastru a řadu atributů specifických pro pracovní zátěž klastru.

Asynchronní chování příkazů CLUSTER v systému z/OS

Vydavatel příkazu klastru v systému z/OS obdrží potvrzení, že byl příkaz odeslán, ale ne že byl úspěšně dokončen.

Související odkazy

[Atributy klastru dostupné v příkazech definice kanálu](#)

[Atributy klastru, které lze zadat v příkazech definice kanálu.](#)

[Atributy klastru dostupné v příkazech definice fronty](#)

[Atributy klastru, které lze zadat v příkazech definice fronty.](#)

[Atributy klastru dostupné v příkazech definice správce front](#)

[Atributy klastru, které lze zadat v příkazech definice správce front.](#)

[DISPLAY CLUSQMgr](#)

Pomocí příkazu **DISPLAY CLUSQMgr** můžete zobrazit informace o klastrech správců front v klastru.

[Aktualizovat klaster](#)

Zadejte příkaz **REFRESH CLUSTER** ze správce front, abyste vyřadili všechny lokálně uchovávané informace o klastru. Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

[SUSPEND QMgr, RESUME QMgr a klastry](#)

Pomocí příkazů `SUSPEND QMGR` a `RESUME QMGR` můžete dočasně snížit aktivitu příchozího klastru pro tohoto správce front, například před provedením údržby tohoto správce front, a poté jej znovu uvést do původního stavu.

[RESET CLUSTER \(resetujte klastr\)](#)

SUSPEND QMGR, RESUME QMGR a klastry

Pomocí příkazů `SUSPEND QMGR` a `RESUME QMGR` můžete dočasně snížit aktivitu příchozího klastru pro tohoto správce front, například před provedením údržby tohoto správce front, a poté jej znovu uvést do původního stavu.


Je-li správce front pozastaven z klastru, neobdrží zprávy ve frontách klastru, které je hostitelem, pokud je v alternativním správci front v klastru k dispozici fronta se stejným názvem. Zprávy, které jsou explicitně zacíleny na tohoto správce front nebo kde je cílová fronta k dispozici pouze pro tohoto správce front, jsou však stále směřovány na tohoto správce front.

Příjem dalších příchozích zpráv v době, kdy je správce front pozastaven, lze zabránit zastavením přijímacích kanálů klastru pro tento klastr. Chcete-li zastavit přijímací kanály klastru, použijte režim `FORCE` příkazu [SUSPEND QMGR](#).

Související pojmy

[Vyrovňování pracovní zátěže v klastrech](#)

Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směřována. K určení nejlepšího správce front, který má být použit, používá algoritmus správy pracovní zátěže klastru a řadu atributů specifických pro pracovní zátěž klastru.

 [Asynchronní chování příkazů CLUSTER v systému z/OS](#)

Vydavatel příkazu klastru v systému z/OS obdrží potvrzení, že byl příkaz odeslán, ale ne že byl úspěšně dokončen.

Související úlohy

[Údržba správce front](#)

Související odkazy

[Atributy klastru dostupné v příkazech definice kanálu](#)

[Atributy klastru, které lze zadat v příkazech definice kanálu.](#)

[Atributy klastru dostupné v příkazech definice fronty](#)

[Atributy klastru, které lze zadat v příkazech definice fronty.](#)

[Atributy klastru dostupné v příkazech definice správce front](#)

[Atributy klastru, které lze zadat v příkazech definice správce front.](#)

[DISPLAY CLUSQMGR](#)

Pomocí příkazu `DISPLAY CLUSQMGR` můžete zobrazit informace o klastrech správců front v klastru.

[Aktualizovat klastr](#)

Zadejte příkaz `REFRESH CLUSTER` ze správce front, abyste vyřadili všechny lokálně uchovávané informace o klastru. Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

[RESET CLUSTER: Vynucené odebrání správce front z klastru](#)

Příkaz **RESET CLUSTER** se používá k vynucovému odebrání správce front z klastru za výjimečných okolností.

[SUSPEND QMgr](#)

[OBNOVTE SPRÁVCE FRONT](#)

Vyrovňování pracovní zátěže v klastrech


Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směřována. K určení nejlepšího správce front, který má být použit, používá algoritmus správy pracovní zátěže klastru a řadu atributů specifických pro pracovní zátěž klastru.

Vhodná místa určení jsou zvolena algoritmem správy pracovní zátěže klastru na základě dostupnosti správce front a fronty a na základě řady atributů specifických pro pracovní zátěž klastru, které jsou přidruženy k kanálům, frontám a správcům front. Tyto atributy jsou popsány v dílčích tématech.

Pokud se konfigurace po konfiguraci atributů specifických pro pracovní zátěž klastru nechová tak, jak jste očekávali, prozkoumejte podrobnosti o tom, jak algoritmus vybírá správce front. Viz [“Algoritmus správy pracovní zátěže klastru”](#) na stránce 142. Pokud výsledky tohoto algoritmu nevyhovují vašim potřebám, můžete napsat uživatelský program pracovní zátěže klastru a pomocí této uživatelské procedury směřovat zprávy do fronty dle vašeho výběru v klastru. Viz [Zápis a kompilace uživatelských procedur pracovní zátěže klastru](#).

<i>Tabulka 59. Souhrn atributů specifických pro pracovní zátěž klastru</i>	
Název atributu	Popis
Atributy kanálu	
CLWLPRTY	Určuje pořadí priorit pro kanály pro distribuci pracovní zátěže klastru.
CLWLRANK	Určuje pořadí kanálů pro distribuci pracovní zátěže klastru.
CLWLWGHT	Určuje váhu použitou pro kanály CLUSSDR a CLUSRCVR pro distribuci pracovní zátěže klastru.
NETPRTY	Určuje prioritu kanálu CLUSRCVR .
Atributy fronty	
CLWLPRTY	Určuje prioritu lokálních, vzdálených nebo alias front pro distribuci pracovní zátěže klastru.
CLWLRANK	Určuje pořadí lokální, vzdálené nebo alias fronty pro distribuci pracovní zátěže klastru.
CLWLUSEQ	Uvádí, zda má být lokální instance fronty upřednostňována jako místo určení nad ostatními instancemi v klastru.
Atributy správce front	
CLWLMRUC	Nastaví počet naposledy vybraných kanálů.
CLWLUSEQ	Určuje, zda je lokální instance fronty upřednostňována jako cíl před ostatními instancemi fronty v klastru.

Související pojmy

 Asynchronní chování příkazů CLUSTER v systému z/OS

Vydavatel příkazu klastru v systému z/OS obdrží potvrzení, že byl příkaz odeslán, ale ne že byl úspěšně dokončen.

Související odkazy

[Atributy klastru dostupné v příkazech definice kanálu](#)

[Atributy klastru, které lze zadat v příkazech definice kanálu.](#)

[Atributy klastru dostupné v příkazech definice fronty](#)

[Atributy klastru, které lze zadat v příkazech definice fronty.](#)

[Atributy klastru dostupné v příkazech definice správce front](#)

[Atributy klastru, které lze zadat v příkazech definice správce front.](#)

[DISPLAY CLUSQMGR](#)

Pomocí příkazu DISPLAY CLUSQMGR můžete zobrazit informace o klastrech správců front v klastru.

Aktualizovat klastr

Zadejte příkaz `REFRESH CLUSTER` ze správce front, abyste vyřadili všechny lokálně uchovávané informace o klastru. Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

RESET CLUSTER: Vynucené odebrání správce front z klastru

Příkaz **RESET CLUSTER** se používá k vynucovému odebrání správce front z klastru za výjimečných okolností.

SUSPEND QMGR, RESUME QMGR a klastry

Pomocí příkazů `SUSPEND QMGR` a `RESUME QMGR` můžete dočasně snížit aktivitu příchozího klastru pro tohoto správce front, například před provedením údržby tohoto správce front, a poté jej znovu uvést do původního stavu.

Vyrovňávání pracovní zátěže klastru-atributy kanálu

Abecední seznam atributů kanálu používaných při vyrovňávání pracovní zátěže klastru.

Poznámka: Zadejte atributy kanálu pracovní zátěže klastru v přijímacích kanálech klastru v cílových správcích front. Jakékoli vyvážení, které zadáte na odpovídajících odesílacích kanálech klastru, bude pravděpodobně ignorováno. Viz [Kanály klastru](#).

CLWLPRTY (priorita pracovní zátěže klastru)

Atribut kanálu `CLWLPRTY` určuje pořadí priorit pro kanály pro distribuci pracovní zátěže klastru. Hodnota musí být v rozsahu 0-9, kde 0 je nejnižší priorita a 9 je nejvyšší.

Pomocí atributu kanálu `CLWLPRTY` můžete nastavit pořadí priorit pro dostupná místa určení klastru. Produkt IBM MQ vybere cíle s nejvyšší prioritou před výběrem cílů s nejnižší prioritou cíle klastru. Pokud existuje více míst určení se stejnou prioritou, vybere nejméně nedávno použité místo určení.

Pokud existují dva možné cíle, můžete pomocí tohoto atributu povolit překonání selhání. Zprávy se odesílají do správce front s kanálem s nejvyšší prioritou. Pokud nebude k dispozici, přejdou zprávy na dalšího správce front s nejvyšší prioritou. Správci front s nižší prioritou vystupují jako rezervy.

Produkt IBM MQ kontroluje stav kanálu před stanovením priority kanálů. Kandidáty na výběr jsou pouze dostupní správci front.

Notes:

- Určete tento atribut v přijímacím kanálu klastru v cílovém správci front. Jakékoli vyvážení, které zadáte v odpovídajícím odesílacím kanálu klastru, bude pravděpodobně ignorováno. Viz [Kanály klastru](#).
- Dostupnost vzdáleného správce front je založena na stavu kanálu pro daného správce front. Při spuštění kanálů se jejich stav několikrát změní, přičemž některé ze stavů mají nižší prioritu než algoritmus správy pracovní zátěže klastru. V praxi to znamená, že lze vybrat cíle s nižší prioritou (záložní), zatímco se začínají kanály s cíli s vyšší prioritou (primární).
- Potřebujete-li se ujistit, že do cíle zálohování nepřejdou žádné zprávy, nepoužívejte příkaz `CLWLPRTY`. Zvažte použití oddělených front nebo `CLWLRANK` s ručním přepínáním z primárního k zálohování.

CLWLRANK (rank pracovní zátěže klastru)

Atribut kanálu `CLWLRANK` určuje pořadí kanálů pro distribuci pracovní zátěže klastru. Hodnota musí být v rozsahu 0-9, kde 0 je nejnižší a 9 je nejvyšší.

Atribut kanálu `CLWLRANK` použijte v případě, že chcete řídit konečné místo určení pro zprávy odeslané správci front v jiném klastru. Výběr konečného místa určení můžete řídit nastavením pořadí kanálů, které připojují správce front ke správcům front brány v průniku klastrů.

Nastavíte-li parametr `CLWLRANK`, zprávy budou mít určenou trasu přes propojené klastry směrem k cíli s vyšším hodnocením. Zprávy například přicházejí do správce front brány, který je může odeslat jednomu ze dvou správců front s použitím kanálů s hodnocením 1 a 2. Jsou automaticky odesílány do správce front připojeného kanálem s nejvyšší hodnotou, v tomto případě kanál do správce front s hodnocením 2.

Produkt IBM MQ získá ohodnocení důležitosti kanálů před kontrolou stavu kanálu. Získání hodnoty před kontrolou stavu kanálu znamená, že pro výběr jsou k dispozici i nepřístupné kanály. Umožňuje směřování zpráv po síti i v případě, že konečný cíl není k dispozici.

Notes:

- Určete tento atribut v přijímacím kanálu klastru v cílovém správci front. Jakékoli vyvážení, které zadáte v odpovídajícím odesílacím kanálu klastru, bude pravděpodobně ignorováno. Viz [Kanály klastru](#).
- Pokud jste také použili atribut priority **CLWLPRTY**, produkt IBM MQ provede výběr mezi dostupnými cíli. Pokud není kanál k dispozici pro místo určené s nejvyšším hodnocením, je zpráva zadržena v přenosové frontě. Je uvolněn, když je kanál k dispozici. Zpráva se neodešle na další dostupný cíl v pořadí podle důležitosti.

CLWLWGHT (váha pracovní zátěže klastru)

Atribut kanálu CLWLWGHT určuje váhu použitou pro kanály CLUSSDR a CLUSRCVR pro distribuci pracovní zátěže klastru. Hodnota musí být v rozsahu 1-99, kde 1 je nejnižší váha a 99 je nejvyšší.

Použijte CLWLWGHT k odeslání serverů s větším výkonem zpracování více zpráv. Čím vyšší je váha kanálu, tím více zpráv je odesláno přes tento kanál.

Notes:

- Určete tento atribut v přijímacím kanálu klastru v cílovém správci front. Jakékoli vyvážení, které zadáte v odpovídajícím odesílacím kanálu klastru, bude pravděpodobně ignorováno. Viz [Kanály klastru](#).
- Je-li funkce CLWLWGHT upravena z výchozí hodnoty 50 na libovolném kanálu, bude vyrovnávání pracovní zátěže záviset na celkovém počtu případů, kdy byl každý kanál vybrán pro zprávu odeslanou do libovolné klastrované fronty. Další informace viz téma [“Algoritmus správy pracovní zátěže klastru”](#) na stránce 142.

NETPRTY (priorita síťového připojení)

Atribut kanálu NETPRTY určuje prioritu kanálu CLUSRCVR. Hodnota musí být v rozsahu 0-9, kde 0 je nejnižší priorita a 9 je nejvyšší.

Pomocí atributu NETPRTY nastavte jednu síť jako primární síť a jinou síť jako záložní síť. Je-li k dispozici sada kanálů se stejným hodnocením, klastrování zvolí cestu s nejvyšší prioritou, je-li k dispozici více cest.

Typickým příkladem použití atributu kanálu NETPRTY je rozlišení mezi sítěmi, které mají různé náklady nebo rychlosti, a připojení stejných cílů.

Poznámka: Určete tento atribut v přijímacím kanálu klastru v cílovém správci front. Jakékoli vyvážení, které zadáte v odpovídajícím odesílacím kanálu klastru, bude pravděpodobně ignorováno. Viz [Kanály klastru](#).

Související pojmy

[Algoritmus správy pracovní zátěže klastru](#)

[Algoritmus správy pracovní zátěže používá atributy vyrovnávání pracovní zátěže a mnoho pravidel k výběru konečného místa určené pro zprávy vkládané do fronty klastru.](#)

Související odkazy

[Atributy vyrovnávání pracovní zátěže klastru-fronta](#)

Abecední seznam atributů fronty používaných při vyrovnávání pracovní zátěže klastru.

[Vyrovnávání pracovní zátěže klastru-atributy správce front](#)

Abecední seznam atributů správce front používaných při vyrovnávání pracovní zátěže klastru.

[“Atributy klastru dostupné v příkazech definice kanálu”](#) na stránce 125

[Atributy klastru, které lze zadat v příkazech definice kanálu.](#)

Atributy vyrovnávání pracovní zátěže klastru-fronta

Abecední seznam atributů fronty používaných při vyrovnávání pracovní zátěže klastru.

CLWLPRTY

Atribut fronty **CLWLPRTY** určuje prioritu lokálních, vzdálených nebo alias front pro distribuci pracovní zátěže klastru. Hodnota musí být v rozsahu 0-9, kde 0 je nejnižší priorita a 9 je nejvyšší.

Pomocí atributu fronty **CLWLPRTY** nastavte předvolbu pro cílové fronty. Produkt IBM MQ vybere cíle s nejvyšší prioritou před výběrem cílů s nejnižší prioritou cíle klastru. Pokud existuje více míst určení se stejnou prioritou, vybere nejméně nedávno použité místo určení.

Produkt IBM MQ získá prioritu správců front po kontrole stavu kanálu. Kandidáty na výběr jsou pouze dostupní správci front.

Poznámka:

Dostupnost vzdáleného správce front je založena na stavu kanálu pro daného správce front. Při spuštění kanálů se jejich stav několikrát změní, přičemž některé ze stavů mají nižší prioritu než algoritmus správy pracovní zátěže klastru. V praxi to znamená, že lze vybrat cíle s nižší prioritou (záložní), zatímco se začínají kanály s cíli s vyšší prioritou (primární).

Potřebujete-li se ujistit, že do místa určení zálohy nesměřují žádné zprávy, nepoužívejte **CLWLPRTY**. Zvažte použití oddělených front nebo **CLWLRANK** s ručním přepínáním z primárního serveru pro zálohování.

Pokud existují dva možné cíle, můžete pomocí tohoto atributu povolit překonání selhání. Správce front s nejvyšší prioritou přijímá požadavky, správci front s nižší prioritou vystupují jako rezervy. Pokud správce front s nejvyšší prioritou selže, převezme další dostupný správce front s nejvyšší prioritou.

CLWLRANK

Atribut fronty **CLWLRANK** určuje pořadí lokální, vzdálené nebo alias fronty pro distribuci pracovní zátěže klastru. Hodnota musí být v rozsahu 0-9, kde 0 je nejnižší a 9 je nejvyšší.

Atribut fronty **CLWLRANK** použijte v případě, že chcete řídit konečné místo určení pro zprávy odeslané správci front v jiném klastru. Nastavíte-li parametr **CLWLRANK**, zprávy budou mít určenou trasu přes propojené klastry směrem k cíli s vyšším hodnocením.

Mohli jste například definovat dva stejně nakonfigurované správce front brány, abyste zlepšili dostupnost brány. Předpokládejme, že jste definovali alias fronty klastru na bránách pro lokální frontu definovanou v klastru. Pokud se lokální fronta stane nedostupnou, zamýšlíte, aby byla zpráva zadržena na jedné z bran čekajících na opětovnou dostupnost fronty. Chcete-li zadržet frontu na bráně, musíte definovat lokální frontu s vyšším hodnocením než alias fronty klastru na bráně.

Pokud definujete lokální frontu se stejným hodnocením jako aliasy fronty a lokální fronta je nedostupná, zpráva se bude pohybovat mezi bránami. Při zjištění, že lokální fronta není k dispozici, směřuje první správce front brány zprávu na druhou bránu. Druhá brána se znovu pokusí doručit zprávu do cílové lokální fronty. Pokud je lokální fronta stále nedostupná, přesměruje zprávu zpět na první bránu. Zpráva se stále přesouvá mezi branami a zpět, dokud nebude cílová lokální fronta znovu k dispozici. Pokud lokální frontě dáte vyšší hodnocení, i když fronta není k dispozici, nebude zpráva přesměrována na místo určení s nižším hodnocením.

Produkt IBM MQ získá ohodnocení důležitosti front před kontrolou stavu kanálu. Získání hodnoty před kontrolou stavu kanálu znamená, že pro výběr jsou k dispozici i nepřístupné fronty. Umožňuje směrování zpráv po síti i v případě, že konečný cíl není k dispozici.

Pokud jste použili atribut priority IBM MQ, vybere mezi dostupnými cíli. Pokud není kanál k dispozici pro místo určení s nejvyšším hodnocením, je zpráva zadržena v přenosové frontě. Je uvolněn, když je kanál k dispozici. Zpráva se neodešle na další dostupný cíl v pořadí podle důležitosti.

CLWLUSEQ

Atribut fronty **CLWLUSEQ** určuje, zda je lokální instance fronty upřednostňována jako cíl před ostatními instancemi v klastru.

Atribut fronty **CLWLUSEQ** je platný pouze pro lokální fronty. Použije se pouze v případě, že je zpráva vložena aplikací nebo kanálem, který není kanálem klastru.

LOKÁLNÍ

Lokální fronta je jediným cílem produktu MQPUT, za předpokladu, že lokální fronta je povolena. MQPUT chování závisí na [správě pracovní zátěže klastru](#).

QMGR

Chování je určeno atributem správce front **CLWLUSEQ**.

ANY

Produkt MQPUT zachází s lokální frontou stejně jako s jakoukoli jinou instancí fronty v klastru pro distribuci pracovní zátěže.

Související pojmy

[Algoritmus správy pracovní zátěže klastru](#)

Algoritmus správy pracovní zátěže používá atributy vyrovnávání pracovní zátěže a mnoho pravidel k výběru konečného místa určení pro zprávy vkládané do front klastru.

Související odkazy

[Vyrovnávání pracovní zátěže klastru-atributy kanálu](#)

Abecední seznam atributů kanálu používaných při vyrovnávání pracovní zátěže klastru.

[Vyrovnávání pracovní zátěže klastru-atributy správce front](#)

Abecední seznam atributů správce front používaných při vyrovnávání pracovní zátěže klastru.

[“Atributy klastru dostupné v příkazech definice fronty” na stránce 128](#)

Atributy klastru, které lze zadat v příkazech definice fronty.

Vyrovnávání pracovní zátěže klastru-atributy správce front

Abecední seznam atributů správce front používaných při vyrovnávání pracovní zátěže klastru.

CLWLMRUC

Atribut správce front **CLWLMRUC** nastavuje počet naposledy vybraných kanálů. Algoritmus správy pracovní zátěže klastru používá produkt **CLWLMRUC** k omezení počtu aktivních odchozích kanálů klastru. Hodnota musí být v rozsahu 1-999 999 999 999.

Počáteční výchozí hodnota je 999 999 999 999.

CLWLUSEQ

Atribut správce front **CLWLUSEQ** určuje, zda je lokální instance fronty upřednostňována jako cíl před ostatními instancemi fronty v klastru. Tento atribut se použije, pokud je atribut fronty **CLWLUSEQ** nastaven na QMGR.

Atribut fronty **CLWLUSEQ** je platný pouze pro lokální fronty. Použije se pouze v případě, že je zpráva vložena aplikací nebo kanálem, který není kanálem klastru.

LOKÁLNÍ

Lokální fronta je jediným cílem fronty MQPUT. LOCAL je předvolba.

ANY

Produkt MQPUT zachází s lokální frontou stejně jako s jakoukoli jinou instancí fronty v klastru pro distribuci pracovní zátěže.

Související pojmy

[Algoritmus správy pracovní zátěže klastru](#)

Algoritmus správy pracovní zátěže používá atributy vyrovnávání pracovní zátěže a mnoho pravidel k výběru konečného místa určení pro zprávy vkládané do front klastru.

Související odkazy

[Vyrovnávání pracovní zátěže klastru-atributy kanálu](#)

Abecední seznam atributů kanálu používaných při vyrovnávání pracovní zátěže klastru.

Atributy vyrovnávání pracovní zátěže klastru-fronta

Abecední seznam atributů fronty používaných při vyrovnávání pracovní zátěže klastru.

“Atributy klastru dostupné v příkazech definice správce front” na stránce 130

Atributy klastru, které lze zadat v příkazech definice správce front.

Algoritmus správy pracovní zátěže klastru

Algoritmus správy pracovní zátěže používá atributy vyrovnávání pracovní zátěže a mnoho pravidel k výběru konečného místa určení pro zprávy vkládané do front klastru.

Algoritmus správy pracovní zátěže se provádí vždy, když je vyžadována volba místa určení:

- Používá se v bodě, kdy je otevřena fronta klastru, pomocí volby MQ00_BIND_ON_OPEN .
- Používá se pokaždé, když je zpráva vložena do fronty klastru, když je otevřena pomocí MQ00_BIND_NOT_FIXED.
- Používá se při každém spuštění nové skupiny zpráv, když se MQ00_BIND_ON_GROUP používá k otevření fronty klastru.
- Pro směrování hostitelů témat se používá při každém publikování zprávy do klastrovaného tématu. Pokud lokální správce front není hostitelem tohoto tématu, použije se algoritmus k výběru správce front hostitele pro směrování zprávy.

Následující oddíl popisuje algoritmus správy pracovní zátěže použitý při určování konečného místa určení pro zprávy vkládané do front klastru. Tato pravidla jsou ovlivněna nastavením použitým na následující atributy pro fronty, správce front a kanály:

Fronty	Správci front	Kanály
<ul style="list-style-type: none">• CLWLPRTY¹• CLWLRANK¹• CLWLUSEQ¹• PUT / PUB	<ul style="list-style-type: none">• CLWLMRUC• CLWLUSEQ¹	<ul style="list-style-type: none">• CLWLPRTY• CLWLRANK• CLWLWGHT• NETPRTY

Na počátku správce front sestaví seznam možných cílů ze dvou procedur:

- Shoda cíle `ObjectName` a `ObjectQmgrName` s definicemi aliasů správce front, které jsou sdíleny ve stejných klastrech jako správce front.
- Hledání jedinečných cest (tj. kanálů) ke správci front, který je hostitelem fronty s názvem `ObjectName`, a nachází se v jednom z klastrů, jejichž je správce front členem.

Algoritmus postupuje podle následujících pravidel, aby se vyloučila místa určení ze seznamu možných míst určení.

1. Vzdálené instance front nebo témat nebo vzdálené kanály CLUSRCVR, které nesdílejí klastr s lokálním správcem front, jsou eliminovány.
2. Je-li uveden název fronty nebo tématu, vzdálené kanály CLUSRCVR, které nejsou ve stejném klastru jako fronta nebo téma, jsou odstraněny.

Poznámka: Všechny zbývající fronty, témata a kanály v této fázi jsou zpřístupněny uživatelské proceduře pracovní zátěže klastru, pokud je konfigurována.

3. Všechny kanály pro správce front nebo aliasy správců front, které mají hodnotu CLWLRANK nižší než maximální počet všech zbývajících kanálů nebo aliasů správců front, jsou eliminovány.
4. Všechny fronty (nikoli aliasy správce front) s hodnotou CLWLRANK nižší než maximální hodnocení všech zbývajících front jsou eliminovány.

¹ Tento atribut se používá pouze při výběru klastrované fronty, nikoli při výběru tématu.

5. Pokud zůstává více než jedna instance aliasu fronty, tématu nebo správce front a je-li povoleno nějaké publikování, budou všechny zakázané položky odstraněny.
- Poznámka:** Pokud zůstanou zachovány pouze zakázané instance, budou úspěšné pouze operace inquire, všechny ostatní operace selžou s hodnotou MQRC_CLUSTER_PUT_INHIBITED.
6. Pokud při výběru fronty výsledná sada front obsahuje lokální instanci fronty, obvykle se použije lokální instance. Lokální instance fronty se používá, pokud je splněna jedna z následujících podmínek:
- Atribut použití fronty CLWLUSEQ je nastaven na hodnotu LOCAL.
 - Obě následující tvrzení jsou pravdivá:
 - Atribut použití fronty CLWLUSEQ je nastaven na QMGR.
 - Atribut use-queue správce front CLWLUSEQ je nastaven na hodnotu LOCAL.
 - Zpráva je přijímána prostřednictvím kanálu klastru, nikoli prostřednictvím lokální aplikace.
 - Pro lokálně definované fronty, které jsou definovány s CLWLUSEQ (ANY) nebo které dědí stejné nastavení od správce front, platí následující body v rámci širší sady podmínek, které platí:
 - Lokální fronta je zvolena na základě status lokálně definovaných kanálů CLUSRCVR ve stejném klastru jako fronta. Tento stav je porovnán se stavem kanálů CLUSSDR, které by zprávu přijaly do vzdáleně definovaných front se stejným názvem.

Například jeden CLUSRCVR je ve stejném klastru jako fronta. Tento CLUSRCVR má stav ZASTAVOVÁNÍ, zatímco ostatní fronty se stejným názvem v klastru mají stav SPUŠTĚNO nebo NEAKTIVNÍ. V tomto případě budou vybrány vzdálené kanály a lokální kanály CLUSSDR nebudou použity.
 - Lokální fronta je zvolena na základě number kanálů CLUSRCVR, v jakémkoli porovnání s kanály CLUSSDR stejného stavu, které by zprávu převezmou do vzdáleně definovaných front se stejným názvem.

Ve stejném klastru jako fronta jsou například čtyři kanály CLUSRCVR a jeden kanál CLUSSDR. Všechny kanály mají stejný stav NEAKTIVNÍ nebo SPUŠTĚNO. Proto si můžete vybrat z pěti kanálů a dvou instancí fronty. Čtyři pětiny (80 procent) zpráv jdou do lokální fronty.
7. Pokud zůstává více než jeden správce front, nejsou-li pozastaveni, budou odstraněny všechny pozastavené správce front.
8. Pokud zůstává ve frontě nebo tématu více než jedna vzdálená instance, budou zahrnuty všechny neaktivní nebo spuštěné kanály. V seznamu jsou uvedeny konstanty stavu:
- MQCHS_INACTIVE
 - MQCHS_RUNNING
9. Pokud nezůstane žádná vzdálená instance fronty nebo tématu, budou zahrnuty všechny kanály, které jsou ve stavu vazby, inicializace, spuštění nebo zastavení. V seznamu jsou uvedeny konstanty stavu:
- MQCHS_BINDING
 - MQCHS_INITIALIZING
 - MQCHS_STARTING (spouštění)
 - MQCHS_ZASTAVENÍ
10. Pokud nezůstane žádná vzdálená instance fronty nebo tématu, zahrnou se všechny kanály, které se zkouší znovu. Konstanta stavu je uvedena v seznamu:
- MQCHS_RETRYING
11. Pokud nezůstane žádná vzdálená instance fronty nebo tématu, zahrnou se všechny kanály v požadujícím, pozastaveném nebo zastaveném stavu. V seznamu jsou uvedeny konstanty stavu:
- MQCHS_VYŽÁDÁNÍ
 - MQCHS_PAUSED
 - MQCHS_STOPPED
 - MQCHS_SWITCHING

12. Pokud zůstává ve správci front více než jedna vzdálená instance fronty nebo tématu, budou vybrány kanály s nejvyšší hodnotou NETPRTY pro každého správce front.
13. Všechny zbývající kanály a aliasy správce front jiné než kanály a aliasy s nejvyšší prioritou CLWLPRTY jsou eliminovány. Pokud některý z aliasů správce front zůstane zachován, kanály pro správce front jsou uchovány.
14. Pokud je zvolena fronta:
 - Všechny fronty jiné než fronty s nejvyšší prioritou, CLWLPRTY, jsou eliminovány a kanály jsou zachovány.
15. Zbývající kanály jsou poté sníženy na maximální povolený počet naposledy použitých kanálů CLWLMRUC odstraněním kanálů s nejnižšími hodnotami MQWDR produktu MQWDR.DestSeqNumber.

Poznámka: Interní řídicí zprávy klastru se odesílají podle potřeby pomocí stejného algoritmu pracovní zátěže klastru.

Po výpočtu seznamu platných míst určení jsou zprávy vyrovnávány pracovní zátěží pomocí následující logiky:

- Pokud zůstává více než jedna vzdálená instance místa určení a všechny kanály do tohoto místa určení mají nastaven parametr CLWLWGHT na výchozí hodnotu 50, bude vybrán nejméně nedávno použitý kanál. To se přibližně rovná stylu round-robin vyvažování pracovní zátěže, když existuje více vzdálených instancí.
- Pokud zůstává více než jedna vzdálená instance místa určení a jeden nebo více kanálů pro tyto fronty má nastaveno jiné než výchozí nastavení CLWLWGHT (i když všechny mají odpovídající jinou než výchozí hodnotu), bude směrování záviset na relativních váhách každého kanálu a na celkovém počtu případů, kdy byl každý kanál dříve vybrán při odesílání zpráv.
- Při sledování distribuce zpráv pro jednu klastrovanou frontu s více instancemi se může zdát, že to vede k nevyvážené distribuci v rámci podmnožiny instancí fronty. Důvodem je skutečnost, že je vyváženo historické využití každého odesílacího kanálu klastru z tohoto správce front, nikoli pouze provoz zpráv pro tuto frontu. Pokud toto chování není žádoucí, proveďte jeden z následujících kroků:
 - Nastavte CLWLWGHT na 50 na všech přijímacích kanálech klastru, pokud je požadována i distribuce.
 - Nebo pokud je třeba určité instance fronty vážit jinak než jiné, definujte tyto fronty ve vyhrazeném klastru s definovanými vyhrazenými přijímacími kanály klastru. Tato akce izoluje vyrovnávání pracovní zátěže těchto front od ostatních v klastru.
- Historická data, která se používají k vyvážení kanálů, jsou resetována, pokud se změní jakékoli atributy pracovní zátěže klastru dostupných přijímacích kanálů klastru nebo se stav přijímacího kanálu klastru stane dostupným. Úprava atributů pracovní zátěže ručně definovaných odesílacích kanálů klastru neresetuje historická data.
- Při zvažování logiky uživatelské procedury pracovní zátěže klastru je vybrán kanál s nejnižším MQWDR.DestSeqFactor. Při každém výběru kanálu je tato hodnota zvýšena přibližně o 1000/CLWLWGHT. Pokud existuje více než jeden kanál s nejnižší hodnotou, jeden z kanálů s nejnižším MQWDR.DestSeqNumber .

Distribuce uživatelských zpráv není vždy přesná, protože administrace a údržba klastru způsobí, že zprávy budou proudit napříč kanály. Výsledkem je nerovnoměrná distribuce uživatelských zpráv, jejichž stabilizace může nějakou dobu trvat. Kvůli kombinaci zpráv administrace a uživatelských zpráv se při vyrovnávání pracovní zátěže nespolehají na přesnou distribuci zpráv.

Související odkazy

[Vyrovnávání pracovní zátěže klastru-atributy kanálu](#)

Abecední seznam atributů kanálu používaných při vyrovnávání pracovní zátěže klastru.

[Atributy vyrovnávání pracovní zátěže klastru-fronta](#)

Abecední seznam atributů fronty používaných při vyrovnávání pracovní zátěže klastru.

[Vyrovnávání pracovní zátěže klastru-atributy správce front](#)

Abecední seznam atributů správce front používaných při vyrovnávání pracovní zátěže klastru.

Asynchronní chování příkazů CLUSTER v systému z/OS

Vydavatel příkazu klastru v systému z/OS obdrží potvrzení, že byl příkaz odeslán, ale ne že byl úspěšně dokončen.

Pro REFRESH CLUSTER i RESET CLUSTER 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 na klastr byl úspěšně dokončen.

Jakékoli chyby jsou nahlášeny konzole z/OS na systému, kde je spuštěn inicializátor kanálu, nejsou odeslány vydavateli příkazu.

Asynchronní chování je na rozdíl od příkazů CHANNEL. Zpráva označující, že byl příkaz kanálu přijat, je vydána okamžitě. Později, když byl příkaz dokončen, je vydavateli příkazu odeslána zpráva, která označuje buď normální, nebo nestandardní dokončení.

Související pojmy

Vyrovňování pracovní zátěže v klastrech

Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směrována. K určení nejlepšího správce front, který má být použit, používá algoritmus správy pracovní zátěže klastru a řadu atributů specifických pro pracovní zátěž klastru.

Související úlohy

Kontrola dokončení asynchronních příkazů pro distribuované sítě

Související odkazy

Atributy klastru dostupné v příkazech definice kanálu

Atributy klastru, které lze zadat v příkazech definice kanálu.

Atributy klastru dostupné v příkazech definice fronty

Atributy klastru, které lze zadat v příkazech definice fronty.

Atributy klastru dostupné v příkazech definice správce front

Atributy klastru, které lze zadat v příkazech definice správce front.

DISPLAY CLUSQMGR

Pomocí příkazu DISPLAY CLUSQMGR můžete zobrazit informace o klastrech správců front v klastru.

Aktualizovat klastr

Zadejte příkaz REFRESH CLUSTER ze správce front, abyste vyřadili všechny lokálně uchovávané informace o klastru. Není pravděpodobné, že byste museli použít tento příkaz, s výjimkou výjimečných okolností.

RESET CLUSTER: Vynucené odebrání správce front z klastru

Příkaz **RESET CLUSTER** se používá k vynucovému odebrání správce front z klastru za výjimečných okolností.

SUSPEND QMGR, RESUME QMGR a klastry

Pomocí příkazů SUSPEND QMGR a RESUME QMGR můžete dočasně snížit aktivitu příchozího klastru pro tohoto správce front, například před provedením údržby tohoto správce front, a poté jej znovu uvést do původního stavu.

Programy kanálů

Tato část se zabývá různými typy programů kanálů (MCA), které jsou k dispozici pro použití na kanálech.

Názvy MCA jsou uvedeny v následujících tabulkách.

Tabulka 61. Programy kanálů pro systémy AIX, Linux, and Windows		
Název programu	Směr připojení	Komunikace
amqrmppa		Libovolný
runmqtsr	Příchozí	Libovolný

Tabulka 61. Programy kanálů pro systémy AIX, Linux, and Windows (pokračování)

Název programu	Směr připojení	Komunikace
amqcrs6a	Příchozí	LU 6.2
amqcrsta	Příchozí	TCP
runmqchl	Odchozí	Libovolný
runmqchi	Odchozí	Libovolný

runmqslr (Spustit modul listener IBM MQ), runmqchl (Spustit kanál IBM MQ) a runmqchi (Spustit inicializátor kanálu IBM MQ) jsou řídicí příkazy, které můžete zadat na příkazovém řádku.

amqcrsta je vyvolán pro kanály TCP na systémech AIX and Linux pomocí inetd, kde není spuštěn žádný modul listener.

amqcrs6a se vyvolá jako transakční program při použití LU6.2

IBM i Úlohy interkomunikace na systému IBM i

Následující úlohy jsou přidruženy k Interkomunikaci na systému IBM i. Názvy jsou obsaženy v následující tabulce.

Tabulka 62. Názvy a popisy úloh	
Jméno úlohy	Popis
AMQCLMAA	Listener bez podprocesů
AMQCRSTA	Úloha odpovíd. modulu bez podprocesů
AMQRMPPA	Úloha fondu kanálů
RUNMQCHI	Iniciátor kanálu
RUNMQCHL	Úloha kanálu
RUNMQLSR	Listener s podprocesy

IBM i Stavby kanálů na systému IBM i

Stavy kanálů jsou zobrazeny na panelu Práce s kanály.

Tabulka 63. Stavby kanálů na systému IBM i	
Název státu	Význam
SPOUŠTĚNÍ	Kanál je připraven zahájit vyjednávání s cílovým agentem MCA.
Vazba	Zavedení relace a počáteční výměny dat
Zpracování požadavků	Žadatelský kanál zahajující připojení
RUNNING	Přenos nebo připraveno k přenosu
Pozastaveno	Čeká se na zprávu-interval opakování
ZASTAVOVÁNÍ	Určení, zda se má opakovat nebo zastavit
Opakovaný pokus	Čeká se na další pokus o opakování
ZASTAVENO	Kanál byl zastaven kvůli chybě nebo kvůli zadání příkazu pro ukončení kanálu.
INACTIVE	Zpracování kanálu bylo ukončeno normálně nebo nebyl kanál nikdy spuštěn.
*Žádné	Žádný stav (pouze pro kanály připojení serveru)

Příklad: Plánování kanálu zpráv v systému AIX, Linux, and Windows

Tyto informace poskytují podrobný příklad toho, jak spojit dva správce front dohromady, aby mezi nimi mohly být odesílány zprávy.

Informace o této úloze

Ve všech příkladech jsou příkazy MQSC zobrazeny tak, jak by se objevily v souboru příkazů a jak by byly zapsány na příkazovém řádku. Tyto dvě metody vypadají stejně, ale chcete-li zadat příkaz na příkazovém řádku, musíte nejprve zadat `runmqscpro` výchozího správce front nebo `runmqsc qmname` kde `qmname` je název požadovaného správce front. Pak zadejte libovolný počet příkazů, jak je uvedeno v příkladech.

Alternativní metodou je vytvořit soubor obsahující tyto příkazy. Případné chyby v příkazech se pak snadno opraví. Pokud jste volali soubor `mqsc.in`, pak jej spusťte ve správci front `QMNAME` pomocí:

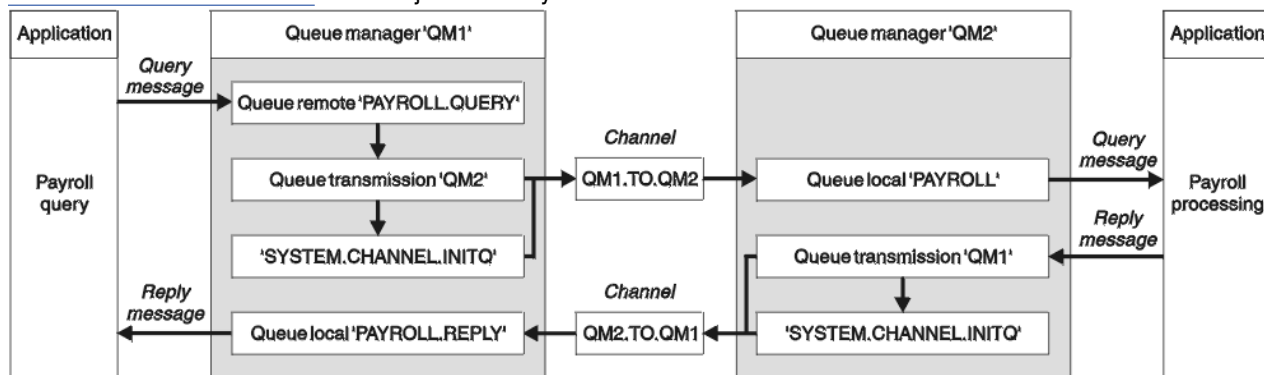
```
runmqsc QMNAME < mqsc.in > mqsc.out
```

Můžete ověřit příkazy v souboru před jeho spuštěním pomocí:

```
runmqsc -v QMNAME < mqsc.in > mqsc.out
```

Pro přenositelnost byste měli omezit délku řádků příkazů na 72 znaků. Chcete-li pokračovat přes více než jeden řádek, použijte znak zřetězení. V systému Windows použijte klávesu `Ctrl-z` k ukončení vstupu na příkazovém řádku. V systémech AIX and Linux použijte kombinaci kláves `Ctrl-d`. Případně použijte příkaz `end`.

Obrázek 7 na stránce 147 zobrazuje ukázkový scénář.



Obrázek 7. Příklad kanálu zpráv pro systémy AIX, Linux, and Windows

Příklad zahrnuje aplikaci dotazu na mzdy připojenou ke správci front QM1, která odesílá zprávy dotazu na mzdy do aplikace pro zpracování mezd spuštěné ve správci front QM2. Aplikace mzdového dotazu potřebuje odpovědi na své dotazy odeslané zpět do QM1. Zprávy dotazu na mzdy jsou odesílány z QM1 do QM2 na přijímacím kanálu odesilatele s názvem `QM1.TO.QM2` a zprávy s odpovědi jsou odesílány zpět z QM2 do QM1 na jiném kanálu příjemce s názvem `QM2.TO.QM1`. Oba tyto kanály jsou spuštěny, aby se spustily ihned po odeslání zprávy jinému správci front.

Aplikace mzdového dotazu vloží zprávu dotazu do vzdálené fronty "PAYROLL.QUERY" definovaný na QM1. Tato definice vzdálené fronty se interpretuje jako lokální fronta "PAYROLL" na QM2. Kromě toho aplikace mzdového dotazu uvádí, že odpověď na dotaz se odešle do lokální fronty "PAYROLL.REPLY" na QM1. Aplikace zpracování mezd získává zprávy z lokální fronty "PAYROLL" na QM2 a odesílá odpovědi všude, kde jsou požadovány; v tomto případě lokální fronta "PAYROLL.REPLY" na QM1.

V ukázkových definicích pro TCP/IP má QM1 adresu hostitele 192.0.2.0 a naslouchá na portu 1411 a QM2 má adresu hostitele 192.0.2.1 a naslouchá na portu 1412. Příklad předpokládá, že jsou již v systému definovány a jsou k dispozici pro použití.

Definice objektů, které je třeba vytvořit v systému QM1 , jsou:

- Definice vzdálené fronty, PAYROLL.QUERY
- Definice přenosové fronty, QM2 (výchozí = název vzdáleného správce front)
- Definice odesílacího kanálu, QM1.TO.QM2
- Definice přijímacího kanálu, QM2.TO.QM1
- Definice fronty pro odpověď, PAYROLL.REPLY

Definice objektů, které je třeba vytvořit na serveru QM2 , jsou:

- Definice lokální fronty, PAYROLL
- Definice přenosové fronty, QM1 (výchozí = název vzdáleného správce front)
- Definice kanálu odesilatele, QM2.TO.QM1
- Definice přijímacího kanálu, QM1.TO.QM2

Podrobnosti o připojení jsou zadány v atributu CONNAME definic kanálu odesilatele.

Diagram uspořádání můžete vidět v souboru [Obrázek 7](#) na stránce 147.

Postup

Viz:

- “[Nastavení příkladu kanálu zpráv pro AIX, Linux, and Windows](#)” na stránce 148 pro podrobnosti o nastavení kanálů zpráv
- “[Spuštění a rozbalení příkladu pro AIX, Linux, and Windows](#)” na stránce 150 pro návrhy, jak můžete používat jiné produkty, například CICS, a jak můžete připojit více aplikací a uživatelských procedur.

ALW

Nastavení příkladu kanálu zpráv pro AIX, Linux, and Windows

Tyto definice objektů umožňují aplikacím připojeným ke správci front QM1 odesílat zprávy požadavků do fronty s názvem PAYROLL v systému QM2a přijímat odpovědi ve frontě s názvem PAYROLL.REPLY v systému QM1a umožňuje aplikacím připojeným ke správci front QM2 načítat zprávy požadavků z lokální fronty s názvem PAYROLL a vkládat odpovědi na tyto zprávy požadavků do fronty s názvem PAYROLL.REPLY ve správci front QM1.

Informace o této úloze

Všechny definice objektů byly poskytnuty s atributy DESCR a REPLACE. Ostatní dodané atributy jsou minimem požadovaným k tomu, aby příklady fungovaly. Atributy, které nejsou zadány, mají výchozí hodnoty pro správce front QM1 a QM2.

Nemusíte poskytovat definici vzdálené fronty, abyste umožnili vrácení odpovědi do QM1. Deskriptor zprávy načtené z lokální fronty PAYROLL obsahuje názvy fronty pro odpověď i správce front pro odpověď. Pokud tedy může produkt QM2 interpretovat název správce front pro odpověď na název přenosové fronty ve správci front QM2, může být odeslána zpráva odpovědi. V tomto příkladu je název správce front pro odpověď QM1 , a proto správce front QM2 vyžaduje přenosovou frontu se stejným názvem.

Procedura

- Spusťte následující příkazy ve správci front QM1:
 - a) Nastavte definici vzdálené fronty:

```
DEFINE QREMOTE(PAYROLL.QUERY) DESCR('Remote queue for QM2') REPLACE +  
PUT(ENABLED) XMITQ(QM2) RNAME(PAYROLL) RQNAME(QM2)
```

Poznámka: Definice vzdálené fronty není fyzickou frontou, ale prostředkem pro směrování zpráv do přenosové fronty QM2, aby je bylo možné odeslat správci front QM2.

b) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QM2) DESCR('Transmission queue to QM2') REPLACE +
USAGE(XMITQ) PUT(ENABLED) GET(ENABLED) TRIGGER TRIGTYPE(FIRST) +
INITQ(SYSTEM.CHANNEL.INITQ) PROCESS(QM1.TO.QM2.PROCESS)
```

Když je do této přenosové fronty vložena první zpráva, odešle se do inicializační fronty SYSTEM.CHANNEL.INITQ. Inicializátor kanálu získá zprávu z inicializační fronty a spustí kanál identifikovaný v uvedeném procesu.

c) Nastavte definici odesílacího kanálu:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) +
REPLACE DESCR('Sender channel to QM2') XMITQ(QM2) +
CONNAME('192.0.2.1(1412)')
```

d) Nastavte definici přijímacího kanálu:

```
DEFINE CHANNEL(QM2.TO.QM1) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QM2')
```

e) Nastavit definici odpovědi do fronty:

```
DEFINE QLOCAL(PAYROLL.REPLY) REPLACE PUT(ENABLED) GET(ENABLED) +
DESCR('Reply queue for replies to query messages sent to QM2')
```

Fronta pro odpověď je definována jako PUT (ENABLED). Tím je zajištěno, že zprávy s odpovědí mohou být vloženy do fronty. Pokud odpovědi nelze vložit do fronty pro odpovědi, jsou odeslány do fronty nedoručených zpráv v systému QM1, nebo pokud tato fronta není k dispozici, zůstávají v přenosové frontě QM1 ve správci front QM2. Fronta byla definována jako GET (ENABLED), aby umožnila načtení zpráv odpovědi.

- Spusťte následující příkazy ve správci front QM2:

a) Nastavte definici lokální fronty:

```
DEFINE QLOCAL(PAYROLL) REPLACE PUT(ENABLED) GET(ENABLED) +
DESCR('Local queue for QM1 payroll details')
```

Tato fronta je definována jako PUT (ENABLED) a GET (ENABLED) ze stejné příčiny jako definice fronty pro odpověď ve správci front QM1.

b) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QM1) DESCR('Transmission queue to QM1') REPLACE +
USAGE(XMITQ) PUT(ENABLED) GET(ENABLED) TRIGGER TRIGTYPE(FIRST) +
INITQ(SYSTEM.CHANNEL.INITQ) PROCESS(QM2.TO.QM1.PROCESS)
```

Když je do této přenosové fronty vložena první zpráva, odešle se do inicializační fronty SYSTEM.CHANNEL.INITQ. Inicializátor kanálu získá zprávu z inicializační fronty a spustí kanál identifikovaný v uvedeném procesu.

c) Nastavte definici odesílacího kanálu:

```
DEFINE CHANNEL(QM2.TO.QM1) CHLTYPE(SDR) TRPTYPE(TCP) +
REPLACE DESCR('Sender channel to QM1') XMITQ(QM1) +
CONNAME('192.0.2.0(1411)')
```

d) Nastavte definici přijímacího kanálu:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QM1')
```

Spuštění a rozbalení příkladu pro AIX, Linux, and Windows

Informace o spuštění inicializátoru kanálu a modulu listener a návrhy na rozšíření tohoto scénáře.

Informace o této úloze

Po vytvoření těchto definic je třeba provést následující akce:

- Spusťte iniciátor kanálu pro každého správce front.
- Spusťte modul listener pro každého správce front.

Můžete také rozbalit příklad.

Postup

1. Spusťte inicializátor kanálu a modul listener.

Viz [Nastavení komunikace pro systémy Windows](#) a [Nastavení komunikace na systémech AIX and Linux](#).

2. Tento příklad můžete rozšířit pomocí:

- Použití komunikací LU 6.2 pro propojení se systémy CICS a zpracování transakcí.
- Přidáním dalších definic front, procesů a kanálů umožníte ostatním aplikacím odesílat zprávy mezi těmito dvěma správci front.
- Přidání uživatelských programů na kanály, které umožní šifrování odkazů, kontrolu zabezpečení nebo další zpracování zpráv.
- Pomocí aliasů správců front a aliasů front pro odpovědi můžete lépe porozumět tomu, jak je lze použít v organizaci sítě správců front.

Příklad: Plánování kanálu zpráv v systému IBM i

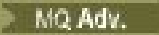

Podrobný příklad toho, jak spojit dva správce front IBM i dohromady, aby mezi nimi mohly být odesílány zprávy. Příklad zahrnuje aplikaci dotazu na mzdy připojenou ke správci front QM1, která odesílá zprávy dotazu na mzdy do aplikace pro zpracování mezd spuštěné ve správci front QM2. Aplikace mzdového dotazu potřebuje odpovědi na své dotazy odeslané zpět do QM1.

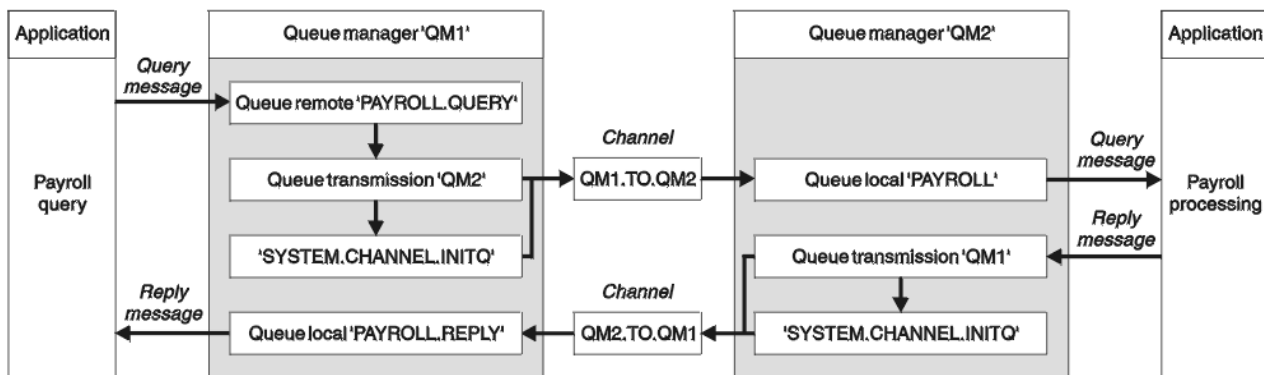
Informace o této úloze

Příklad ilustruje přípravu potřebné k tomu, aby aplikace používající správce front QM1 mohla vkládat zprávy do fronty ve správci front QM2. Aplikace spuštěná na serveru QM2 může tyto zprávy načíst a odeslat odpovědi do fronty odpovědí na serveru QM1.

Příklad ilustruje použití připojení TCP/IP. Příklad předpokládá, že se mají spustit kanály, které se spustí, když první zpráva dorazí do přenosové fronty, kterou obsluhují.

Tento příklad používá SYSTEM.CHANNEL.INITQ jako inicializační fronta. Tato fronta je již definována produktem IBM MQ. Můžete použít jinou inicializační frontu, ale musíte ji definovat sami, spustit novou instanci inicializátoru kanálu pomocí příkazu STRMQMCHLI a poskytnout jí název inicializační fronty. Další informace o spuštění kanálů naleznete v tématu [Spouštěcí kanály](#).

Poznámka:   Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Viz [Definování Aspera gateway připojení na Linux nebo Windows](#).



Obrázek 8. Příklad kanálu zpráv pro IBM MQ for IBM i

Zprávy dotazu na mzdy jsou odesílány z QM1 do QM2 na přijímacím kanálu odesilatele s názvem QM1.TO.QM2 a zprávy s odpovědí jsou odesílány zpět z QM2 do QM1 na jiném kanálu příjemce s názvem QM2.TO.QM1. Oba tyto kanály jsou spuštěny, aby se spustily ihned po odeslání zprávy jinému správci front.

Aplikace mzdového dotazu vloží zprávu dotazu do vzdálené fronty "PAYROLL.QUERY" definovaný na QM1. Tato definice vzdálené fronty se interpretuje jako lokální fronta "PAYROLL" na QM2. Kromě toho aplikace mzdového dotazu uvádí, že odpověď na dotaz se odešle do lokální fronty "PAYROLL.REPLY" na QM1. Aplikace zpracování mezd získává zprávy z lokální fronty "PAYROLL" na QM2 a odesílá odpovědi všude, kde jsou požadovány; v tomto případě lokální fronta "PAYROLL.REPLY" na QM1.

Předpokládá se, že oba správci front jsou spuštěni v systému IBM i. V ukázkových definicích má QM1 adresu hostitele 192.0.2.0 a naslouchá na portu 1411. QM2 má adresu hostitele 192.0.2.1 a naslouchá na portu 1412. Příklad předpokládá, že tito správci front jsou již ve vašem systému IBM i definováni a jsou k dispozici pro použití.

Definice objektů, které je třeba vytvořit v systému QM1, jsou:

- Definice vzdálené fronty, PAYROLL.QUERY
- Definice přenosové fronty, QM2 (výchozí = název vzdáleného správce front)
- Definice odesílacího kanálu, QM1.TO.QM2
- Definice přijímacího kanálu, QM2.TO.QM1
- Definice fronty pro odpověď, PAYROLL.REPLY

Definice objektů, které je třeba vytvořit na serveru QM2, jsou:

- Definice lokální fronty, PAYROLL
- Definice přenosové fronty, QM1 (výchozí = název vzdáleného správce front)
- Definice kanálu odesilatele, QM2.TO.QM1
- Definice přijímacího kanálu, QM1.TO.QM2

Podrobnosti o připojení jsou zadány v atributu CONNAME definic kanálu odesilatele.

Diagram uspořádání můžete vidět v souboru [Obrázek 8 na stránce 151](#).

Postup

Viz:

- [“Nastavení agenta kanálu zpráv v systému IBM i” na stránce 152](#) pro podrobnosti o nastavení kanálů zpráv
- [“Spuštění a rozbalení příkladu pro IBM i” na stránce 154](#) pro návrhy, jak připojit více aplikací a uživatelských procedur.

Nastavení agenta kanálu zpráv v systému IBM i

Následující definice objektů umožňují aplikacím připojeným ke správci front QM1 odesílat zprávy požadavků do fronty s názvem PAYROLL na QM2, přijímat odpovědi ve frontě s názvem PAYROLL.REPLY v systému QM1 umožňuje aplikacím připojeným ke správci front QM2 načítat zprávy požadavků z lokální fronty s názvem PAYROLL a vkládat odpovědi na tyto zprávy požadavků do fronty s názvem PAYROLL.REPLY ve správci front QM1.

Informace o této úloze

Všechny definice objektů byly poskytnuty s atributy TEXT. Ostatní dodané atributy jsou minimem požadovaným k tomu, aby příklad fungoval. Atributy, které nejsou zadány, mají výchozí hodnoty pro správce front QM1 a QM2.

Nemusíte poskytovat definici vzdálené fronty, abyste umožnili vrácení odpovědí do QM1. Deskriptor zprávy načtené z lokální fronty PAYROLL obsahuje názvy fronty pro odpověď i správce front pro odpověď. Pokud tedy může produkt QM2 interpretovat název správce front pro odpověď na název přenosové fronty ve správci front QM2, může být odeslána zpráva odpovědi. V tomto příkladu je název správce front pro odpověď QM1, a proto správce front QM2 vyžaduje přenosovou frontu se stejným názvem.

Procedura

- Spusťte následující příkazy ve správci front QM1:
 - Nastavte definici vzdálené fronty pomocí příkazu CRTMQMQ s následujícími atributy:

QNAME	'PAYROLL.QUERY'
QTYPE	*RMT
TEXT	'Vzdálená fronta pro QM2'
PUTENBL	*YES
Název produktu TMQNAME	'QM2' (výchozí = název vzdáleného správce front)
RMTQNAME	'MZDY'
RMTMQMNAME	'QM2'

Poznámka: Definice vzdálené fronty není fyzickou frontou, ale prostředkem pro směrování zpráv do přenosové fronty QM2, aby je bylo možné odeslat správci front QM2.

- Nastavte definici přenosové fronty pomocí příkazu CRTMQMQ s následujícími atributy:

QNAME	QM2
QTYPE	*LCL
TEXT	'Přenosová fronta do QM2'
USAGE	*TMQ
PUTENBL	*YES
GETENBL	*YES
TRGENBL	*YES
TRGTYPE-typ	*PRVNÍ
INITQNAME	SYSTEM.CHANNEL.INITQ
TRIGDATA	QM1.TO.QM2

Když je do této přenosové fronty vložena první zpráva, odešle se do inicializační fronty SYSTEM.CHANNEL.INITQ. Inicializátor kanálu získá zprávu z inicializační fronty a spustí kanál identifikovaný v uvedeném procesu.

- c) Nastavte definici odesílacího kanálu pomocí příkazu CRTMQCHL s následujícími atributy:

CHLNAME	QM1.TO.QM2
CHLTYPE	*SDR
TRPTYPE	*TCP (TCP)
TEXT	'Kanál odesilatele do QM2'
Název produktu TMQNAME	QM2
CONNNAME	'192.0.2.1(1412)'

- d) Nastavte definici přijímacího kanálu pomocí příkazu CRTMQCHL s následujícími atributy:

CHLNAME	QM2.TO.QM1
CHLTYPE	*RCVR
TRPTYPE	*TCP (TCP)
TEXT	'Přijímací kanál z QM2'

- e) Nastavte definici fronty pro odpověď pomocí příkazu CRTMQMQ s následujícími atributy:

QNAME	PAYROLL.REPLY
QTYPE	*LCL
TEXT	'Fronta odpovědí pro odpovědi na dotazové zprávy odeslané na QM2'
PUTENBL	*YES
GETENBL	*YES

Fronta pro odpověď je definována jako PUT (ENABLED). Tato definice zajišťuje, že zprávy odpovědí mohou být vloženy do fronty. Pokud odpovědi nelze vložit do fronty pro odpovědi, jsou odeslány do fronty nedoručených zpráv v systému QM1, nebo pokud tato fronta není k dispozici, zůstávají v přenosové frontě QM1 ve správci front QM2. Fronta byla definována jako GET (ENABLED), aby umožnila načtení zpráv odpovědi.

- Spusťte následující příkazy ve správci front QM2:

- a) Nastavte definici lokální fronty pomocí příkazu CRTMQMQ s následujícími atributy:

QNAME	Mzdy
QTYPE	*LCL
TEXT	'Podrobnosti mezd lokální fronty pro QM1 '
PUTENBL	*YES
GETENBL	*YES

Tato fronta je definována jako PUT (ENABLED) a GET (ENABLED) ze stejné příčiny jako definice fronty pro odpověď ve správci front QM1.

- b) Nastavte definici přenosové fronty pomocí příkazu CRTMQMQ s následujícími atributy:

QNAME	QM1
QTYPE	*LCL
TEXT	'Přenosová fronta do QM1'

USAGE	*TMQ
PUTENBL	*YES
GETENBL	*YES
TRGENBL	*YES
TRGTYPE-typ	*PRVNÍ
INITQNAME	SYSTEM.CHANNEL.INITQ
TRIGDATA	QM2.TO.QM1

Když je do této přenosové fronty vložena první zpráva, odešle se do inicializační fronty SYSTEM.CHANNEL.INITQ. Inicializátor kanálu získá zprávu z inicializační fronty a spustí kanál identifikovaný v datech spouštěče.

c) Nastavte definici odesílacího kanálu pomocí příkazu CRTMQMCHL s následujícími atributy:

CHLNAME	QM2.TO.QM1
CHLTYPE	*SDR
TRPTYPE	*TCP (TCP)
TEXT	'Kanál odesílatele do QM1'
Název produktu	QM1
TMQNAME	
CONNNAME	'192.0.2.0(1411)'

d) Nastavte definici přijímacího kanálu pomocí příkazu CRTMQMCHL s následujícími atributy:

CHLNAME	QM1.TO.QM2
CHLTYPE	*RCVR
TRPTYPE	*TCP (TCP)
TEXT	'Přijímací kanál z QM1'

IBM i

Spuštění a rozbalení příkladu pro IBM i

Informace o spuštění inicializátoru kanálu a modulu listener a návrhy na rozšíření tohoto scénáře.

Informace o této úloze

Po vytvoření těchto definic je třeba provést následující akce:

- Spusťte iniciátor kanálu pro každého správce front.
- Spusťte modul listener pro každého správce front.

Aplikace si pak mohou vzájemně posílat zprávy. Kanály jsou spuštěny první zprávou přicházející do každé přenosové fronty, takže nemusíte zadat příkaz STRMQMCHL.

Můžete také rozbalit příklad.

Postup

1. Spusťte inicializátor kanálu a modul listener.

Podrobnosti o spuštění inicializátoru kanálu a modulu listener naleznete v tématu [Monitorování a řízení kanálů v systému IBM i](#).

2. Tento příklad můžete rozšířit pomocí:

- Přidáním dalších definic front a kanálů umožníte ostatním aplikacím odesílat zprávy mezi těmito dvěma správci front.
- Přidání uživatelských programů na kanálech, které umožní šifrování odkazů, kontrolu zabezpečení nebo další zpracování zpráv.
- Pomocí aliasů správců front a aliasů front pro odpovědi můžete lépe porozumět tomu, jak lze tyto objekty používat v organizaci sítě správců front.

Verze tohoto příkladu, která používá příkazy MQSC, viz [“Příklad: Plánování kanálu zpráv v systému z/OS”](#) na stránce 155.



z/OS Příklad: Plánování kanálu zpráv v systému z/OS

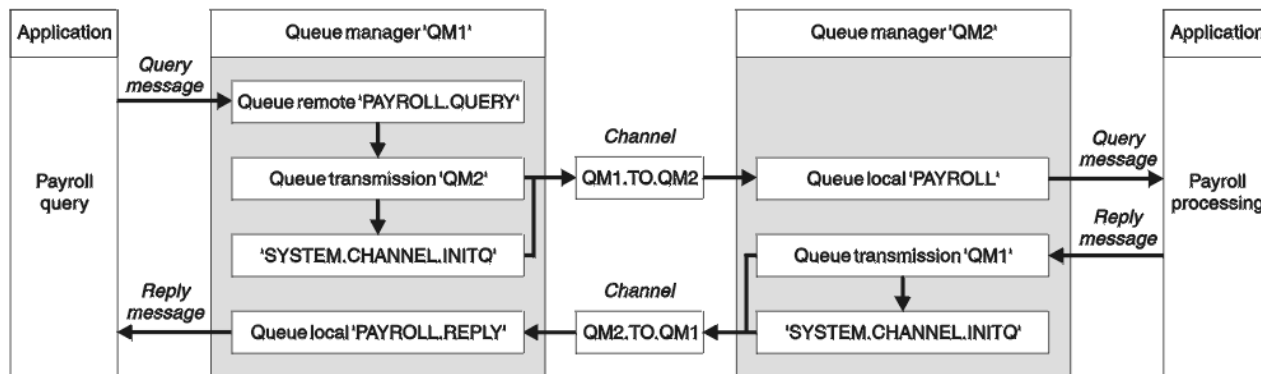
Jak spojit správce front systému z/OS nebo MVS dohromady, aby mezi nimi mohly být odesílány zprávy. Tento příklad zahrnuje aplikaci mzdového dotazu připojenou ke správci front QM1, která odesílá zprávy mzdového dotazu do aplikace zpracování mezd spuštěné ve správci front QM2. Aplikace mzdového dotazu potřebuje odpovědi na své dotazy odeslané zpět do QM1.

Informace o této úloze

Příklad ilustruje přípravy potřebné k tomu, aby aplikace používající správce front QM1 mohla vkládat zprávy do fronty ve správci front QM2. Aplikace spuštěná na serveru QM2 může tyto zprávy načíst a odeslat odpovědi do fronty odpovědí na serveru QM1.

Příklad ilustruje použití připojení TCP/IP i LU 6.2. Příklad předpokládá, že se mají spustit kanály, které se spustí, když první zpráva dorazí do přenosové fronty, kterou obsluhují.

Poznámka:   Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Viz [Definování Aspera gateway připojení na Linux nebo Windows](#).



Obrázek 9. První příklad pro IBM MQ for z/OS

Zprávy dotazu na mzdy jsou odesílány z QM1 do QM2 na přijímacím kanálu odesilatele s názvem QM1.TO.QM2 a zprávy s odpovědi jsou odesílány zpět z QM2 do QM1 na jiném kanálu příjemce s názvem QM2.TO.QM1. Oba tyto kanály jsou spuštěny, aby se spustily ihned po odeslání zprávy jinému správci front.

Aplikace mzdového dotazu vloží zprávu dotazu do vzdálené fronty "PAYROLL.QUERY" definovaný na QM1. Tato definice vzdálené fronty se interpretuje jako lokální fronta "PAYROLL" na QM2. Kromě toho aplikace mzdového dotazu uvádí, že odpověď na dotaz se odešle do lokální fronty "PAYROLL.REPLY" na QM1. Aplikace zpracování mezd získává zprávy z lokální fronty "PAYROLL" na QM2 a odesílá odpovědi všude, kde jsou požadovány; v tomto případě lokální fronta "PAYROLL.REPLY" na QM1.

Předpokládá se, že oba správci front jsou spuštěni v systému z/OS. V ukázkových definicích pro TCP/IP má QM1 adresu hostitele 192.0.2.0 a naslouchá na portu 1411 a QM2 má adresu hostitele 192.0.2.1 a naslouchá na portu 1412. V definicích pro LU 6.2 naslouchá produkt QM1 na symbolickém luname s názvem LUNAME1 a QM2 naslouchá na symbolickém luname s názvem LUNAME2. Příklad předpokládá,

že tyto názvy jsou již definovány ve vašem systému z/OS a jsou k dispozici pro použití. Chcete-li je definovat, viz [“Příklad: nastavení komunikace mezi platformami IBM MQ na systému z/OS”](#) na stránce 44.

Definice objektů, které je třeba vytvořit v systému QM1 , jsou:

- Definice vzdálené fronty, PAYROLL.QUERY
- Definice přenosové fronty, QM2 (výchozí = název vzdáleného správce front)
- Definice odesílacího kanálu, QM1.TO.QM2
- Definice přijímacího kanálu, QM2.TO.QM1
- Definice fronty pro odpověď, PAYROLL.REPLY

Definice objektů, které je třeba vytvořit na serveru QM2 , jsou:

- Definice lokální fronty, PAYROLL
- Definice přenosové fronty, QM1 (výchozí = název vzdáleného správce front)
- Definice kanálu odesilatele, QM2.TO.QM1
- Definice přijímacího kanálu, QM1.TO.QM2

Příklad předpokládá, že všechny položky SYSTEM.COMMAND.* a SYSTEM.CHANNEL.* fronty potřebné ke spuštění DQM byly definovány tak, jak je uvedeno v dodaných ukázkových definicích **CSQ4INSG** a **CSQ4INSX**.

Podrobnosti o připojení jsou zadány v atributu CONNAME definic kanálu odesilatele.

Diagram uspořádání můžete vidět v souboru [Obrázek 9](#) na stránce 155.

Postup

Viz:

- [“Nastavení agenta kanálu zpráv v systému z/OS”](#) na stránce 156 pro podrobnosti o nastavení kanálů zpráv
- [“Spuštění a rozbalení příkladu pro z/OS”](#) na stránce 158 pro návrhy, jak připojit více aplikací a uživatelských procedur.

z/OS

Nastavení agenta kanálu zpráv v systému z/OS

Následující definice objektů umožňují aplikacím připojeným ke správci front QM1 odesílat zprávy požadavků do fronty s názvem PAYROLL na QM2 a také aplikacím umožňuje přijímat odpovědi ve frontě s názvem PAYROLL.REPLY na QM1. Definice také umožňují aplikacím připojeným ke správci front QM2 načítat zprávy požadavků z lokální fronty s názvem PAYROLL a vkládat odpovědi na tyto zprávy požadavků do fronty s názvem PAYROLL.REPLY ve správci front QM1.

Informace o této úloze

Všechny definice objektů byly poskytnuty s atributy DESCR a REPLACE a jsou minimem nutným pro provedení práce na příkladu. Atributy, které nejsou zadány, mají výchozí hodnoty pro správce front QM1 a QM2.

Nemusíte poskytovat definici vzdálené fronty, abyste umožnili vrácení odpovědi do QM1. Deskriptor zprávy načtené z lokální fronty PAYROLL obsahuje názvy fronty pro odpověď i správce front pro odpověď. Pokud tedy může produkt QM2 interpretovat název správce front pro odpověď na název přenosové fronty ve správci front QM2, může být odeslána zpráva odpovědi. V tomto příkladu je název správce front pro odpověď QM1 , a proto správce front QM2 vyžaduje přenosovou frontu se stejným názvem.

Procedura

- Spusťte následující příkazy ve správci front QM1:
 - a) Nastavte definici vzdálené fronty:

```
DEFINE QREMOTE(PAYROLL.QUERY) DESCR('Remote queue for QM2') REPLACE +
PUT(ENABLED) XMITQ(QM2) RNAME(PAYROLL) RQMNAME(QM2)
```

Poznámka: Definice vzdálené fronty není fyzickou frontou, ale prostředkem pro směrování zpráv do přenosové fronty QM2, aby je bylo možné odeslat správci front QM2.

b) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QM2) DESCR('Transmission queue to QM2') REPLACE +
USAGE(XMITQ) PUT(ENABLED) GET(ENABLED) TRIGGER TRIGTYPE(FIRST) +
TRIGDATA(QM1.TO.QM2) INITQ(SYSTEM.CHANNEL.INITQ)
```

Když je do této přenosové fronty vložena první zpráva, odešle se do inicializační fronty SYSTEM.CHANNEL.INITQ. Inicializátor kanálu získá zprávu z inicializační fronty a spustí kanál identifikovaný v datech spouštěče. Inicializátor kanálu může získat zprávy spouštěče pouze ze systému SYSTEM.CHANNEL.INITQ, proto jako inicializační frontu nepoužívejte žádnou jinou frontu.

c) Nastavte definici odesílacího kanálu:

Pro připojení TCP/IP:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) +
REPLACE DESCR('Sender channel to QM2') XMITQ(QM2) +
CONNAME('192.0.2.1(1412)')
```

Pro připojení LU 6.2 :

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(LU62) +
REPLACE DESCR('Sender channel to QM2') XMITQ(QM2) +
CONNAME('LUNAME2')
```

d) Nastavte definici přijímacího kanálu:

Pro připojení TCP/IP:

```
DEFINE CHANNEL(QM2.TO.QM1) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QM2')
```

Pro připojení LU 6.2 :

```
DEFINE CHANNEL(QM2.TO.QM1) CHLTYPE(RCVR) TRPTYPE(LU62) +
REPLACE DESCR('Receiver channel from QM2')
```

e) Nastavte definici fronty pro odpověď:

```
DEFINE QLOCAL(PAYROLL.REPLY) REPLACE PUT(ENABLED) GET(ENABLED) +
DESCR('Reply queue for replies to query messages sent to QM2')
```

Fronta pro odpověď je definována jako PUT (ENABLED), což zajišťuje, že zprávy odpovědi mohou být vloženy do fronty. Pokud odpovědi nelze vložit do fronty pro odpovědi, jsou odeslány do fronty nedoručených zpráv v systému QM1, nebo pokud tato fronta není k dispozici, zůstávají v přenosové frontě QM1 ve správci front QM2. Fronta byla definována jako GET (ENABLED), aby umožnila načtení zpráv odpovědi.

• Spusťte následující příkazy ve správci front QM2:

a) Nastavte definici lokální fronty:

```
DEFINE QLOCAL(PAYROLL) REPLACE PUT(ENABLED) GET(ENABLED) +
DESCR('Local queue for QM1 payroll details')
```

Tato fronta je definována jako PUT (ENABLED) a GET (ENABLED) ze stejné příčiny jako definice fronty pro odpověď ve správci front QM1.

b) Nastavte definici přenosové fronty:

```
DEFINE QLOCAL(QM1) DESCR('Transmission queue to QM1') REPLACE +
USAGE(XMITQ) PUT(ENABLED) GET(ENABLED) TRIGGER TRIGTYPE(FIRST) +
TRIGDATA(QM2.TO.QM1) INITQ(SYSTEM.CHANNEL.INITQ)
```

Když je do této přenosové fronty vložena první zpráva, odešle se do inicializační fronty SYSTEM.CHANNEL.INITQ. Inicializátor kanálu získá zprávu z inicializační fronty a spustí kanál identifikovaný v datech spouštěče. Inicializátor kanálu může získat zprávy spouštěče pouze ze systému SYSTEM.CHANNEL.INITQ, takže jako inicializační frontu nepoužívejte žádnou jinou frontu.

c) Nastavte definici odesílacího kanálu:

Pro připojení TCP/IP:

```
DEFINE CHANNEL(QM2.TO.QM1) CHLTYPE(SDR) TRPTYPE(TCP) +
REPLACE DESCR('Sender channel to QM1') XMITQ(QM1) +
CONNAME('192.0.2.0(1411)')
```

Pro připojení LU 6.2 :

```
DEFINE CHANNEL(QM2.TO.QM1) CHLTYPE(SDR) TRPTYPE(LU62) +
REPLACE DESCR('Sender channel to QM1') XMITQ(QM1) +
CONNAME('LUNAME1')
```

d) Nastavte definici přijímacího kanálu:

Pro připojení TCP/IP:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QM1')
```

Pro připojení LU 6.2 :

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(LU62) +
REPLACE DESCR('Receiver channel from QM1')
```

z/OS

Spuštění a rozbalení příkladu pro z/OS

Informace o spuštění inicializátoru kanálu a modulu listener a návrhy na rozšíření v tomto příkladu.

Informace o této úloze

Po vytvoření těchto definic je třeba provést následující akce:

- Spusťte iniciátor kanálu pro každého správce front.
- Spusťte modul listener pro každého správce front.

Aplikace si pak mohou vzájemně posílat zprávy. Vzhledem k tomu, že kanály jsou spouštěny při příjmu první zprávy v každé přenosové frontě, není nutné zadat příkaz START CHANNEL MQSC.

Můžete také rozbalit příklad.

Postup

1. Spusťte inicializátor kanálu a modul listener.

Podrobnosti o spuštění inicializátoru a modulu listener kanálu naleznete v tématu [Spuštění inicializátoru kanálu](#) a [Spuštění modulu listener kanálu](#).

2. Tento příklad můžete rozšířit pomocí:

- Přidáním dalších front a definic kanálů umožníte ostatním aplikacím odesílat zprávy mezi těmito dvěma správci front.
- Přidání uživatelských programů na kanálech, které umožní šifrování odkazů, kontrolu zabezpečení nebo další zpracování zpráv.
- Pomocí aliasů správců front a aliasů front pro odpovědi můžete lépe porozumět tomu, jak lze tyto aliasy používat v organizaci sítě správců front.

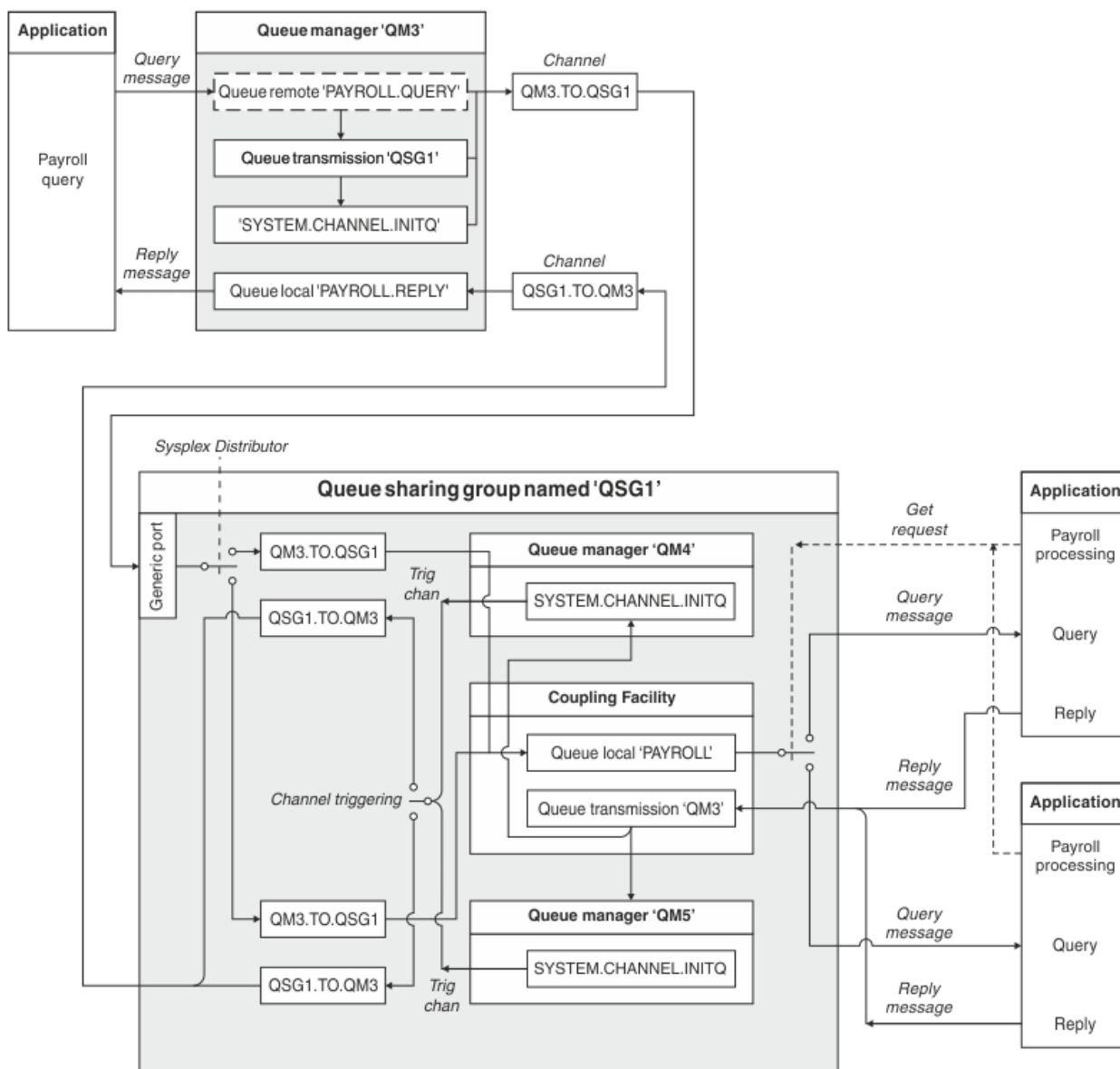
Příklad: Plánování kanálu zpráv pro z/OS pomocí skupin sdílení front

Tento příklad ilustruje přípravy potřebné k tomu, aby aplikace používající správce front QM3 mohla vložit zprávu do fronty ve skupině sdílení front, která má členy fronty QM4 a QM5, a také zobrazuje příkazy IBM MQ (MQSC), které můžete použít v produktu IBM MQ for z/OS pro distribuované fronty se skupinami sdílení front.

Informace o této úloze

Před tímto pokusem se ujistěte, že jste obeznámeni s příkladem v souboru [“Příklad: Plánování kanálu zpráv v systému z/OS”](#) na stránce 155 . Tento příklad rozbalí scénář dotazu na mzdu tohoto příkladu, aby ukázal, jak přidat vyšší dostupnost zpracování dotazu přidáním dalších obsluhujících aplikací pro obsluhu sdílené fronty.

Aplikace mzdového dotazu je nyní připojena ke správci front QM3 a vkládá dotaz do vzdálené fronty 'PAYROLL QUERY' definované v QM3. Tato definice vzdálené fronty se interpretuje jako sdílená fronta 'PAYROLL', jejímž hostitelem jsou správci front ve skupině sdílení front QSG1. Aplikace zpracování mezd má nyní spuštěné dvě instance, jednu připojenou k QM4 a jednu připojenou k QM5.



Obrázek 10. Příklad plánování kanálu zpráv pro IBM MQ for z/OS používající skupiny sdílení front

Předpokládá se, že všichni tři správci front jsou spuštěni v systému z/OS. V příkladech definic pro TCP/IP má QM4 adresu VIPA MVSIP01 a QM5 adresu VIPA MVSIP02. Oba správci front naslouchají na portu 1414. Generická adresa, kterou distributor prostředím sysplex poskytuje pro tuto skupinu, je QSG1.MVSIP. Server QM3 má adresu hostitele 192.0.2.0 a naslouchá na portu 1411.

V příkladových definicích pro produkt LU6.2 naslouchá produkt QM3 na symbolickém luname s názvem LUNAME1. Název generického prostředku definovaného pro VTAM pro lony, na nichž naslouchá QM4 a QM5, je LUQSG1. Příklad předpokládá, že jsou již definovány ve vašem systému z/OS a jsou k dispozici pro použití. Chcete-li je definovat, viz [“Vytvoření připojení LU 6.2 ke skupině sdílení front”](#) na stránce 49.

V tomto příkladu je QSG1 název skupiny sdílení front a správci front QM4 a QM5 jsou názvy členů skupiny.

Postup

Viz:

- [“Nastavení definic skupin sdílení front a správce front QM3, který není ve skupině sdílení front”](#) na stránce 161 pro podrobnosti o nastavení definic.

- “Příklad spuštění skupiny sdílení front pro z/OS” na stránce 162 obsahuje podrobnosti o spuštění inicializátorů kanálu a modulů listener pro jednotlivé správce front.

z/OS Nastavení definic skupin sdílení front a správce front QM3 , který není ve skupině sdílení front

Vytvoření následujících definic objektů pro jednoho člena skupiny sdílení front je zpřístupní všem ostatním členům. Server QM3 není členem skupiny sdílení front.

Informace o této úloze

Správci front QM4 a QM5 jsou členy skupiny sdílení front. Definice vytvořené pro QM4 jsou také k dispozici pro QM5.

Předpokládá se, že struktura seznamu prostředku Coupling Facility se nazývá 'APPLICATION1'. Pokud se nenazývá 'APPLICATION1', musíte pro příklad použít vlastní název struktury seznamu prostředku Coupling Facility.

Protože QM3 není členem skupiny sdílení front, potřebujete definice objektů pro tohoto správce front, aby mohl vkládat zprávy do fronty ve skupině sdílení front.

Procedura

- Nastavte sdílené objekty pro definici skupiny sdílení front:
 - a) Pomocí následujících příkazů můžete nastavit definice sdílených objektů, které jsou uloženy v databázi Db2, a jejich přidružené zprávy, které jsou uloženy v prostředku Coupling Facility.

```
DEFINE QLOCAL(PAYROLL) QSGDISP(SHARED) REPLACE PUT(ENABLED) GET(ENABLED) +
CFSTRUCT(APPLICATION1) +
DESCR('Shared queue for payroll details')

DEFINE QLOCAL(QM3) QSGDISP(SHARED) REPLACE USAGE(XMITQ) PUT(ENABLED) +
CFSTRUCT(APPLICATION1) +
DESCR('Transmission queue to QM3') TRIGGER TRIGTYPE(FIRST) +
TRIGDATA(QSG1.TO.QM3) GET(ENABLED) INITQ(SYSTEM.CHANNEL.INITQ)
```

- Pomocí následujících příkazů nastavte definice skupinových objektů, které jsou uloženy v adresáři Db2. Každý správce front ve skupině sdílení front vytvoří lokální kopii definovaného objektu.

- a) Nastavte kanál odesílatele:

Definice odesílacího kanálu pro připojení TCP/IP:

```
DEFINE CHANNEL(QSG1.TO.QM3) CHLTYPE(SDR) QSGDISP(GROUP) TRPTYPE(TCP) +
REPLACE DESCR('Sender channel to QM3') XMITQ(QM3) +
CONNNAME('192.0.2.0(1411)')
```

Definice odesílacího kanálu pro připojení LU 6.2 :

```
DEFINE CHANNEL(QSG1.TO.QM3) CHLTYPE(SDR) QSGDISP(GROUP) TRPTYPE(LU62) +
REPLACE DESCR('Sender channel to QM3') XMITQ(QM3) +
CONNNAME('LUNAME1')
```

- b) Nastavení přijímacího kanálu:

Definice přijímacího kanálu pro připojení TCP/IP:

```
DEFINE CHANNEL(QM3.TO.QSG1) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QM3') QSGDISP(GROUP)
```

Definice přijímacího kanálu pro připojení LU 6.2 :

```
DEFINE CHANNEL(QM3.TO.QSG1) CHLTYPE(RCVR) TRPTYPE(LU62) +
REPLACE DESCR('Receiver channel from QM3') QSGDISP(GROUP)
```

- Nastavení definic objektů správce front QM3 .

a) Nastavení CONNAME

CONNAME pro tento kanál je generická adresa skupiny sdílení front, která se liší podle typu přenosu.

Pro připojení TCP/IP:

```
DEFINE CHANNEL(QM3.TO.QSG1) CHLTYPE(SDR) TRPTYPE(TCP) +
REPLACE DESCR('Sender channel to QSG1') XMITQ(QSG1) +
CONNAME('QSG1.MVSIP(1414)')
```

Pro připojení LU 6.2 :

```
DEFINE CHANNEL(QM3.TO.QSG1) CHLTYPE(SDR) TRPTYPE(LU62) +
REPLACE DESCR('Sender channel to QSG1') XMITQ(QSG1) +
CONNAME('LUQSG1') TPNAME('MQSERIES') MODENAME('#INTER')
```

b) Nastavte ostatní definice.

Tyto definice jsou nezbytné pro stejné účely jako definice použité v dílčích tématech produktu “Příklad: Plánování kanálu zpráv v systému z/OS” na stránce 155.

```
DEFINE QREMOTE(PAYROLL.QUERY) DESCR('Remote queue for QSG1') REPLACE +
PUT(ENABLED) XMITQ(QSG1) RNAME(APPL) RQMNAME(QSG1)
```

```
DEFINE QLOCAL(QSG1) DESCR('Transmission queue to QSG1') REPLACE +
USAGE(XMITQ) PUT(ENABLED) GET(ENABLED) TRIGGER TRIGTYPE(FIRST) +
TRIGDATA(QM3.TO.QSG1) INITQ(SYSTEM.CHANNEL.INITQ)
```

```
DEFINE CHANNEL(QSG1.TO.QM3) CHLTYPE(RCVR) TRPTYPE(TCP) +
REPLACE DESCR('Receiver channel from QSG1')
```

```
DEFINE CHANNEL(QSG1.TO.QM3) CHLTYPE(RCVR) TRPTYPE(LU62) +
REPLACE DESCR('Receiver channel from QSG1')
```

```
DEFINE QLOCAL(PAYROLL.REPLY) REPLACE PUT(ENABLED) GET(ENABLED) +
DESCR('Reply queue for replies to query messages sent to QSG1')
```

z/OS

Příklad spuštění skupiny sdílení front pro z/OS

Informace o spuštění inicializátorů a modulů listener kanálu.

Informace o této úloze

Po vytvoření požadovaných objektů je třeba provést následující akce:

- Spusťte inicializátor kanálu pro všechny tři správce front.
- Spusťte moduly listener pro oba správce front.

Postup

1. Spusťte iniciátory kanálu.

Podrobné informace o způsobu spuštění inicializátoru kanálu naleznete v tématu [Spuštění inicializátoru kanálu](#) .

2. Spusťte listenery.

Podrobnosti o tom, jak spustit modul listener, naleznete v tématu [Spuštění modulu listener kanálu](#) .

Pro připojení TCP/IP musí mít každý člen skupiny spuštěný modul listener skupiny, který naslouchá na portu 1414.

```
STA LSTR PORT(1414) IPADDR(MVSIP01) INDISP(GROUP)
```

Předchozí položka například spustí modul listener na QM4.

V případě připojení LU6.2 musí mít každý člen skupiny spuštěný modul listener skupiny, který naslouchá na symbolickém luname. Tento název logické jednotky musí odpovídat generickému prostředku LUQSG1.

```
STA LSTR PORT(1411)
```

Předchozí položka spustí modul listener na serveru QM3.

Použití aliasu k odkazování na knihovnu produktu MQ

Můžete definovat alias pro odkazování na knihovnu MQ ve svém JCL, spíše než přímo používat název knihovny MQ. Pokud se pak název knihovny MQ změní, musíte alias pouze odstranit a předefinovat.

Příklad

Následující příklad definuje alias MQM.SCSQANLE pro odkazování na knihovnu MQ MQM.V600.SCSQANLE:

```
//STEP1 EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
DELETE (MQM.SCSQANLE)
DEFINE ALIAS (NAME(MQM.SCSQANLE) RELATE(MQM.V600.SCSQANLE))
/*
```

Poté se podívejte na MQM.V600.SCSQANLE s aliasem MQM.SCSQANLE.

Poznámka: Názvy knihoven a aliasů musí být ve stejném katalogu, proto pro oba použijte stejný kvalifikátor vyšší úrovně; v tomto příkladu je kvalifikátor vyšší úrovně MQM.

Managed File Transfer odkaz na konfiguraci

Referenční informace, které vám pomohou nakonfigurovat produkt Managed File Transfer.

Použití proměnných prostředí ve vlastnostech MFT

Je možné, aby se proměnné prostředí používaly ve vlastnostech Managed File Transfer, které představují umístění souborů nebo adresářů. To umožňuje, aby se umístění souborů nebo adresářů používaných při spouštění částí produktu lišila v závislosti na aktuálním prostředí (například uživatel spouštějící příkaz).

Následující vlastnosti přijímají umístění souborů nebo adresářů, a proto mohou obsahovat proměnné prostředí:

- agentQMgrAuthenticationCredentialsFile
- agentSslKeyStore
- agentSslKeyStoreCredentialsFile
- agentSslTrustStore
- agentSslTrustStoreCredentialsFile
- cdNodeKeystoreCredentialsFile
- cdNodeTruststoreCredentialsFile
- cdTmpDir
- cdNodeKeystore

- cdNodeTruststore
- commandPath
- connectionQMgrAuthenticationCredentialsFile
- connectionSslKeyStore
- connectionSslKeyStoreCredentialsFile
- connectionSslTrustStore
- connectionSslTrustStoreCredentialsFile
- coordinationSslKeyStore
- coordinationSslKeyStoreCredentialsFile
- coordinationQMgrAuthenticationCredentialsFile
- coordinationSslTrustStore
- coordinationSslTrustStoreCredentialsFile
- exitClassPath
- exitNativeLibraryPath
- javaCoreTriggerFile
- loggerQMgrAuthenticationCredentialsFile
- sandboxRoot
- transferRoot
- wmqfte.database.credentials.file

Příklad pro Windows

Windows V tomto příkladu na systému Windows se jedná o uživatele `fteuser`, který používá proměnnou prostředí `USERPROFILE`:

```
wmqfte.database.credentials.file=%USERPROFILE%\logger\mqmftcredentials.xml
```

Interpretuje následující cestu k souboru:

```
C:\Users\fteuser\logger\mqmftcredentials.xml
```

Příklad pro AIX and Linux

Linux **AIX** V tomto příkladu na systému UNIX se jedná o uživatele `fteuser`, který používá proměnnou prostředí `HOME`:

```
transferRoot=$HOME/fte/
```

Interpretuje následující cestu k souboru:

```
/home/fteuser/fte/
```

Související odkazy

[“Soubor MFT coordination.properties” na stránce 191](#)

Soubor `coordination.properties` uvádí podrobnosti připojení ke koordinačnímu správci front. Vzhledem k tomu, že několik instalací produktu Managed File Transfer může sdílet stejného koordinačního správce front, můžete použít symbolický odkaz na společný soubor `coordination.properties` na sdílené jednotce.

[“Soubor MFT command.properties” na stránce 195](#)

Soubor `command.properties` uvádí správce front příkazů, ke kterému se chcete připojit při zadávání příkazů, a informace, které produkt Managed File Transfer vyžaduje pro kontaktování tohoto správce front.

[“Soubor MFT agent.properties” na stránce 169](#)

Každý Managed File Transfer Agent má svůj vlastní soubor vlastností `agent.properties`, který musí obsahovat informace, které agent používá pro připojení ke svému správcí front. Soubor `agent.properties` může také obsahovat vlastnosti, které mění chování agenta.

[Vlastnosti SSL/TLS pro MFT](#)

[“Soubor MFT logger.properties” na stránce 199](#)

Modul protokolování Managed File Transfer má sadu vlastností konfigurace. Tyto vlastnosti zadejte v souboru `logger.properties`, který se nachází v adresáři `MQ_DATA_PATH/mqft/config/coordination_qmgr_name/loggers/logger_name`.

[MFT Vlastnosti agenta pro uživatelské procedury](#)

[Formát souboru vlastností mostu protokolů](#)

[Formát souboru definice procesu Connect:Direct](#)

[Formát souboru vlastností uzlu Connect:Direct](#)

Soubor MFT `installation.properties`

Soubor `installation.properties` uvádí název výchozí sady voleb konfigurace. Tato položka ukazuje Managed File Transfer na strukturovanou sadu adresářů a souborů vlastností, které obsahují konfiguraci, která se má použít. Obvykle je název sady voleb konfigurace názvem přidruženého koordinačního správce front.

Tento soubor je vytvořen instalačním programem a lze jej změnit pomocí příkazu **`fteChangeDefaultConfigurationOptions`**.

Soubor `installation.properties` se nachází ve vašem adresáři `MQ_DATA_PATH`. Například v systému Windows je výchozí umístění souboru `MQ_DATA_PATH\mqft\installations\installation_name` a v systémech AIX and Linux je výchozí umístění souboru `/var/mqm/mqft/installations/installation_name`.

Pro Redistributable Managed File Transfer Agent je cesta k datům nastavena při spuštění příkazu **`fteCreateEnvironment`**. Pokud spustíte příkaz a uvedete zvolené umístění s parametrem **`-d`**, nastaví se cesta k datům pro toto umístění. Pokud neuvedete umístění pomocí příkazu **`fteCreateEnvironment`**, vytvoří se adresář `mqftdata` v kořenovém adresáři, kam se extrahuje soubor Redistributable Managed File Transfer Agent. Soubor `installation.properties` pro Redistributable Managed File Transfer Agent je umístěn v adresáři `MQ_DATA_PATH\mqft\installations\MFTZipInstall`.

Soubor `installation.properties` obsahuje následující hodnoty:

Tabulka 64. Základní vlastnosti

Název vlastnosti	Popis	Výchozí hodnota
<p>Priorita commandMessage</p>	<p>Nastaví prioritu interních zpráv i zpráv příkazů pro příkazy fteStopAgent, fteCancelTransfer a ftePingAgent .</p> <p>Zadáte-li například velký počet požadavků na přenos pro přenos mnoha malých souborů v rychlém sledu, mohou být nové požadavky na přenos zařazeny do fronty příkazů zdrojového agenta. Externí a interní zprávy mají výchozí prioritu zpráv IBM MQ , takže jsou interní zprávy blokovány novými požadavky na přenos. To může způsobit překročení doby vyjednávání přenosu a zotavení přenosů.</p> <p>Pomocí vlastnosti commandMessagePriority můžete také nastavit prioritu interních zpráv s potvrzením a očekávanými potvrzením.</p> <p>Chcete-li stanovit prioritu interních zpráv Managed File Transfer nad novými požadavky na přenos, nastavte tuto vlastnost na hodnotu mezi 1 (nejnižší) a 9 (nejvyšší).</p> <p>Výchozí hodnota vlastnosti commandMessagePriority je 8. To znamená, že pokud je atribut IBM MQ DEFPRTY (výchozí priorita) ve frontě příkazů agenta menší nebo roven 7, budou interní zprávy vyjednávání upřednostněny před novými požadavky na přenos. Pokud je hodnota atributu DEFPRTY nastavena na hodnotu 8 nebo 9, musíte kvůli zachování účinnosti vlastnosti priority commandMessage změnit buď vlastnost DEFPRTY, nebo vlastnost priority commandMessage.</p>	<p>Pro systém IBM MQ 9.0.0.0 a novější je výchozí hodnota 8.</p> <p>V předchozích verzích a před opravou APAR IT06213 je výchozí hodnotou konstanta MQPRI_PRIORITY_AS_Q_DEF, která má hodnotu -1.</p>

Tabulka 64. Základní vlastnosti (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
commonCredentialsKeyFile	<p>Úplný název cesty k souboru obsahujícímu klíč pověření použitý při šifrování pověření. Nejběžnějším názvem souboru pověření MFT je <code>MQMFTCredentials.xml</code>.</p> <p>Další informace o použití vlastnosti <code>commonCredentialsKeyFile</code> naleznete v tématu Dešifrování pověření.</p>	Úplná cesta k souboru s klíči
defaultProperties	<p>Název výchozí sady voleb konfigurace. Tato hodnota představuje název adresáře umístěného v konfiguračním adresáři, který obsahuje adresáře a soubory vlastností, které určují informace o konfiguraci.</p>	Bez výchozí hodnoty
enableFunctionalFixPack	<p>Úroveň funkce opravné sady, která má být povolena. Ve výchozím nastavení není žádná nová funkce zahrnutá v opravné sadě povolena. Nastavte tuto vlastnost na identifikátor verze, chcete-li povolit nové funkce dostupné pro tuto verzi.</p> <p>Můžete uvést identifikátor verze se znaky tečky nebo bez nich (.). Chcete-li například použít funkci, která je k dispozici s produktem IBM MQ 8.0.0 Fix Pack 2, nastavte tuto vlastnost na hodnotu <code>8002</code> nebo <code>8.0.0.2</code>.</p>	Bez výchozí hodnoty

Tabulka 64. Základní vlastnosti (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
Formát messagePublication	<p>Umožňuje vám uvést formát publikování zpráv používaný agenty MFT pro jejich stavové zprávy XML. Tuto vlastnost lze nastavit na následující hodnoty:</p> <p>messagePublicationFormát = smíšený Zprávy jsou publikovány bez parametru MQMD FORMAT (MQFMT_NONE), s výjimkou zpráv publikovaných ve stromu témat /LOG, které jsou publikovány ve formátu MQMD MQFMT_STRING.</p> <p>messagePublicationFormat=MQFMT_NONE Zprávy jsou publikovány bez parametru MQMD FORMAT.</p> <p>messagePublicationFormát = MQFMT_STRING Zprávy jsou publikovány ve formátu řetězce.</p>	messagePublicationFormát = smíšený
<div style="background-color: #f0f0f0; padding: 5px;"> z/OS z/OS z/OS-specifické pro: </div>		
<div style="background-color: #f0f0f0; padding: 5px;"> z/OS productID </div>	<p>Typ výrobku, u kterého má být zaznamenáno použití MFT:</p> <ul style="list-style-type: none"> • Samostatný produkt Managed File Transfer . (MFT je productID). • Část produktu IBM MQ Advanced . (ADVANCED je productID). • Část produktu IBM MQ Advanced for z/OS Value Unit Edition . (ADVANCEDVUE je productID). <p>Další informace o záznamu využití produktu viz Informace o produktu vytváření sestav .</p> <div style="background-color: #d0d0d0; padding: 2px 5px; display: inline-block;">Multi</div> Tato vlastnost je v systému Multiplatformsignorována .	MFT

Následující text je příkladem obsahu souboru installation.properties .

```
defaultProperties=ERIS
```

ERIS je název adresáře, který je umístěn ve stejném adresáři jako soubor installation.properties . Adresář ERIS obsahuje adresáře a soubory vlastností, které popisují sadu voleb konfigurace.

Související pojmy

Volby konfigurace MFT na platformě Multiplatforms

Související odkazy

[fteChangeDefaultConfiguration](#)

Soubor MFT 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.

Soubor agent.properties je vytvořen instalačním programem nebo příkazem **fteCreateAgent**, **fteCreateBridgeAgent** nebo **fteCreateCDAgent**. Kterýkoli z těchto příkazů s příznakem **-f** můžete použít ke změně základních vlastností správce front agenta a těch rozšířených vlastností agenta, které jsou přidruženy k typu vytvářeného agenta. Chcete-li změnit nebo přidat rozšířené vlastnosti agenta, musíte upravit soubor v textovém editoru.

Multi Na platformě Multiplatforms se soubor agent.properties pro agenta nachází v adresáři `MQ_DATA_PATH/mqft/config/coordination_qmgr_name/agents/agent_name`.

z/OS V systému z/OS je umístění souboru agent.properties `$BFG_CONFIG variable/mqft/config/coordination_qmgr_name/agents/agent_name`.

Pokud změníte soubor agent.properties, musíte restartovat agenta, aby se změny projevyly.

Můžete použít proměnné prostředí v některých vlastnostech Managed File Transfer, které představují umístění souborů nebo adresářů. To vám umožňuje použít umístění souborů nebo adresářů, když spouštíte části produktu, aby se lišily v závislosti na změnách prostředí, například na tom, který uživatel spouští proces. Další informace viz téma [“Použití proměnných prostředí ve vlastnostech MFT”](#) na stránce 163.

Windows

Poznámka: V systému Windows se jedná o dvě vlastnosti:

- windowsService
- windowsServiceVersion

jsou přidány do souboru agent.properties pomocí příkazů MFT, které se používají k nastavení agenta ke spuštění jako služba Windows.

Vlastnosti byste neměli přidávat ani je upravovat ručně, protože to zabrání správnému fungování agenta.

Základní vlastnosti agenta

Každý soubor MFT agent.properties obsahuje následující základní vlastnosti agenta:

Název vlastnosti	Popis	Výchozí hodnota
agentName	Název agenta. Název agenta musí odpovídat konvencím pojmenování objektů IBM MQ. Další informace viz téma “Konvence pojmenování objektů MFT” na stránce 226.	Bez výchozí hodnoty
agentDesc	Popis agenta-pokud se rozhodnete vytvořit popis.	Bez výchozí hodnoty
agentQMGr	Název správce front agenta.	Bez výchozí hodnoty
agentQMGrHostitel	Název hostitele nebo adresa IP správce front agenta.	Bez výchozí hodnoty
Port agentQMGr	Číslo portu, které se používá pro připojení klienta ke správci front agenta.	1414
Kanál agentQMGr	Název kanálu SVRCONN, který se používá pro připojení ke správci front agenta.	SYSTEM.DEF.SVRCONN


Tabulka 65. Základní vlastnosti agenta (pokračování)


Název vlastnosti	Popis	Výchozí hodnota
agentType	Typ agenta: <ul style="list-style-type: none"> • Standardní agent mimo most (STANDARD) • Agent mostu protokolů (BRIDGE) • Connect:Direct agent mostu (CD_BRIDGE) • Vestavěný agent používaný produktem IBM Integration Bus (EMBEDDED) • Vestavěný agent Sterling File Gateway (SFG) 	STANDARD


Pokud nezadáte hodnotu pro vlastnost hostitele agentQMGr, použije se standardně režim vazeb.

Pokud zadáte hodnotu pro vlastnost hostitele agentQMGr, ale neuvedete hodnoty pro vlastnosti kanálu agentQMGrPort a agentQMGr, číslo portu 1414 a kanál SYSTEM.DEF.SVRCONN .

Rozšířené vlastnosti agenta

Produkt Managed File Transfer také poskytuje rozšířené vlastnosti agenta, které vám pomohou konfigurovat agenty. Chcete-li použít některou z následujících vlastností, ručně upravte soubor agent . properties a přidejte požadované rozšířené vlastnosti. Závorky (.) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\).  Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/). Další informace o řídicím znaku v souborech vlastností Java naleznete v dokumentaci Oracle [Javadoc pro třídu vlastností](#).

- [Vlastnosti velikosti agenta](#)
- [Vlastnosti kódové stránky](#)
- [Vlastnosti příkazu](#)
- [Vlastnosti připojení](#)
- [Connect:Direct vlastnosti mostu](#)
- [Vlastnosti souboru do zprávy a zprávy do agenta souboru](#)
- [Obecné vlastnosti agenta](#)
- [Vlastnosti vysoké dostupnosti](#)
- [Vlastnosti vstupu/výstupu](#)
-  [Vlastnosti protokolu přenosu](#)
- [Vlastnosti vícekanálové podpory](#)
- [Vlastnosti s více instancemi](#)
- [Vlastnosti řadiče procesů](#)
- [Vlastnosti mostu protokolů](#)
- [Vlastnosti protokolu agenta mostu protokolů](#)
- [Vlastnosti fronty](#)
- [Vlastnosti monitorování prostředků](#)
- [Vlastnosti kořenového adresáře](#)
- [Vlastnost plánovače](#)
- [Vlastnosti zabezpečení](#)
- [Vlastnosti SSL/TLS](#)
- [Vlastnosti časového limitu](#)
- [Vlastnosti časového limitu obnovy přenosu](#)

- Vlastnosti trasování a protokolování
- Vlastnosti omezení přenosu
- Vlastnosti uživatelské procedury
- IBM MQ vlastnosti komprese klienta
-  z/OS
- Jiné vlastnosti

Tabulka 66. Rozšířené vlastnosti agenta: Velikost agenta

Název vlastnosti	Popis	Výchozí hodnota
Interval agentCheckpoint	Interval v úplných rámcích dat, mezi kterými se provádí kontrolní bod pro účely obnovy. Jedná se o rozšířenou vlastnost a pro většinu konfigurací produktu Managed File Transfer není nutné upravovat její hodnotu. Pokud se vyskytne problém, který způsobí, že přenos přejde do obnovy, přenos se může obnovit pouze na hranici kontrolního bodu. Čím větší je tato hodnota (s velkými hodnotami agentChunkSize, agentWindowSize a agentFrameSize), tím delší je doba, kterou agent potřebuje k obnově přenosů. U spolehlivých sítí Managed File Transfer, kde přenosy zřídka vstupují do stavu obnovy, může být výhodné zvýšit tuto hodnotu, aby se zvýšil celkový výkon.	1
Velikost agentChunk	Velikost každého přenosového bloku pro přenos dat souboru. Proto označuje maximální velikost zpráv IBM MQ, které jsou přenášeny mezi zdrojovými a cílovými agenty. Jedná se o rozšířenou vlastnost a pro většinu konfigurací produktu Managed File Transfer není nutné upravovat její hodnotu. Tato hodnota je vyjednána mezi zdrojovým a cílovým agentem a použije se větší ze dvou hodnot. Chcete-li změnit hodnotu této vlastnosti, změňte hodnotu na zdrojovém i cílovém agentovi. agentChunkVelikost je celočíselná hodnota. Například: agentChunkSize = 10240 nastaví velikost diskového bloku na 10 kB.	262144 bajtů (ekvivalent 256 kB)
Velikost agentFrame	Počet oken pro přenosový rámec. Jedná se o rozšířenou vlastnost a pro většinu konfigurací produktu Managed File Transfer není nutné upravovat její hodnotu. U sítí s vysokou latencí může zvýšení této hodnoty zlepšit celkový výkon, protože způsobí, že agent bude mít souběžně aktivních více diskových bloků zpráv. Hodnota této vlastnosti vynásobená velikostí agentWindowvynásobená velikostí agentChunkoznačuje horní limit spotřeby paměti agenta pro každý přenos. Například 262144bajtové diskové bloky x 10 x 5 = 12.5 MB pro každý přenos. Poznámka: Pokud je velikost přenesených souborů v jednom přenosu menší než 12.5 MB, zvýšení této vlastnosti nemá žádný vliv na výkon přenosu.	5
Velikost agentWindow	Počet diskových bloků pro každé okno. Jedná se o rozšířenou vlastnost a pro většinu konfigurací produktu Managed File Transfer není nutné upravovat její hodnotu. U sítí s vysokou latencí může zvýšení této hodnoty zlepšit celkový výkon. Důvodem je, že agent má souběžně aktivních více diskových bloků zpráv a snižuje frekvenci odesílání potvrzených zpráv zpět do zdrojového agenta. Hodnota této vlastnosti, vynásobená velikostí agentFrame, vynásobená velikostí agentChunk, označuje horní limit spotřeby paměti agenta pro každý přenos a označuje horní limit dat zprávy IBM MQ v datové frontě cílového agenta. Například 262144bajtové diskové bloky x 10 x 5 = horní limit 12.5 MB pro každý přenos. Poznámka: Pokud je velikost přenášovaných souborů v jednom přenosu menší než 12.5 MB, zvýšení hodnoty této vlastnosti nemá žádný vliv na výkon přenosu.	10

Tabulka 67. Rozšířené vlastnosti agenta: Kódová stránka

Název vlastnosti	Popis	Výchozí hodnota
agentCcsid	Kódová stránka, se kterou se agent připojuje ke svému správci front agenta. Pokud uvedete hodnotu pro agentCcsid, musíte také uvést hodnotu pro název agentCcsid. Informace o tom, jak zobrazit známé kódové stránky pro prostředí JVM, viz parametr <code>-hsc</code> v příkazu <code>fteCreateBridgeAgent</code> .	1208
Název agentCcsid	Java reprezentace agentCcsid. Pokud uvedete hodnotu pro název agentCcsid, musíte také uvést hodnotu pro agentCcsid.	UTF8

Tabulka 68. Rozšířené vlastnosti agenta: Příkaz		
Název vlastnosti	Popis	Výchozí hodnota
maxCommandHandlerThreads	Řídí počet podprocesů, které jsou k dispozici pro počáteční analýzu a zpracování zpráv příkazu přenosu. Když jsou podprocesy aktivní, vyžadují připojení ke správci front, ale podprocesy uvolní připojení, když jsou nečinné.	5
Výstup příkazu maxCommand	Maximální počet bajtů uložených pro výstup příkazu. Tato vlastnost platí pro příkazy zadané pro spravované volání a příkazy preSource, postSource, preDestinationa postDestination pro spravovaný přenos. Tím se omezuje délka výstupu příkazu, který je zapsán do protokolu přenosu v systému SYSTEM.FTE .	10240
maxCommandOpakování pokusů	Maximální počet opakování pro příkaz, který agent povoluje. Tato vlastnost platí pro příkazy zadané pro spravované volání a příkazy preSource, postSource, preDestinationa postDestination pro spravovaný přenos.	9
maxCommandČekání	Maximální doba čekání, v sekundách, mezi opakovými pokusy, které agent povolí. Tato vlastnost platí pro příkazy zadané pro spravované volání a příkazy preSource, postSource, preDestinationa postDestination pro spravovaný přenos.	60
immediateShutdownvypršení časového limitu	V případě okamžitého ukončení činnosti agenta můžete pomocí této vlastnosti určit maximální dobu v sekundách, po kterou agent čeká na dokončení přenosů před vynucením ukončení práce systému. Poznámka: Neměňte hodnotu této vlastnosti na méně než výchozí hodnotu 10 sekund. Okamžité ukončení činnosti agenta vyžaduje dostatek času k ukončení všech externích procesů. Je-li hodnota této vlastnosti příliš nízká, procesy mohou zůstat spuštěné. Je-li pro tuto vlastnost zadána hodnota 0, agent čeká na zastavení všech nevyřízených přenosů. Pokud je pro tuto vlastnost zadána neplatná hodnota, použije se výchozí hodnota.	10













Tabulka 69. Rozšířené vlastnosti agenta: Připojení		
Název vlastnosti	Popis	Výchozí hodnota
Cesta javaLibrary	Při připojování ke správci front v režimu vazeb musí mít produkt Managed File Transfer přístup ke knihovně vazeb produktu IBM MQ Java . Standardně produkt Managed File Transfer vyhledává knihovny vazeb ve výchozím umístění, které je definováno pomocí IBM MQ. Pokud se knihovny vazeb nacházejí v jiném umístění, použijte tuto vlastnost k určení umístění knihoven vazeb.	Není

Tabulka 70. Rozšířené vlastnosti agenta: Connect:Direct bridge		
Název vlastnosti	Popis	Výchozí hodnota
cdNode	Vyžadovaná vlastnost, chcete-li použít most Connect:Direct . Název uzlu Connect:Direct , který má být použit pro přenos zpráv z uzlů Connect:Direct agenta mostu do cílových uzlů Connect:Direct . Tento uzel je součástí mostu Connect:Direct , nikoli vzdáleného uzlu, který je zdrojem nebo cílem přenosu. Další informace naleznete v tématu Most Connect:Direct .	Bez výchozí hodnoty
Hostitel cdNode	Název hostitele nebo adresa IP uzlu Connect:Direct , který se má použít k přenosu souborů z agenta mostu Connect:Direct do cílových uzlů (uzel mostu Connect:Direct). Ve většině případů se uzel mostu Connect:Direct nachází na stejném systému jako agent mostu Connect:Direct . V těchto případech je výchozí hodnota této vlastnosti, která je adresou IP lokálního systému, správná. Pokud má váš systém více adres IP nebo je váš uzel mostu Connect:Direct na jiném systému než váš agent mostu Connect:Direct a jejich systémy sdílejí systém souborů, použijte tuto vlastnost k určení správného názvu hostitele pro uzel mostu Connect:Direct . Pokud jste nenastavili vlastnost cdNode , bude tato vlastnost ignorována.	Název hostitele nebo adresa IP lokálního systému
Port cdNode	Číslo portu uzlu mostu Connect:Direct , který klientské aplikace používají ke komunikaci s uzlem. V dokumentaci k produktu Connect:Direct se na tento port odkazuje jako na port rozhraní API. Pokud jste nenastavili vlastnost cdNode , bude tato vlastnost ignorována.	1363

Tabulka 70. Rozšířené vlastnosti agenta: Connect:Direct bridge (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
cimpDir	<p>Umístění pro dočasné uložení souborů na systému, kde je spuštěn agent mostu Connect:Direct , než jsou přeneseny do cílového uzlu Connect:Direct .</p> <p>Tato vlastnost určuje úplnou cestu k adresáři, ve kterém jsou dočasně uloženy soubory. Pokud je například parametr cdTmpDir nastaven na hodnotu /tmp , jsou soubory dočasně umístěny do adresáře /tmp .</p> <p>Agent mostu Connect:Direct a uzel mostu Connect:Direct musí mít přístup k adresáři určeném tímto parametrem s použitím stejného názvu cesty. Zvažte toto při plánování instalace mostu Connect:Direct. Je-li to možné, vytvořte agenta na systému, na kterém je umístěn uzel Connect:Direct, který je součástí mostu Connect:Direct. Jsou-li váš agent a uzel na samostatných systémech, musí být adresář na sdíleném systému souborů a musí být přístupný z obou systémů používajících stejný název cesty. Další informace o podporovaných konfiguracích viz Most Connect:Direct.</p> <p>Pokud jste nenastavili vlastnost cdNode , bude tato vlastnost ignorována.</p> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí.</p> <p>Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.</p>	<pre>value_of_java.io.tmpdir /cdbridge-agentName</pre>
cdTrace	Zda agent trasuje data odesílaná mezi agentem mostu Connect:Direct a jeho uzlem Connect:Direct . Hodnota této vlastnosti může být true nebo false.	ne
cdMaxConnectionRetries	Maximální počet pokusů o připojení systému Connect:Direct pro přenos souborů, kde ještě nebylo provedeno úspěšné připojení, než se přenos nezdaří.	-1 (nekonečný počet pokusů)
cdMaxPartialWorkConnectionRetries	Maximální počet pokusů o připojení systému Connect:Direct pro přenos souborů, kde byl předchozí pokus o připojení úspěšný a byla dokončena práce na přenosu, než se přenos nezdaří.	-1 (nekonečný počet pokusů)
cdMaxWaitForProcessEnd	Maximální doba v milisekundách, po kterou se má čekat na dostupnost informací o dokončení procesu Connect:Direct v rámci statistických informací o uzlu Connect:Direct po ukončení procesu, než se přenos souborů považuje za nezdařený. Obvykle jsou informace k dispozici okamžitě, ale za určitých podmínek selhání nejsou informace publikovány. Za těchto podmínek se přenos souborů nezdaří po čekání na dobu určenou touto vlastností.	60000
Název cdApp	Název aplikace, kterou agent mostu Connect:Direct používá pro připojení k uzlu Connect:Direct , který je součástí mostu.	Managed File Transfer <i>aktuální verze</i> , kde <i>aktuální verze</i> je číslo verze produktu.
cdNodeLocalPort	Rozsah lokálních portů, které se mají použít pro připojení soketů mezi agentem mostu Connect:Direct a uzlem Connect:Direct , který je součástí mostu. Formát této hodnoty je seznam hodnot nebo rozsahů oddělených čárkami. Standardně operační systém vybírá čísla lokálních portů.	Není
Protokol cdNode	Protokol, který agent mostu Connect:Direct používá pro připojení k uzlu Connect:Direct , který je součástí mostu. Platné jsou tyto hodnoty: <ul style="list-style-type: none"> • TCPIP • SSL • TLS 	TCPIP
Úložiště klíčů cdNode	Cesta k úložišti klíčů, které se používá pro zabezpečenou komunikaci mezi agentem mostu Connect:Direct a uzlem Connect:Direct , který je součástí mostu. Pokud jste nenastavili vlastnost protokolu cdNodena zabezpečení SSL nebo TLS, bude tato vlastnost ignorována. Hodnota této vlastnosti může obsahovat proměnné prostředí. Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.	Není
cdNodeKeystoreType	Formát souboru úložiště klíčů, který je určen vlastností úložiště klíčů cdNode. Platné jsou tyto hodnoty: jks a pkcs12. Pokud jste nenastavili vlastnost protokolu cdNodena zabezpečení SSL nebo TLS, bude tato vlastnost ignorována.	JKS

Tabulka 70. Rozšířené vlastnosti agenta: Connect:Direct bridge (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
Soubor cdNodeKeystoreCredentials	<p>Cesta k souboru, který obsahuje pověření úložiště klíčů cdNode.</p> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí. Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.</p> <p> Podrobnosti o vytváření souborů pověření viz MFT a IBM MQ ověření připojení</p> <p> Podrobnosti o vytváření souborů pověření viz Konfigurace MQMFTCredentials.xml na webu z/OS.</p>	<p>Výchozí hodnota této vlastnosti je:</p> <p> Linux</p> <p> z/OS</p> <p> AIX \$HOME/MQMFTCredentials.xml</p> <p> Windows %USERPROFILE%/MQMFTCredentials.xml</p>
Úložiště údajů o důvěryhodnosti cdNode	<p>Cesta k úložišti údajů o důvěryhodnosti, které se používá pro zabezpečenou komunikaci mezi agentem mostu Connect:Direct a uzlem Connect:Direct, který je součástí mostu.</p> <p>Pokud jste nenastavili vlastnost protokolu cdNodena zabezpečení SSL nebo TLS, bude tato vlastnost ignorována.</p> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí.</p> <p>Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.</p>	Není
cdNodeTruststoreType	<p>Formát souboru úložiště údajů o důvěryhodnosti, který je určen vlastností úložiště údajů o důvěryhodnosti cdNode. Platné jsou tyto hodnoty: jks a pkcs12.</p> <p>Pokud jste nenastavili vlastnost protokolu cdNodena zabezpečení SSL nebo TLS, bude tato vlastnost ignorována.</p>	JKS
Soubor cdNodeTruststoreCredentials	<p>Cesta k souboru, který obsahuje pověření úložiště údajů o důvěryhodnosti cdNode.</p> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí. Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.</p> <p> Podrobnosti o vytváření souborů pověření viz MFT a IBM MQ ověření připojení</p> <p> Podrobnosti o vytváření souborů pověření viz Konfigurace MQMFTCredentials.xml na webu z/OS.</p>	<p>Výchozí hodnota této vlastnosti je:</p> <p> Linux</p> <p> z/OS</p> <p> AIX \$HOME/MQMFTCredentials.xml</p> <p> Windows %USERPROFILE%/MQMFTCredentials.xml</p>
logCDProcess	<p>Úroveň protokolování procesů Connect:Direct zaznamenaná v protokolu událostí agenta v souboru output0.log. Hodnoty, které tato vlastnost může mít, jsou Žádná nebo Selhání nebo Vše.</p>	Není

Tabulka 71. Rozšířené vlastnosti agenta: Soubor do zprávy a zpráva do agenta souboru

Název vlastnosti	Popis	Výchozí hodnota
deleteTmpFileAfterRenameFailure	<p>Nastavení této vlastnosti na hodnotu false zajistí, že v případě selhání operace přejmenování nebudou dočasné soubory z místa určení odstraněny. V tomto případě přenášená data zůstávají v místě určení v dočasném souboru (.part). Tento soubor můžete později přejmenovat ručně. Standardně má tato vlastnost hodnotu true. Tato vlastnost se vztahuje jak na přenos zpráv do souboru, tak na přenos souborů do souboru.</p>	ano
enableQueueInputOutput	<p>Standardně nemůže agent číst data ze zdrojové fronty nebo zapisovat data do cílové fronty jako součást přenosu. Nastavení této hodnoty na true umožní agentovi provádět přenos souborů do zpráv a přenos zpráv do souborů. Hodnota této vlastnosti může být true nebo false.</p>	ne
enableSystemQueueInput	<p>Uvádí, zda agent může číst ze systémových front IBM MQ nebo do nich zapisovat. Systémové fronty mají předponu s kvalifikátorem SYSTEM.</p> <p>Poznámka: Systémové fronty jsou používány aplikacemi IBM MQ, Managed File Transfera dalšími aplikacemi pro přenos důležitých informací. Změna této vlastnosti umožní agentovi přístup k těmto frontám. Pokud povolíte tuto vlastnost, použijte pískoviště uživatele k omezení front, ke kterým má agent přístup.</p>	ne
enableClusterQueueInput	<p>Určuje, zda může agent číst z klastrovaných front systému IBM MQ nebo do nich zapisovat.</p> <p>Poznámka: Kromě vlastnosti enableQueueInputOutput musíte zadat vlastnost výstupního agenta enableClusterQueueInput.</p>	ne

Tabulka 71. Rozšířené vlastnosti agenta: Soubor do zprávy a zpráva do agenta souboru (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
maxDelimiterMatchLength	Maximální počet znaků, které lze porovnat s regulárním výrazem Java, který se používá k rozdělení textového souboru do více zpráv jako součást přenosu souborů na zprávy.	5
maxInputOutputMessage	Maximální délka (v bajtech) zprávy, která je přečtena ze zdrojové fronty nebo zapsána agentem do cílové fronty. Vlastnost maxInputOutputMessageDélka zdrojového agenta v přenosu určuje, kolik bajtů lze číst ze zprávy ve zdrojové frontě. Vlastnost délky maxInputOutputMessageCílového agenta v přenosu určuje, kolik bajtů lze zapsat do zprávy v cílové frontě. Pokud délka zprávy překročí hodnotu této vlastnosti, přenos se nezdaří s chybou. Tato vlastnost nemá vliv na interní fronty Managed File Transfer. Informace o změně této vlastnosti naleznete v tématu Pokyny pro nastavení atributů produktu MQ a MFT vlastností přidružených k velikosti zprávy.	1048576
monitorGroupRetryLimit	Maximální počet případů, kdy monitor znovu spustí přenos zprávy do souboru, pokud skupina zpráv stále existuje ve frontě. Počet případů, kdy jsou spouštěče přenosu zpráv do souborů určeny z počtu vrácení MQMD první zprávy ve skupině. Pokud je agent restartován, monitor spustí přenos znovu, i když počet spouštěčů přenosu překročí hodnotu monitorGroupRetryLimit. Pokud toto chování způsobí, že počet spouštěčů přenosu překročí hodnotu monitorGroupRetryLimit, agent zapíše chybu do svého protokolu událostí. Pokud je pro tuto vlastnost uvedena hodnota -1, monitor spustí přenos znovu neomezeně, dokud není splněna podmínka spouštěče.	10


Tabulka 72. Rozšířené vlastnosti agenta: Obecné		
Název vlastnosti	Popis	Výchozí hodnota
agentStatusPublishRateLimit	Maximální rychlost v sekundách, jakou agent znovu publikuje svůj stav kvůli změně stavu přenosu souborů. Nastavíte-li tuto vlastnost na příliš malou hodnotu, výkon sítě IBM MQ může být negativně ovlivněn.	30
agentStatusPublishRateMin	Minimální rychlost v sekundách, kterou agent publikuje svůj stav. Tato hodnota musí být větší nebo rovna hodnotě vlastnosti agentStatusPublishRateLimit .	300
enableMemoryAllocationChecking	Hodnota této vlastnosti může být <code>true</code> nebo <code>false</code> . Určuje, zda produkt Managed File Transfer Agent kontroluje, zda je k dispozici dostatek paměti pro spuštění přenosu před přijetím přenosu. Kontrola se provádí na zdrojovém i cílovém agentech. Pokud není k dispozici dostatek paměti, přenos bude odmítnut. Při výpočtu paměti požadované pro přenos je použita maximální paměť vyžadovaná přenosem. Proto může být hodnota větší než skutečná paměť, kterou přenos používá. Z tohoto důvodu může být počet souběžných přenosů, které lze spustit, snížen, pokud je vlastnost enableMemoryAllocationChecking nastavena na hodnotu <code>true</code> . Doporučuje se nastavit vlastnost na hodnotu <code>true</code> pouze v případě, že dochází k problémům s Managed File Transfer selháním s chybami nedostatku paměti. Přenosy, které pravděpodobně spotřebovávají velké množství paměti, jsou přenosy mezi soubory a zprávami a přenosy mezi zprávami a soubory, kde jsou velikosti zpráv velké.	ne
enableDetailedReplyMessages	Hodnota této vlastnosti může být <code>true</code> nebo <code>false</code> . Nastavení této vlastnosti na hodnotu <code>true</code> umožní, aby odpovědi na požadavky na spravovaný přenos obsahovaly podrobné informace o přenesených souborech. Podrobné informace a formát jsou stejné jako ty, které byly publikovány do protokolu přenosu ve zprávách o průběhu, tj. prvek <code><transferSet></code> . Další informace naleznete v tématu Formáty zpráv protokolu přenosu souborů . Podrobné informace o odpovědi jsou zahrnuty pouze v případě, že požadavek na spravovaný přenos uvádí, že jsou požadovány podrobné informace o odpovědi. Chcete-li zadat tento požadavek, nastavte atribut detailed prvku <code><reply></code> zprávy požadavku XML managedTransfer odeslané zdrojovému agentu. Další informace viz Formát zprávy požadavku na přenos souborů . Pro každý požadavek na přenos lze vygenerovat více zpráv odpovědi. Toto číslo se rovná počtu zpráv o průběhu přenosu protokolu pro přenos plus 1 (kde první zpráva odpovědi je jednoduchá odpověď ACK). Podrobné informace jsou zahrnuty ve všech zprávách, s výjimkou zpráv odpovědi ACK, ale celkový výsledek přenosu je zahrnut pouze v poslední podrobné zprávě odpovědi.	ano

Tabulka 72. Rozšířené vlastnosti agenta: Obecné (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
enableUserMetadataOptions	<p>Hodnota této vlastnosti může být <code>true</code> nebo <code>false</code>. Určuje, zda můžete použít známé klíče pro metadata definovaná uživatelem v nových požadavcích na přenos, abyste poskytli více voleb přenosu. Tyto známé klíče vždy začínají následující předponou <code>com.ibm.wmqfte.</code>. V důsledku toho, když je vlastnost enableUserMetadataOptions nastavena na hodnotu <code>true</code>, klíče, které používají tuto předponu, nejsou podporovány pro uživatelem definované použití. Když je vlastnost enableUserMetadataOptions nastavena na hodnotu <code>true</code>, klíče, které jsou momentálně podporovány, jsou následující:</p> <p>com.ibm.wmqfte.insertRecordLineSeparator</p> <p>Pro textové přenosy. Když je tento klíč nastaven na hodnotu <code>true</code>, uvádí, že při čtení souborů orientovaných na záznamy, jako jsou datové sady z/OS, se mezi záznamy vkládají oddělovače řádků.</p> <p>Je-li tento klíč nastaven na hodnotu <code>false</code>, určuje, že při čtení souborů orientovaných na záznamy se mezi záznamy nemají vkládat oddělovače řádků.</p> <p>com.ibm.wmqfte.newRecordOnLineSeparator</p> <p>Pro textové přenosy. Když je tento klíč nastaven na hodnotu <code>true</code>, uvádí, že při zápisu do souborů orientovaných na záznamy, jako jsou datové sady z/OS, tyto oddělovače řádků označují nový záznam a nezapisují se jako součást dat.</p> <p>Je-li tento klíč nastaven na hodnotu <code>false</code>, určuje, že při zápisu do souborů orientovaných na záznamy se s oddělovači řádků bude zacházet jako s jakýmkoli jiným znakem (tj. bez zalomení záznamů).</p> <p>com.ibm.wmqfte.convertLineSeparators</p> <p>Pro textové přenosy. Určuje, zda jsou posloupnosti oddělovačů řádků CRLF a LF převedeny na požadovanou posloupnost oddělovačů řádků pro místo určení. Tento převod se v současné době projevuje pouze v následujících případech:</p> <ul style="list-style-type: none"> • Je-li uživatelem definovaný klíč metadat com.ibm.wmqfte.newRecordOnLineSeparator nastaven na hodnotu <code>false</code> a přenos je do souboru orientovaného na záznamy. • Je-li uživatelem definovaný klíč metadat com.ibm.wmqfte.com.ibm.wmqfte.insertRecordLineSeparator nastaven na hodnotu <code>false</code> a přenos je ze souboru orientovaného na záznamy. <p>Viz také fteCreateTransfer: zahájení nového přenosu souborů.</p>	ne
failTransferOnFirstSelhání	<p>Hodnota této vlastnosti může být <code>true</code> nebo <code>false</code>. Umožňuje konfiguraci agenta, aby selhal spravovaný přenos, jakmile dojde k selhání položky přenosu v rámci tohoto spravovaného přenosu.</p> <p>Chcete-li tuto funkci povolit, APAR IT03450 musí být použita pro zdrojového i cílového agenta a vlastnost failTransferOnFirstFailure musí být nastavena na hodnotu <code>true</code> v souboru <code>agent.properties</code> zdrojového agenta. Nastavení vlastnosti na hodnotu <code>true</code> v cílovém agentu je volitelné.</p> <p>Když je vlastnost failTransferOnFirstFailure nastavena na hodnotu <code>true</code>, agent začne zpracovávat spravované požadavky na přenos jako obvykle. Jakmile však dojde k selhání položky přenosu, spravovaný přenos bude označen jako nezdařený a nebudou zpracovány žádné další položky přenosu. Položky přenosu, které byly úspěšně zpracovány před selháním spravovaného přenosu, jsou zpracovány následujícím způsobem:</p> <ul style="list-style-type: none"> • Dispozice zdroje pro tyto položky přenosu je uznána. Pokud byla například zdrojová dispozice pro položku přenosu nastavena na hodnotu <code>delete</code>, bude zdrojový soubor odstraněn. • Cílové soubory, které byly zapsány, zůstávají v cílovém systému souborů a nejsou odstraněny. <p>Pokud není vlastnost failTransferOnFirstFailure nastavena na hodnotu <code>true</code> a spravovaný přenos souborů obsahuje více souborů a jeden z těchto souborů se nezdaří přenést, například protože cílový soubor již existuje a vlastnost přepisu je nastavena na <code>error</code>, zdrojový agent pokračuje a pokusí se přenést všechny zbývající soubory v požadavku.</p>	ne
itemsPerProgressMessage	<p>Počet přenesených souborů, než agent publikuje svou další zprávu protokolu průběhu. Tato vlastnost řídí rychlost, jakou jsou zprávy protokolu průběhu publikovány do koordinačního správce front během přenosu.</p> <p>Maximální hodnota, na kterou lze tuto vlastnost nastavit, je 1000.</p> <p>Poznámka: Zprávy o průběhu zahrnují informace o každém souboru, který byl přenesen od posledního publikování zprávy o průběhu. Zvýšení této hodnoty zvýší velikost zpráv o průběhu, což může ovlivnit výkon.</p>	50

Tabulka 72. Rozšířené vlastnosti agenta: Obecné (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
maxInlineFileSize	<p>V případě přenosů z jednoho souboru do souboru nebo ze souboru do zprávy se jedná o maximální velikost souboru (v bajtech), kterou lze automaticky zahrnout do počáteční zprávy požadavku na přenos.</p> <p>Pomocí této vlastnosti můžete zvýšit rychlost přenosů, ale pokud nastavíte velikost souboru na příliš velkou hodnotu, může to snížit výkon. Doporučená počáteční velikost této vlastnosti je 100 kB, ale doporučuje se důkladně otestovat různé hodnoty, dokud nenajdete nejlepší velikost souboru pro váš systém.</p> <p>Tato funkce je standardně vypnuta nebo nastavením vlastnosti maxInlineFileSize na hodnotu 0.</p>	0

Tabulka 73. Rozšířené vlastnosti agenta: Vysoká dostupnost		
Název vlastnosti	Popis	Výchozí hodnota
highlyAvailable	Tato vlastnost se čte během spuštění agenta a je-li nastavena na hodnotu <code>true</code> , agent se spustí v režimu vysoké dostupnosti. Pokud nevedete vlastnost nebo nastavíte hodnotu na <code>false</code> , agent se spustí jako agent, který není vysoce dostupný.	ne
standbyPollInterval	<p>Tuto vlastnost používá rezervní instance k pokusu o otevření sdílené fronty v určených intervalech.</p> <p>V produktu IBM MQ 9.3.0 tuto vlastnost také používají všechny instance k určení, jak dlouho instance čeká mezi pokusy o opětovné připojení, pokud se odpojí od svého správce front agenta.</p> <p>Pokusy se opakují, dokud se instance znovu nepřipojí ke svému správci front agenta, neotevře frontu <code>SYSTEM.FTE.HA.<agent name></code> (pokud se již zaregistrovala jako instance v pohotovostním režimu) nebo není zastavena příkazem fteStopAgent.</p>	5 sekund
standbyStatusDiscardTime	<p>Tato vlastnost nastavuje dobu trvání, po kterou aktivní instance čeká na publikování stavu z rezervní instance.</p> <p>Není-li z instance v pohotovostním režimu přijato žádné publikování, odebere aktivní instance informace o instanci v pohotovostním režimu ze seznamu instancí v pohotovostním režimu.</p> <p>Výchozí hodnota je dvakrát vyšší než hodnota vlastnosti standbyStatusPublishInterval, takže aktivní instance před odebráním rezervní instance ze seznamu čeká déle.</p>	600 sekund
standbyStatusVypršení platnosti	Tato vlastnost nastavuje dobu vypršení platnosti stavové zprávy v pohotovostním režimu, která je vložena do fronty příkazů agenta. Zpráva vyprší, pokud aktivní instance agenta nezpracuje tuto zprávu.	30 sekund
standbyStatusPublishInterval	Tato vlastnost se používá k nastavení frekvence, se kterou rezervní instance publikuje svůj stav.	300 sekund

Tabulka 74. Rozšířené vlastnosti agenta: Vstup/výstup		
Název vlastnosti	Popis	Výchozí hodnota
doNotUseTempOutputFile	<p>Standardně agent zapisuje do dočasného souboru v místě určení a přejmenuje tento dočasný soubor na požadovaný název souboru po dokončení přenosu souboru. Nastavení této hodnoty na <code>true</code> způsobí, že agent bude zapisovat přímo do konečného cílového souboru.</p> <p> Na systémech z/OS se toto chování nevztahuje na sekvenční datové sady, ale platí pro členy datové sady PDS.</p> <p>Hodnota této vlastnosti pro přenos je definována cílovým agentem.</p>	ne

Tabulka 74. Rozšířené vlastnosti agenta: Vstup/výstup (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
enableMandatoryzamykání	<p>Při přístupu k normálním souborům produkt Managed File Transfer vezme sdílený zámek pro čtení a vylučný zámek pro zápis.</p> <p>Windows Zamykání souboru Windows je pouze poradní. Je-li tato vlastnost nastavena na hodnotu true, produkt Managed File Transfer vynucuje zamykání souborů. V systému Windows to znamená, že pokud má jiná aplikace otevřený soubor, monitorování tohoto souboru se nespustí, dokud se soubor nezavře. Přenosy Managed File Transfer, které se týkají tohoto souboru, selhaly.</p> <p>UNIX Na platformách typu UNIX je zamykání souborů mezi procesy splněno. Na platformách typu UNIX nemá nastavení této vlastnosti žádný vliv.</p> <p>Tato vlastnost platí pouze pro běžné agenty Managed File Transfer. Produkt Managed File Transfer nepodporuje mechanismus zamykání souborů na souborovém serveru. Tato vlastnost proto nefunguje pro agenta mostu protokolů, protože při přenosu souboru agent mostu protokolů nezamyká soubor na souborovém serveru.</p> <p>Hodnota této vlastnosti může být true nebo false.</p>	ne
ioIdleThreadTimeout	<p>Doba v milisekundách, po kterou má vstupní/výstupní podproces systému souborů zůstat nečinný, než se podproces ukončí.</p> <p>V 9.3.0 z/OS V produktu IBM MQ 9.3.0 se tato vlastnost nevztahuje na agenty spuštěné na systému IBM MQ for z/OS.</p>	10000
Hloubka ioQueue	Maximální počet vstupních/výstupních požadavků pro zařazení do fronty.	10
ioThreadPoolSize	<p>Maximální počet dostupných vstupních/výstupních podprocesů systému souborů. Obvykle každý přenos používá vlastní vstupní/výstupní podproces systému souborů, ale pokud počet souběžných přenosů překročí tento limit, vstupní/výstupní podprocesy systému souborů jsou sdíleny mezi přenosy.</p> <p>Pokud se domníváte, že bude pravidelně docházet k více probíhajícím souběžným přenosům než hodnota ioThreadPoolSize, může dojít ke zlepšení zvýšením této hodnoty, takže každý přenos bude mít svůj vlastní podproces vstupu/výstupu systému souborů.</p>	10
textReplacementCharacterSequence	<p>V případě přenosu v textovém režimu platí, že pokud některý z bajtů dat nelze převést ze zdrojové kódové stránky na cílovou kódovou stránku, výchozí chování je pro selhání přenosu souborů.</p> <p>Nastavte tuto vlastnost tak, aby umožňovala úspěšné dokončení přenosu vložením zadané znakové hodnoty. Tato hodnota vlastnosti je jeden znak. Obvykle se pro všechny nemapovatelné znaky používá otazník (?). Použijte například tento formát textReplacementCharacterSequence=? kde otazník (?) je náhradní znak. Jako nahrazující znak nelze použít mezeru.</p>	Není

V 9.3.0

Tabulka 75. Rozšířené vlastnosti agenta: Protokol přenosu

Název vlastnosti	Popis	Výchozí hodnota
V 9.3.0 logTransfer	<p>Zapněte nebo vypněte protokolování přenosu.</p> <p>Možné hodnoty jsou:</p> <p>informace Povoluje informace protokolu vysoké úrovně přenosu. Toto je výchozí hodnota.</p> <p>střední Povoluje informace protokolu střední úrovně přenosu.</p> <p>Podrobně Povolí podrobné informace protokolu přenosu.</p> <p>off Vypne protokolování přenosu.</p>	informace
V 9.3.0 logTransferFileSize	Definuje maximální velikost souboru protokolu přenosu v megabajtech	20
V 9.3.0 logTransferSoubory	Definuje maximální počet přenosových souborů, které jsou uchovány před zrušením nejstaršího souboru.	5

Tabulka 76. Rozšířené vlastnosti agenta: Podpora více kanálů		
Název vlastnosti	Popis	Výchozí hodnota
agentMultipleChannelsEnabled	<p>Nastavení této vlastnosti na hodnotu <code>true</code> umožní produktu Managed File Transfer Agent odesílat zprávy přenosu dat přes více kanálů IBM MQ. V některých scénářích může nastavení této vlastnosti zlepšit výkon. Podporu více kanálů však povolte pouze v případě, že existuje prokazatelný přínos pro výkon. Pouze zprávy, které jsou vloženy do <code>SYSTEM.FTE.DATA.destinationAgentNázev</code> fronty jsou odesílány přes více kanálů. Chování všech ostatních zpráv zůstává nezměněno.</p> <p>Když nastavíte tuto vlastnost na hodnotu <code>true</code>, musíte také provést kroky konfigurace IBM MQ v jednom z následujících témat, abyste povolili podporu více kanálů:</p> <ul style="list-style-type: none"> Konfigurace agenta MFT pro více kanálů v klastru Konfigurace agenta MFT pro více kanálů: neklastrovaný <p>Dále musíte provést standardní kroky konfigurace IBM MQ, které jsou nezbytné pro agenta Managed File Transfer a které jsou podrobně popsány v části Konfigurace MFT pro první použití.</p> <p>Hodnota této vlastnosti může být <code>true</code> nebo <code>false</code>.</p>	ne
agentMessageBatchSize	Při konfiguraci s více kanály odesílá zdrojový agent datové zprávy pro přenos přes každý kanál na základě metody <code>round-robin</code> . Tato vlastnost řídí počet zpráv, které jsou v daném okamžiku odesílány po jednotlivých kanálech.	5

Tabulka 77. Rozšířené vlastnosti agenta: Správce front s více instancemi		
Název vlastnosti	Popis	Výchozí hodnota
agentQMGrPohotovost	<p>Název hostitele a číslo portu, které se používají pro připojení klienta, ve formátu IBM MQ CONNAME, pro rezervní instanci správce front agenta s více instancemi, který je definován <code>agentQMGr</code>. Například <code>host_name(port_number)</code></p> <p>Agent se pokusí připojit ke správci front v pohotovostním režimu, když zjistí chybu přerušení připojení, například MQRC 2009. Po připojení agenta ke správci front v pohotovostním režimu zůstane agent připojen, dokud nebude správce front v pohotovostním režimu nedostupný.</p>	Bez výchozí hodnoty

Tabulka 78. Rozšířené vlastnosti agenta: Řadič procesů		
Název vlastnosti	Popis	Výchozí hodnota
agentQMGrRetryInterval	Interval v sekundách mezi kontrolami dostupnosti správce front řadičem procesů agenta.	30
Počet maxRestart	Maximální počet restartů, ke kterým může dojít v časovém intervalu určeném hodnotou vlastnosti <code>maxRestartInterval</code> . Když je tato hodnota překročena, řadič procesů agenta zastaví restartování agenta a místo toho provede akci, která je založena na hodnotě vlastnosti <code>prodlevy maxRestart</code> .	4
maxRestartInterval	Interval v sekundách, po který agent měří, že se agent restartuje. Pokud počet restartů v tomto intervalu překročí hodnotu vlastnosti <code>maxRestartCount</code> , řadič procesů agenta zastaví restartování agenta. Místo toho řadič procesů agenta provede akci, která je založena na hodnotě vlastnosti <code>prodlevy maxRestart</code> .	120
Prodleva maxRestart	Určuje chování řadiče procesů agenta, když rychlost restartů agenta překročí hodnotu vlastností <code>intervalu maxRestartCount</code> a <code>maxRestart</code> . Zadáte-li hodnotu menší nebo rovnou nule, zastaví se řadič procesů agenta. Pokud uvedete hodnotu větší než nula, je to počet sekund, po který se má čekat, než se informace o historii restartování, které držel řadič procesů agenta, vynulují a agent se restartuje.	-1

Tabulka 79. Rozšířené vlastnosti agenta: Most protokolů		
Název vlastnosti	Popis	Výchozí hodnota
protocolBridgeCredentialConfiguratio n	Hodnota této vlastnosti je předána jako řetězec metodě <code>initialize()</code> tříd ukončení, které jsou určeny třídami <code>protocolBridgeCredentialExit</code> .	null
protocolBridgeCredentialExitClasses	Určuje seznam tříd oddělený čárkami, který implementuje uživatelskou proceduru pověření mostu protokolů. Další informace viz Mapování pověření pro souborový server pomocí tříd uživatelské procedury .	Žádné výchozí nastavení.

Tabulka 79. Rozšířené vlastnosti agenta: Most protokolů (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
protocolBridgeDataTimeout	Časový limit v milisekundách, po který agent mostu protokolů čeká na vytvoření datového připojení k serveru FTP nebo na přijetí dat ze serveru FTP prostřednictvím již zavedeného připojení. Nastavíte-li tuto vlastnost na hodnotu 0, agent mostu protokolů bude čekat neomezeně dlouho. Pokud časový limit uplyne, agent mostu protokolů zavře všechna existující datová připojení k serveru FTP a pokusí se vytvořit nové datové připojení před obnovením aktuálního přenosu. Pokud se pokus o zavedení nového datového připojení nezdaří, aktuální přenos také selže.	0
protocolBridgeLogoutBeforeOdpojit	Určuje, zda agent mostu protokolů před uzavřením relace FTP a odpojením odhlásí uživatele ze souborového serveru. Nastavíte-li tuto vlastnost na hodnotu <code>true</code> , agent mostu protokolů vydá na souborový server příkaz QUIT .	ne
protocolBridgePropertiesConfiguratio n	Předáno jako jedna z vlastností mostu do metody <code>initialize()</code> uživatelských tříd určených vlastností <code>protocolBridgeServerPropertiesExitClasses</code> .	Bez výchozí hodnoty
protocolBridgePropertiesExitClasses	Určuje seznam tříd oddělený čárkami, který implementuje uživatelskou proceduru vlastností serveru mostu protokolů. Další informace viz ProtocolBridgePropertiesExit2: Vyhledání vlastností souborového serveru protokolů .	Bez výchozí hodnoty

Tabulka 80. Rozšířené vlastnosti agenta: Protokolování agenta mostu protokolů		
Název vlastnosti	Popis	Výchozí hodnota
agentLog	Komponenta a operace dvojice klíčových hodnot pro povolení nebo zakázání protokolování příkazů a odpovědí FTP mezi agentem mostu protokolů a souborovými servery FTP/SFTP/FTPS. Příklad: agentLog=on Zapnout protokolování pro všechny komponenty agentLog=off Vypnout protokolování pro všechny komponenty agentLog=ftp=on, sftp=on, ftps=off Zapněte protokolování pro FTP a SFTP a vypněte pro FTPS	Bez výchozí hodnoty
agentLogFileSize	Definuje maximální velikost souboru zachycení v megabajtech. Stejně jako výchozí pro standardní velikost výchozího souboru trasování.	20
Soubory agentLog	Definuje maximální počet souborů zachycení, které jsou zachovány před zrušením nejstaršího souboru. V 9.3.0 <ul style="list-style-type: none"> Výchozí hodnota vlastnosti agenta agentLogFiles se změnila z 10 na 5. To znamená, že v systému IBM MQ 9.3.0, je-li nastavena výchozí hodnota, může existovat maximálně pět souborů protokolu událostí agenta mostu protokolů, počínaje soubory <code>agentevent0.log</code> až <code>agentevent4.log</code>. Tuto hodnotu však můžete v případě potřeby změnit. Pokud je agent migrován z verze starší než IBM MQ 9.3.0, měli byste ručně odstranit soubory <code>agentevent5.log</code> do <code>agentevent9.log</code>, pokud existují. Velikost každého souboru protokolu však zůstává 20 MB. 	V 9.3.0 V systému IBM MQ 9.3.0 je výchozí hodnota 5. Před hodnotou IBM MQ 9.3.0 je výchozí hodnota 10.
Filtr agentLog	Standardně zachycuje komunikaci se všemi servery FTP, ke kterým se agent připojuje. Příklad: <ul style="list-style-type: none"> Filtrovat podle hostitele/adresy IP <pre>host=ftpprod.ibm.com, ftp2.ibm.com host=9.182.*</pre> Filtrovat na základě metadat <pre>metadata="outbound files to xyz corp"</pre> 	*

Tabulka 81. Rozšířené vlastnosti agenta: Fronta		
Název vlastnosti	Popis	Výchozí hodnota
dynamicQueuePředpona	Tato vlastnost definuje předponu, která se má použít při vytváření dočasné dynamické fronty.	WMQFTE.*
modelQueueNázev	Tato vlastnost definuje název fronty modulu, která se má použít při vytváření dočasné dynamické fronty.	SYSTEM.DEFAULT.MODEL.QUEUE
publicationMDUser	ID uživatele MQMD, které má být přidruženo ke zprávám odesílaným za účelem publikování koordinačním správcem front. Pokud tuto vlastnost nenastavíte, bude ID uživatele MQMD nastaveno na základě pravidel IBM MQ pro nastavení ID uživatelů MQMD.	Bez výchozí hodnoty

Tabulka 82. Rozšířené vlastnosti agenta: Monitorování prostředků		
Název vlastnosti	Popis	Výchozí hodnota
monitorFilepathPlatformSeparator	Určuje, zda mají být použity oddělovače cest specifické pro platformu v rámci proměnné <code>\$FILEPATH</code> . Hodnota <code>true</code> používá oddělovače cest specifické pro platformu. Hodnota <code>false</code> používá na všech platformách oddělovač cesty UNIX ve stylu dopředného lomítka (<code>/</code>).	ano
monitorMaxResourcesInPoll	Uvádí maximální počet monitorovaných prostředků, které se mají spustit v každém intervalu výzev. Pokud například zadáte vzorek monitorování <code>*.txt</code> , interval výzev 10 sekund a nastavíte vlastnost <code>monitorMaxResourcesInPoll</code> na hodnotu 10, vlastnost <code>Poll</code> <code>monitorMaxResourcesIn</code> mezí agenta na spuštění maximálně 10 shod pro každý interval výzev. Odpovídající prostředky nad limit 10 jsou spuštěny v pozdějších intervalech výzev. Kromě toho můžete použít vlastnost <code>Poll</code> <code>monitorMaxResourcesInv</code> kombinací s odpovídajícím parametrem <code>-bs</code> v příkazu <code>fteCreateMonitor</code> , chcete-li například omezit každý interval výzev tak, aby spouštěl pouze jeden přenos. Hodnota menší nebo rovna nule znamená, že počet prostředků monitoru, které jsou spuštěny v intervalu výzev, je neomezený.	-1
monitorReportTriggerFail	Uvádí, zda jsou podmínky selhání, v prostředí a konfiguraci, které jsou zjištěny v monitoru, hlášeny jako zpráva protokolu do <code>SYSTEM.FTE</code> . Hodnota <code>true</code> protokoluje zprávy. Hodnota <code>false</code> neprotokoluje zprávy.	ano
monitorReportTriggerNotsplněn	Určuje, zda neuspokojený spouštěč odešle zprávu protokolu do <code>SYSTEM.FTE</code> , které obsahuje podrobnosti. Hodnota <code>true</code> protokoluje zprávy. Hodnota <code>false</code> neprotokoluje zprávy.	ne
monitorReportTriggerSatisfied	Určuje, zda splněný spouštěč odešle zprávu protokolu do <code>SYSTEM.FTE</code> , které obsahuje podrobnosti. Hodnota <code>true</code> protokoluje zprávy. Hodnota <code>false</code> neprotokoluje zprávy.	ne
monitorSilenceOnTriggerSelhání	Počet po sobě jdoucích selhání spouštěče monitoru prostředků před tím, než již nejsou hlášena selhání.	5
monitorStopOnInternalSelhání	Počet následných vnitřních podmínek FFDC monitoru prostředků, než monitor změní svůj stav na zastaveno.	10

Tabulka 83. Rozšířené vlastnosti agenta: Kořenový adresář

Název vlastnosti	Popis	Výchozí hodnota
commandPath	<p>Určuje sadu cest, pomocí kterých lze příkazy volat, a to pomocí jedné z následujících metod:</p> <ul style="list-style-type: none"> Úlohy agenta Ant fte: call Ant, fte: filecopy nebo fte: filemove Ve zprávě XML předané agentovi pomocí jednoho z podporovaných schémat XML příkazu Managed File Transfer Agent (například managedCall nebo managedTransfer). <p>Informace o platné syntaxi hodnoty vlastnosti commandPath viz commandPath MFT property.</p> <p>Důležité: Při nastavování této vlastnosti buďte velmi opatrní, protože jakýkoli příkaz v jednom z uvedených commandPath lze efektivně volat ze vzdáleného klientského systému, který je schopen odesílat příkazy agentovi. Z tohoto důvodu, při výchozím nastavení, když zadáte commandPath:</p> <ul style="list-style-type: none"> Jakékoli existující prostředí sandbox agenta je konfigurováno agentem při jeho spuštění, takže všechny adresáře commandPath jsou automaticky přidány do seznamu adresářů, které mají odepřený přístup pro přenos. Všechna existující uživatelská pískoviště se aktualizují při spuštění agenta, takže všechny adresáře commandPath (a jejich podadresáře) se přidávají jako prvky <exclude> do prvků <read> a <write>. Pokud není agent nakonfigurován pro použití sandboxů agenta nebo sandboxů uživatele, vytvoří se při spuštění agenta nový sandbox agenta, který má adresáře commandPath určené jako odepřené adresáře. <p>Hodnota této vlastnosti může obsahovat proměnné prostředí.</p> <p>Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.</p> <p>Chcete-li toto výchozí chování přepsat, můžete nastavit vlastnost addCommandPathToSandbox na hodnotu false.</p> <p>Důležité: Uvědomte si, že toto přepsání efektivně umožňuje klientovi přenést jakýkoli příkaz na systém agenta a volat příkaz, a proto by měl být používán s velkou opatrností.</p>	Žádný-nelze volat žádné příkazy
addCommandPathToPískoviště	<p>Určuje, zda mají být adresáře určené vlastností commandPath (a všechny jejich podadresáře) přidány do:</p> <ul style="list-style-type: none"> Odepřené adresáře pro existující prostředí sandbox agenta. Prvky <exclude> pro prvky <read> a <write> pro všechna definovaná uživatelská pískoviště. Nové prostředí sandbox agenta, pokud nebyl agent nakonfigurován buď s sandboxem agenta, nebo s jedním či více uživatelskými sandboxy. <p>Informace o platné syntaxi hodnoty vlastnosti commandPath viz commandPath vlastnost MFT.</p>	Pravda
additionalWildcardSandboxChecking	<p>Určuje, zda se mají provádět další kontroly přenosů se zástupnými znaky pro agenta, který byl nakonfigurován s uživatelem nebo sandboxem agenta, aby se omezila umístění, ze kterých může agent přenášet soubory.</p> <p>Je-li tato vlastnost nastavena na hodnotu true, je povolena další kontrola. Pokud se požadavek na přenos pokusí načíst umístění, které je mimo definovaný sandbox pro porovnávání souborů se zástupným znakem, přenos se nezdaří. Pokud v rámci jednoho požadavku na přenos existuje více přenosů a jeden z těchto požadavků se nezdaří kvůli pokusu o čtení umístění mimo pískoviště, celý přenos se nezdaří. Pokud kontrola selže, je příčina selhání uvedena v chybových zprávách (viz Další kontroly přenosů se zástupnými znaky).</p> <p>Je-li vlastnost vynechána nebo nastavena na hodnotu false, neprovádějí se žádné další kontroly přenosů se zástupnými znaky.</p>	Není
sandboxRoot	<p>Určuje sadu kořenových cest, které mají být zahrnuty a vyloučeny při použití pískoviště. Informace o této funkci naleznete v tématu Práce s MFT pískovišti agenta.</p> <p>Oddělte cesty pomocí oddělovače cesty specifického pro platformu. Cesty s předponou se znakem vykřičníku (!) označuje cesty vyloučené ze sandboxu. Tato funkce je užitečná, pokud chcete vyloučit podadresář pod zahrnutou kořenovou cestou.</p> <p>Vlastnost sandboxRoot není podporována na agentech mostu protokolů.</p> <p>Vlastnost sandboxRoot a vlastnost userSandboxes nelze zadat společně.</p> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí.</p> <p>Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.</p>	Žádný-žádné pískoviště







Tabulka 83. Rozšířené vlastnosti agenta: Kořenový adresář (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
transferRoot	Výchozí kořenový adresář pro relativní cesty, které jsou určeny pro agenta. Hodnota této vlastnosti může obsahovat proměnné prostředí. Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.	Domovský adresář uživatele, který spustil proces agenta.
transferRootHLQ	Výchozí HLQ (ID uživatele) pro neúplné datové sady určené pro agenta	Jméno uživatele, který spustil proces agenta.
userSandboxes	Omezte oblast systému souborů, do které mohou být soubory přenášeny a ze které mohou být přenášeny, na základě jména uživatele MQMD, který požaduje přenos. Další informace naleznete v tématu Práce s MFT uživatelskými pískovišti . Vlastnost userSandboxes není u agentů mostu protokolů podporována. Vlastnost sandboxRoot a vlastnost userSandboxes nelze zadat společně.	ne

Tabulka 84. Rozšířené vlastnosti agenta: Vlastnost plánovače





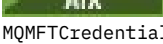

Název vlastnosti	Popis	Výchozí hodnota
maxSchedulerRunDelay	Maximální interval v minutách, po který agent čeká na kontrolu naplánovaných přenosů. Chcete-li tuto vlastnost povolit, zadejte kladné celé číslo. Další informace o tom, proč chcete tuto vlastnost použít, naleznete v tématu Co dělat v případě, že naplánovaný přenos souborů není spuštěn nebo je zpožděn . Vzhledem k tomu, že agent může číst příkaz ze své fronty příkazů v době, kdy mají naplánované přenosy proběhnout, může dojít k další prodlevě před spuštěním naplánovaných přenosů. V tomto případě se plánovač spustí okamžitě po dokončení tohoto příkazu.	-1

Tabulka 85. Rozšířené vlastnosti agenta: Zabezpečení

Název vlastnosti	Popis	Výchozí hodnota
agentCredentialsKeyFile	Název souboru obsahujícího klíč pověření použitý při šifrování pověření.	Vlastnost řetězce bez výchozí hodnoty.
agentQMGrAuthenticationCredentials	Cesta k souboru, který obsahuje pověření, která by měla být použita při připojování ke správci front agenta. Hodnota této vlastnosti může obsahovat proměnné prostředí. Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.  Podrobnosti o vytváření souborů pověření viz MFT a IBM MQ ověření připojení  Podrobnosti o vytvoření souboru ověřovacích pověření viz Konfigurace MQMFTCredentials.xml na webu z/OS .	Výchozí hodnota této vlastnosti je:    \$HOME/MQMFTCredentials.xml  %USERPROFILE%/MQMFTCredentials.xml
authorityChecking	Určuje, zda jsou povoleny funkce zabezpečení popsané v tématu Omezení oprávnění uživatelů na akcích agenta MFT . Oprávnění <code>inquire</code> je požadované oprávnění pro všechny fronty oprávnění agenta.	ne
logAuthorityKontroly	Úroveň protokolování kontroly oprávnění, která je zaznamenána v protokolu událostí agenta v souboru <code>output0.log</code> . Hodnoty, které tato vlastnost může mít, jsou Žádná nebo Selhání nebo Vše.	Není
userIdForClientConnect	ID uživatele, které je protékáno přes připojení klienta k produktu IBM MQ. Je-li zadána hodnota <code>java</code> , bude jméno uživatele hlášené prostředím JVM zadáno jako součást požadavku na připojení IBM MQ. Hodnoty, které tato vlastnost může mít, jsou Žádná nebo <code>java</code> .	Není

Tabulka 86. Rozšířené vlastnosti agenta: SSL/TLS




Název vlastnosti	Popis	Výchozí hodnota
agentSslCipherSpec	<p>Určuje použitý protokol, hašovací algoritmus a šifrovací algoritmus a počet bitů použitých v šifrovacím klíči při výměně dat mezi agentem a správcem front agenta.</p> <p>Hodnota agentSslCipherSpec je název CipherSpec . Tento název CipherSpec je stejný jako název CipherSpec použitý v kanálu správce front agenta. Seznam platných názvů CipherSpec je obsažen v specifikacích SSL/TLS CipherSpecs a CipherSuites ve třídách IBM MQ pro specifikace Java a SSL/TLS CipherSpecs a CipherSuites ve třídách IBM MQ pro JMS.</p> <p>agentSslCipherSpec je podobná položce agentSslCipherSuite. Pokud jsou zadány oba parametry agentSslCipherSuite a agentSslCipherSpec , použije se hodnota agentSslCipherSpec .</p>	Není
agentSslCipherSuite	<p>Určuje aspekty zabezpečení SSL způsobu výměny dat mezi agentem a správcem front agenta.</p> <p>Hodnota agentSslCipherSuite je název CipherSuite . Název CipherSuite se mapuje na název CipherSpec použitý v kanálu správce front agenta. Další informace viz CipherSuite a CipherSpec mapování názvů.</p> <p>agentSslCipherSuite je podobná položce agentSslCipherSpec. Pokud jsou zadány oba parametry agentSslCipherSuite a agentSslCipherSpec , použije se hodnota agentSslCipherSpec .</p>	Není
agentSslPeerName	<p>Určuje kostru rozlišujícího názvu, která se musí shodovat s názvem poskytnutým správcem front agenta. Rozlišující název se používá ke kontrole identifikačního certifikátu předloženého správcem front při připojení.</p>	Není
agentSslTrustStore	<p>Určuje umístění certifikátů, kterým agent důvěřuje. Hodnota agentSslTrustStore je cesta k souboru. Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\).</p> <p>Windows Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/).</p> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí.</p>	Není
agentSslKeyStore	<p>Určuje umístění soukromého klíče agenta. Hodnota agentSslKeyStore je cesta k souboru. Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\).</p> <p>Windows Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/). Tato vlastnost je vyžadována pouze v případě, že správce front agenta vyžaduje ověření klienta.</p> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí.</p>	Není
agentSslFipsRequired	<p>Uvádí, že chcete povolit podporu FIPS na úrovni agenta. Hodnota této vlastnosti může být <code>true</code> nebo <code>false</code>. Další informace viz Podpora FIPS v MFT.</p>	ne
agentSslKeyStoreTyp	<p>Typ úložiště klíčů SSL, které chcete použít. Úložiště klíčů JKS a PKCS#12 jsou podporována. Hodnota této vlastnosti může být buď <code>jks</code> , nebo <code>pkcs12</code>.</p>	JKS
agentSslKeyStoreCredentialsFile	<p>Cesta k souboru, který obsahuje pověření pro přístup k úložišti klíčů agenta. Hodnota této vlastnosti může obsahovat proměnné prostředí. Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.</p> <p>ALW Podrobnosti o vytváření souborů pověření viz MFT a IBM MQ ověření připojení</p> <p>z/OS Podrobnosti o vytvoření souboru ověřovacích pověření viz Konfigurace MQMFTCredentials.xml na webu z/OS.</p>	<p>Výchozí hodnota této vlastnosti je:</p> <p>Linux</p> <p>z/OS</p> <p>AIX \$HOME/MQMFTCredentials.xml</p> <p>Windows %USERPROFILE%/MQMFTCredentials.xml</p>
agentSslTrustStoreTyp	<p>Typ úložiště klíčů SSL, které chcete použít. Úložiště klíčů JKS a PKCS#12 jsou podporována. Hodnota této vlastnosti může být buď <code>jks</code> , nebo <code>pkcs12</code>.</p>	JKS

Tabulka 86. Rozšířené vlastnosti agenta: SSL/TLS (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
agentSslTrustStoreCredentialsFile	<p>Cesta k souboru, který obsahuje pověření pro přístup k úložišti údajů o důvěryhodnosti agenta.</p> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí. Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.</p> <p> Podrobnosti o vytváření souborů pověření viz MFT a IBM MQ ověření připojení</p> <p> Podrobnosti o vytvoření souboru ověřovacích pověření viz Konfigurace MQMFTCredentials.xml na webu z/OS.</p>	<p>Výchozí hodnota této vlastnosti je:</p> <p> Linux</p> <p> z/OS</p> <p> AIX \$HOME/MQMFTCredentials.xml</p> <p> Windows %USERPROFILE%/MQMFTCredentials.xml</p>

Tabulka 87. Rozšířené vlastnosti agenta: Časový limit		
Název vlastnosti	Popis	Výchozí hodnota
maxTransferNegotiationTime	<p>Maximální doba v milisekundách, po kterou přenos čeká na dokončení vyjednávání cílového agenta. Pokud se vyjednávání v této době nedokončí, přenos se uvede do stavu resynchronizace a umožní spuštění dalšího přenosu, je-li k dispozici.</p> <p>Ve scénářích, kde je zdrojový nebo cílový agent silně zatížen, je možné, že výchozí hodnota je příliš nízká na to, aby agent reagoval dostatečně rychle na požadavek na vyjednávání. Nejpravděpodobnější je, když má zdrojový agent definován velký počet monitorů prostředků nebo když jsou monitory prostředků monitorovány adresáře, které obsahují velký počet souborů. Může se však také vyskytnout, když je agentovi odeslán velký počet požadavků na přenos. V takových scénářích může být nezbytné zvýšit hodnotu této vlastnosti na 200 000 nebo více.</p>	30 000
recoverableTransferRetryInterval	Doba čekání v milisekundách mezi zjištěním opravitelné chyby přenosu a pokusem o obnovení přenosu.	60 000
senderTransferRetryInterval	Doba v milisekundách, po kterou se má čekat na zopakování odmítnutého přenosu, protože cíl již spouští maximální počet přenosů. Minimální hodnota je 1000.	30 000
Časový limit transferAck	<p>Časový limit v milisekundách, po který přenos čeká na potvrzení nebo data z druhého konce před opakovaním pokusu. Jedná se o rozšířenou vlastnost a pro většinu konfigurací produktu Managed File Transfer není nutné upravovat její hodnotu.</p> <p>Potvrzení se odesílají z přijímajícího agenta do odesílajícího agenta, kdykoli je přijato úplné okno dat. V případě sítí s omezením šířky pásma nebo nespolehlivých sítí a velkých nastavení agentWindowSize a agentChunkSize je možné, že výchozí nastavení není dostatečně dlouhé. To může způsobit zbytečný opětovný přenos dat mezi agenty. Proto může být zvýšení této hodnoty výhodné a může snížit pravděpodobnost, že přenos přejde do režimu obnovy kvůli pomalé síti.</p>	60 000
transferAckTimeoutRetries	Maximální počet opakovaných pokusů o potvrzení pro přenos bez odezvy, než se agent vzdá a přesune přenos do stavu obnovy	5
xmlConfigReloadInterval	<p>Interval v sekundách mezi opětovným načtením konfiguračních souborů XML agenta za běhu. Chcete-li agentovi zabránit v opětovném načtení konfiguračních souborů XML za běhu, nastavte tuto vlastnost na hodnotu -1. Následující konfigurační soubory XML jsou ovlivněny touto vlastností:</p> <ul style="list-style-type: none"> • ConnectDirectCredentials.xml • ConnectDirectNodeProperties.xml • ConnectDirectProcessDefinitions.xml • ProtocolBridgeCredentials.xml • ProtocolBridgeProperties.xml • UserSandboxes.xml 	30

Tabulka 88. Rozšířené vlastnosti agenta: Trasování a protokolování

Název vlastnosti	Popis	Výchozí hodnota
javaCoreTriggerFile	<p>Úplná cesta k umístění souboru, které agent monitoruje. Pokud soubor v zadaném umístění existuje, spuštění agenta spustí Javacore. Pokud po spuštění agenta aktualizujete soubor v tomto umístění, agent spustí soubor Javacore znovu.</p> <p>Samostatný podproces vyzývá tento soubor každých 30 sekund, aby zkontroloval, zda byl soubor vytvořen nebo aktualizován. Pokud byl soubor vytvořen nebo aktualizován od poslední výzvy, agent vygeneruje soubor Javacore v následujícím adresáři: <code>MQ_DATA_PATH/mqft/logs/coordination_qmgr_name/agents/agent_name</code></p> <p>Zadáte-li tuto vlastnost, agent při spuštění zobrazí následující zprávu:</p> <pre>BFGAG0092I The <insert_0> file will be used to request JVM diagnostic information.</pre> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí.</p> <p>Další informace viz "Použití proměnných prostředí ve vlastnostech MFT" na stránce 163.</p>	Není
trasování	<p>Specifikace trasování, která se má použít při spuštění agenta. Jedná se o čárkami oddělený seznam tříd a/nebo balíků, znak rovná se a úroveň trasování.</p> <p>Chcete-li například trasovat třídu <code>com.ibm.wmqfte.agent.Agent</code> a třídy v balíku <code>com.ibm.wmqfte.commandhandler</code> ze spuštění agenta, přidejte do souboru <code>agent.properties</code> následující položku:</p> <pre>trace=com.ibm.wmqfte.agent.Agent,com.ibm.wmqfte.commandhandler=all</pre> <p>V seznamu odděleném dvojtečkami můžete zadat více specifikací trasování. Například:</p> <pre>trace=com.ibm.wmqfte.agent.Agent=all:com.ibm.wmqfte.commandhandler=moderate</pre> <p>Speciální specifikace trasování <code>=all</code> se používá k trasování agenta a rozhraní JMQUI (Java Message Queuing Interface), které obsluhuje veškerou komunikaci se správcem front agenta. Chcete-li to povolit, přidejte do souboru <code>agent.properties</code> následující položku:</p> <pre>trace==all</pre> <p>Pokud zástupce podpory IBM neurčí jinak, použijte specifikaci trasování <code>com.ibm.wmqfte=all</code> takto:</p> <pre>trace=com.ibm.wmqfte=all</pre>	Není
Soubory outputLog	Celkový počet souborů <code>output.log</code> , které se mají uchovat. Tato hodnota platí pro řadič procesů agenta a samotného agenta.	5
outputLog-velikost	Maximální velikost každého souboru <code>output.log</code> v MB před vložením výstupu do dalšího souboru. Tato hodnota platí pro řadič procesů agenta a samotného agenta.	1
outputLogKódování	Kódování znaků, které agent používá při zápisu do souboru <code>output.log</code> .	Výchozí kódování znaků platformy, na které je agent spuštěn.
traceFiles	Celkový počet trasovacích souborů, které se mají uchovat. Tato hodnota se týká také řadiče procesů agenta a samotného agenta.	5
traceSize	Maximální velikost každého trasovacího souboru v MB před tím, než se trasování zalomí na další soubor. Tato hodnota platí pro řadič procesů agenta a samotného agenta.	20
traceMaxBajty	Omezení množství dat zprávy, která jsou výstupem v trasovacím souboru.	4096 bajtů
Obnova logTransfer	Je-li tato vlastnost nastavena na hodnotu <code>true</code> , vždy, když přenos zadá diagnostické události zotavení, jsou hlášeny do protokolu událostí agenta v souboru <code>output0.log</code> .	Pro systém IBM MQ 9.0.0.0 a novější je výchozí hodnota <code>true</code> .

Tabulka 88. Rozšířené vlastnosti agenta: Trasování a protokolování (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
logCapture	Zachytí zprávy požadavků na přenos, které jsou odeslány tomuto agentu, a zprávy protokolu, které agent publikuje do koordinačního správce front. Tyto zachycené zprávy mohou být užitečné při ladění problémů s přenosem. Zachycené zprávy jsou uloženy v souborech v adresáři protokolu agenta s názvem capture?.log. ? je číselná hodnota. Soubor obsahující číslo 0 obsahuje nejnovější zachycené zprávy.	ne
logCaptureFileSize	Definuje maximální velikost souboru zachycení v megabajtech.	10
Soubory logCapture	Definuje maximální počet souborů zachycení, které jsou zachovány před zrušením nejstaršího souboru.	10
Filtr logCapture	Regulární výraz Java, který agent používá pro shodu s názvem tématu zprávy. Zachyceny jsou pouze ty zprávy, které odpovídají regulárnímu výrazu.	* (odpovídá všem)
Protokol resourceMonitor	Dvojice klíčových hodnot monitoru prostředků a operace pro zapnutí nebo vypnutí protokolování. Možné hodnoty jsou: <ul style="list-style-type: none"> informace střední Podrobně off Příklad: <ul style="list-style-type: none"> resourceMonitorLog=MON1, MON2=info: MON3=off Zapněte protokolování pro MON1 a MON2 a vypněte protokolování pro MON3. resourceMonitorLog=info Zapněte protokolování na úrovni info pro všechny monitory prostředků. Protokoly monitoru prostředků se zapisují do souboru s názvem resmoneventN.log, kde N představuje číslo; například resmonevent0.log.  Upozornění: Všechny monitory prostředků agenta zapisují do stejného souboru protokolu. Další informace viz Protokolování monitorů prostředků MFT .	informace
resourceMonitorLogFile	Definuje maximální velikost souboru zachycení v megabajtech.	20
resourceMonitorLogFiles	Definuje maximální počet souborů zachycení, které jsou zachovány před zrušením nejstaršího souboru.  <ul style="list-style-type: none"> Výchozí hodnota vlastnosti agenta resourceMonitorLogFiles se změnila z 10 na 5. To znamená, že v systému IBM MQ 9.3.0, je-li nastavena výchozí hodnota, může existovat maximálně pět souborů protokolu událostí monitoru prostředků, počínaje soubory resmonevent0.log až po resmonevent4.log. Tuto hodnotu však můžete v případě potřeby změnit. Pokud je agent migrován z verze starší než IBM MQ 9.3.0, měli byste ručně odstranit soubory resmonevent5.log do resmonevent9.log, pokud existují. Velikost každého souboru protokolu však zůstává 20 MB. 	 V systému IBM MQ 9.3.0 je výchozí hodnota 5. Před hodnotou IBM MQ 9.3.0 je výchozí hodnota 10.

Tabulka 89. Rozšířené vlastnosti agenta: Limit přenosu		
Název vlastnosti	Popis	Výchozí hodnota
maxDestinationTransfers	Maximální počet souběžných přenosů, které cílový agent zpracuje v libovolném časovém okamžiku. Každý požadavek na přenos, který je odeslán agentovi, se započítává do tohoto celkového počtu bez ohledu na počet souborů, které jsou přeneseny k uspokojení požadavku. To znamená, že požadavek na přenos, který přenáší jeden soubor, se počítá stejným způsobem jako požadavek na přenos, který přenáší 10 souborů. Když cílový agent dosáhne limitu určeného vlastností maxDestinationTransfers, agent zařadí přenosy do fronty. Pokud součet následujících hodnot vlastností agenta: maxSourceTransfers + maxDestinationTransfers + maxQueuedTransfers překročí hodnotu nastavení MAXDEPTH u fronty stavového úložiště (SYSTEM.FTE.STATE.název agenta), agent se nespustí.	25 (pro všechny agenty kromě Connect:Direct) 5 (pro agenty mostu Connect:Direct)

Tabulka 89. Rozšířené vlastnosti agenta: Limit přenosu (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
maxFilesForTransfer	<p>Maximální počet položek přenosu, které jsou povoleny pro jeden spravovaný přenos. Pokud spravovaný přenos obsahuje více položek, než je hodnota maxFilesForTransfer, spravovaný přenos se nezdaří a nezpracují se žádné položky přenosu.</p> <p>Nastavení této vlastnosti vám zabrání v náhodném přenosu příliš mnoha souborů kvůli chybnému požadavku na přenos, například pokud uživatel náhodně určí přenos kořenového adresáře/na klíčové slovo conref=" ../common/mqent.dita#mqent/unixlinuxbis " /> systémy.</p>	5000
maxSourcePřenosy	<p>Maximální počet souběžných přenosů, které zdrojový agent zpracuje v libovolném časovém okamžiku. Každý požadavek na přenos, který je odeslán agentovi, se započítává do tohoto celkového počtu bez ohledu na počet souborů, které jsou přeneseny k uspokojení požadavku. To znamená, že požadavek na přenos, který přenáší jeden soubor, se počítá stejným způsobem jako požadavek na přenos, který přenáší 10 souborů.</p> <p>Zdrojový agent zařazuje přenosy do fronty, když cílový agent dosáhne limitu určeného vlastností maxSourceTransfers.</p> <p>Pokud součet následujících hodnot vlastností agenta: maxSourceTransfers + maxDestinationTransfers + maxQueuedTransfers překročí hodnotu nastavení MAXDEPTH u fronty stavového úložiště (SYSTEM.FTE.STATE.název agenta), agent se nespustí.</p>	<p>25 (pro všechny agenty kromě agentů mostu Connect:Direct)</p> <p>5 (pro agenty mostu Connect:Direct)</p>
maxQueuedPřenosy	<p>Maximální počet nevyřízených přenosů, které může zdrojový agent zařadit do fronty, dokud agent neodmítne nový požadavek na přenos. Tuto vlastnost můžete nastavit tak, aby navzdory omezením maxDestinationTransfers a maxSourceTransferům, které jsou splněny nebo překročeny, byly všechny nové požadavky na přenos, které nyní provedete, přijaty, zařazeny do fronty a poté provedeny později.</p> <p>Pořadí, ve kterém jsou požadavky na přenos ve frontě zpracovány, je faktorem jejich priority a délky jejich zařazení do fronty. Nejprve jsou vybrány nevyřízené přenosy se starou a vysokou prioritou. Přenosy s nízkou prioritou, které byly ve frontě dlouhou dobu, jsou vybrány přednostně před novějšími přenosy s vyšší prioritou.</p> <p>Pokud součet následujících hodnot vlastností agenta: maxSourceTransfers + maxDestinationTransfers + maxQueuedTransfers překročí hodnotu nastavení MAXDEPTH u fronty stavového úložiště (SYSTEM.FTE.STATE.název agenta), agent se nespustí.</p>	1000

Tabulka 90. Rozšířené vlastnosti agenta: Časový limit obnovy přenosu		
Název vlastnosti	Popis	Výchozí hodnota
Časový limit transferRecovery	<p>Nastavte dobu v sekundách, během které se zdrojový agent neustále pokouší obnovit pozastavený přenos souborů.</p> <p>Není-li vlastnost nastavena, je výchozím chováním agenta pokračovat v opakování, dokud se úspěšně neobnoví přenos. Pro vlastnost časového limitu obnovy přenosu můžete nastavit následující hodnoty:</p> <p>-1 Agent se nadále pokouší obnovit pozastavený přenos, dokud není přenos dokončen. Použití této volby je ekvivalentem výchozího chování agenta, když není vlastnost nastavena.</p> <p>0 Agent zastaví přenos souborů, jakmile vstoupí do obnovy.</p> <p>>0 Agent se nadále pokouší obnovit pozastavený přenos po dobu v sekundách nastavenou uvedenou kladnou celočíselnou hodnotou. Například transferRecoveryTimeout=21600 označuje, že se agent stále pokouší obnovit přenos po dobu 6 hodin od okamžiku, kdy vstoupí do obnovy. Maximální hodnota tohoto parametru je 99999999 . .</p>	-1

Tabulka 91. Rozšířené vlastnosti agenta: Uživatelská procedura		
Název vlastnosti	Popis	Výchozí hodnota
agentForceConsistentPathDelimiters	Vynutí, aby oddělovačem cesty v informacích o zdrojovém a cílovém souboru, které jsou poskytnuty pro uživatelské procedury přenosu, byl styl UNIX : dopředné lomítko (/). Platné volby jsou true a false.	ne
destinationTransferEndExitTřidy	Určuje seznam tříd oddělených čárkami, které implementují cílovou uživatelskou proceduru přenosu.	Bez výchozí hodnoty



Tabulka 91. Rozšířené vlastnosti agenta: Uživatelská procedura (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
destinationTransferStartExitTřídy	Určuje seznam tříd oddělených čárkami, které implementují uživatelskou proceduru spuštění přenosu cíle.	Bez výchozí hodnoty
exitClassCesta	Určuje seznam adresářů specifických pro konkrétní platformu, oddělených znaky, které slouží jako cesta ke třídám pro uživatelské procedury. Adresář uživatelských procedur agenta se prohledává před všemi položkami v této cestě ke třídám.	Adresář exits agenta
exitNativeLibraryPath	Určuje seznam adresářů, které se chovají jako cesta k nativní knihovně pro uživatelské procedury, oddělených znaky pro konkrétní platformu.	Adresář exits agenta
ioMaxRecordLength	Maximální délka záznamu v bajtech, která může být podporována pro soubor orientovaný na záznamy. Produkt Managed File Transfer může podporovat zápis do záznamově orientovaných souborů s libovolnou délkou záznamu. Avšak velké délky záznamů mohou způsobit chyby nedostatku paměti, takže abyste se vyvarovali těchto chyb, maximální délka záznamu je standardně omezena na 64 K. Při čtení ze souborů orientovaných na záznamy se musí celý záznam vejít do jednoho bloku přenosu, proto je délka záznamu navíc omezena velikostí bloku přenosu. Tato vlastnost se používá pouze pro soubory orientované na záznamy uživatelské procedury I/O.	64 kB
monitorExitClasses	Určuje seznam tříd oddělených čárkami, který implementuje uživatelskou proceduru monitoru. Další informace viz Uživatelské procedury monitoru prostředků produktu MFT .	Bez výchozí hodnoty
protocolBridgeCredentialExitClasses	Určuje seznam tříd oddělených čárkami, který implementuje uživatelskou proceduru pověření mostu protokolů. Další informace viz Mapování pověření pro souborový server pomocí tříd uživatelské procedury .	Žádné výchozí nastavení.
sourceTransferEndExitTřídy	Určuje seznam tříd, které implementují uživatelskou proceduru ukončení přenosu zdroje, oddělených čárkami.	Bez výchozí hodnoty
sourceTransferStartExitTřídy	Určuje seznam tříd oddělených čárkami, které implementují uživatelskou proceduru spuštění přenosu zdroje.	Bez výchozí hodnoty
IOExitClasses	Určuje seznam tříd oddělených čárkami, který implementuje uživatelskou proceduru I/O. Vypište pouze ty třídy, které implementují rozhraní IOExit, tj. neuvádějte třídy, které implementují ostatní rozhraní uživatelské procedury I/O, například IOExitResourcePath a IOExitChannel. Další informace viz Použití uživatelských procedur I/O přenosu MFT .	Žádné výchozí nastavení.

Tabulka 92. Rozšířené vlastnosti agenta: Komprese klienta IBM MQ		
Název vlastnosti	Popis	Výchozí hodnota
agentDataKomprese	Tato vlastnost je podporována pouze pro připojení klienta. Čárkami oddělený seznam typů komprese pro přenos dat souboru pro vyjednávání se vzdáleným serverem IBM MQ . Informace o těchto typech komprese naleznete v následujícím tématu: Seznam komprese dat zpráv . Hodnoty jsou zkontrolovány na platnost a poté předány v pořadí podle vzhledu jako vlastnosti kanálu klienta agenta. Klient IBM MQ poté zpracovává vyjednávání mezi tímto kanálem klienta a kanálem vzdáleného serveru, aby našel odpovídající nejnižší společný jmenovatel mezi vlastnostmi komprese na obou kanálech. Pokud není nalezena žádná shoda, je vždy vybrána volba MQCOMPRESS_NONE.	MQCOMPRESS_NONE
agentHeaderKomprese	Tato vlastnost je podporována pouze pro připojení klienta. Seznam typů komprese oddělených čárkami pro přenos dat záhlaví pro vyjednávání se vzdáleným serverem IBM MQ . Přijaté hodnoty jsou MQCOMPRESS_NONE nebo MQCOMPRESS_SYSTEM. Informace o těchto typech komprese naleznete v následujícím tématu: HdrCompSeznam [2] (MQLONG) . Hodnoty jsou zkontrolovány na platnost a poté předány v pořadí podle vzhledu jako vlastnosti kanálu klienta agenta. Klient IBM MQ poté zpracovává vyjednávání mezi tímto kanálem klienta a kanálem vzdáleného serveru, aby našel odpovídající nejnižší společný jmenovatel mezi vlastnostmi komprese na obou kanálech. Pokud není nalezena žádná shoda, je vždy vybrána volba MQCOMPRESS_NONE.	MQCOMPRESS_NONE

Tabulka 93. Rozšířené vlastnosti agenta: z/OS-specific

Název vlastnosti	Popis	Výchozí hodnota
adminGroup	<p>Skupina správců zabezpečení. Členové této skupiny mohou:</p> <ul style="list-style-type: none"> Spustíte agenta pomocí příkazu fteStartAgent. Zastavíte agenta pomocí příkazu fteStopAgent. Zapnete nebo vypnete trasování pro agenta pomocí příkazu fteSetAgentTraceLevel. Zapnete nebo vypnete protokoly pro agenta pomocí příkazu fteSetAgentLogLevel. Zobrazíte podrobnosti lokálního agenta spuštěním příkazu fteShowAgentDetails s uvedeným parametrem -d. <p>Definujte skupinu správce zabezpečení, například MFTADMIN, a pak do této skupiny přidejte ID uživatele spuštěné úlohy a ID TSO administrátora. Upravte soubor vlastností agenta a nastavte vlastnost adminGroup na název této skupiny správců zabezpečení.</p> <pre>adminGroup=MFTADMIN</pre>	Není
bpxwdynAllocAdditionalOptions	<p>Produkt Managed File Transfer používá textové rozhraní BPXWDYN k vytvoření a otevření datových sad z/OS. Když se BPXWDYN používá pro přidělení datové sady ve výchozím nastavení, Managed File Transfer zajišťuje, pokud je to možné, připojení datového zařízení (není vyžadováno pro datové sady založené na disku, ale je vyžadováno pro datové sady pásek). Vzhledem k tomu, že volby nemusí být pro určitá prostředí podporovány, použijte tuto vlastnost ke změně tohoto chování. Při přenosu do datové sady je také možné zadat volby pro BPXWDYN na příkazovém řádku; tyto volby jsou navíc k volbám určeným touto vlastností.</p> <p>Při použití vlastnosti bpxwdynAllocAdditionalOptions v souboru <code>agent.properties</code> nesmí být zadány některé volby BPXWDYN. Seznam těchto vlastností naleznete v tématu Vlastnosti BPXWDYN, které se nesmí používat s MFT.</p>	<p>Výchozí nastavení je následující:</p> <ul style="list-style-type: none"> MOUNT pro z/OS V1R8 a novější
armELEMTYPE	<p>Volitelná vlastnost. Pokud je agent konfigurován pro restart správcem ARM (Automatic Restart Manager), nastavte tuto vlastnost na hodnotu parametru ARM ELEMTYPE určenou v přidružené zásadě ARM. Pro agenta nastavte ELEMTYPE na SYSBFGAG.</p>	Nenastaveno
armELEMENT	<p>Volitelná vlastnost. Pokud je agent konfigurován pro restart správcem ARM (Automatic Restart Manager), nastavte tuto vlastnost na hodnotu parametru ARM ELEMENT určenou v přidružené zásadě ARM. Hodnotu ELEMENT můžete nastavit tak, aby odpovídala názvu agenta.</p>	Nenastaveno

Tabulka 94. Rozšířené vlastnosti agenta: Jiné vlastnosti

Název vlastnosti	Popis	Výchozí hodnota
  legacyXMLMessageFormát MQMDFormat	<p>Managed File Transfer Zprávy XML generované agentem (například zprávy o průběhu protokolu a přenosu) jsou nyní odesílány do fronty s prázdným polem formátu MQMD. Předchozí verze produktu nastavily pole formátu MQMD na hodnotu MQSTR (textový řetězec zprávy). Nastavení této vlastnosti na hodnotu true povolí odesílání zpráv XML Managed File Transfer generovaných agentem do fronty s polem formátu MQMD MQSTR.</p> <p>Poznámka: Zprávy odpovědi agenta na příkazy budou odeslány s formátem zprávy, který odpovídá odpovídajícímu požadavku příkazu.</p> <p>Je-li pole formátu MQMD nastaveno na hodnotu MQSTR, může dojít k poškození zpráv XML příkazu Managed File Transfer, pokud jsou v síti produktu MQ kanály s povoleným převodem dat.</p>	ne
adjustScheduleTimeForDaylightSavin g	<p>Pokud váš podnik spouští naplánované přenosy každý den, protože plánovaný přenos byl vytvořen s:</p> <ul style="list-style-type: none"> Parametr -oi je nastaven na dny a Parametr -tb nastaven na zdroj <p>v příkazu <code>fteCreateTransfer</code> například po nastavení této vlastnosti na hodnotu <code>true</code> se plánovaný čas přenosu přesune o hodinu dopředu, když se hodiny posunou o hodinu dopředu a o hodinu zpět, když se hodiny vrátí o hodinu zpět.</p> <p>Pokud má být například naplánovaný přenos spuštěn v 1:00, když se hodiny přesunou vpřed, přenos se spustí ve 2:00 a když se hodiny vrátí zpět, přenos se vrátí do 1:00.</p>	ano

Související pojmy

[Volby konfigurace MFT na platformě Multiplatforms](#)

[Volba časového limitu pro přenosy souborů při obnově](#)

[MFT pískoviště](#)

Související úlohy

[Konfigurace agenta MFT pro více kanálů v klastru](#)

[Konfigurace agenta MFT pro více kanálů: neklastrovaný](#)

Související odkazy

[“Java systémové vlastnosti pro MFT” na stránce 212](#)

Řada vlastností příkazu Managed File Transfer a agenta musí být definována jako systémové vlastnosti Java , protože definují konfiguraci pro funkci typu early (dřívější), která nemůže používat mechanismus vlastností příkazu nebo agenta.

[Vlastnosti SSL/TLS pro MFT](#)

[“Soubor MFT command.properties” na stránce 195](#)

Soubor `command.properties` uvádí správce front příkazů, ke kterému se chcete připojit při zadávání příkazů, a informace, které produkt Managed File Transfer vyžaduje pro kontaktování tohoto správce front.

[“Soubor MFT coordination.properties” na stránce 191](#)

Soubor `coordination.properties` uvádí podrobnosti připojení ke koordinačnímu správci front. Vzhledem k tomu, že několik instalací produktu Managed File Transfer může sdílet stejného koordinačního správce front, můžete použít symbolický odkaz na společný soubor `coordination.properties` na sdílené jednotce.

[“Soubor MFT logger.properties” na stránce 199](#)

Modul protokolování Managed File Transfer má sadu vlastností konfigurace. Tyto vlastnosti zadejte v souboru `logger.properties` , který se nachází v adresáři `MQ_DATA_PATH/mqft/config/coordination_qmgr_name/loggers/logger_name` .

[fteCreateAgent](#)

[fteCreateBridgeAgent](#)

[fteCreateCDAgent](#)

[“Použití proměnných prostředí ve vlastnostech MFT” na stránce 163](#)

Je možné, aby se proměnné prostředí používaly ve vlastnostech Managed File Transfer , které představují umístění souborů nebo adresářů. To umožňuje, aby se umístění souborů nebo adresářů používaných při spouštění částí produktu lišila v závislosti na aktuálním prostředí (například uživatel spouštějící příkaz).

Soubor MFT coordination.properties

Soubor `coordination.properties` uvádí podrobnosti připojení ke koordinačnímu správci front. Vzhledem k tomu, že několik instalací produktu Managed File Transfer může sdílet stejného koordinačního správce front, můžete použít symbolický odkaz na společný soubor `coordination.properties` na sdílené jednotce.

Soubor `coordination.properties` je vytvořen instalačním programem nebo příkazem **fteSetupCoordination** . Pomocí příkazu **fteSetupCoordination** s příznakem **-f** můžete změnit vlastnosti základního koordinačního správce front v tomto souboru. Chcete-li změnit nebo přidat rozšířené vlastnosti koordinačního správce front, musíte upravit soubor v textovém editoru.

Soubor `coordination.properties` je umístěn v adresáři `MQ_DATA_PATH/mqft/config/coordination_qmgr_name` .

Soubor MFT `coordination.properties` obsahuje následující hodnoty:

Název vlastnosti	Popis	Výchozí hodnota
<code>coordinationCredentialsKeyFile</code>	Název souboru obsahujícího klíč pověření použitý při šifrování pověření.	Vlastnost řetězce bez výchozí hodnoty.
<code>coordinationQMgr</code>	Název koordinačního správce front.	Bez výchozí hodnoty

Tabulka 95. Základní vlastnosti koordinačního správce front (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
coordinationQMGrHostitel	Název hostitele nebo adresa IP koordinačního správce front.	Bez výchozí hodnoty
coordinationQMGrPort	Číslo portu použité pro připojení klienta ke koordinačnímu správci front.	1414
coordinationQMGrKanal	Název kanálu SVRCONN použitý pro připojení ke koordinačnímu správci front.	SYSTEM.DEF.SVRCONN

Pokud nezádáte hodnotu pro vlastnost hostitele coordinationQMGr, použije se standardně režim vazeb.


Pokud zadáte hodnotu pro vlastnost hostitele coordinationQMGr, ale nezádáte hodnoty pro vlastnosti kanálu coordinationQMGrPort a coordinationQMGr, číslo portu 1414 a kanál SYSTEM.DEF.SVRCONN .

Zde je příklad obsahu souboru coordination.properties :

```
coordinationQMGr=ERIS
coordinationQMGrHost=kuiper.example.com
coordinationQMGrPort=2005
coordinationQMGrChannel=SYSTEM.DEF.SVRCONN
```

V tomto příkladu je ERIS název IBM MQ správce front, který je umístěn v systému kuiper.example.com. Správce front ERIS je správce front, kterému produkt Managed File Transfer odesílá informace protokolu.

Rozšířené vlastnosti koordinace

Produkt Managed File Transfer také poskytuje rozšířené vlastnosti koordinace. Chcete-li použít některou z následujících vlastností, ručně upravte soubor coordination.properties a přidejte požadované rozšířené vlastnosti. Závorky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\).  Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/). Další informace o řídicím znaku v souborech vlastností Java naleznete v dokumentaci Oracle [Javadoc pro třídu vlastností](#).

- [Vlastnosti agenta](#)
- [Vlastnosti kódové stránky](#)
- [Vlastnosti připojení](#)
- [Vlastnosti správce front pro více instancí](#)
- [Vlastnosti fronty](#)
- [Vlastnosti zabezpečení](#)
- [Vlastnosti SSL](#)
- [Vlastnosti odběru](#)



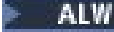
Tabulka 96. Rozšířené vlastnosti koordinace: Agent		
Název vlastnosti	Popis	Výchozí hodnota
agentStatusJitterTolerance	<p>Maximální doba, po kterou může být publikování stavových zpráv agenta zpožděno, než je zpráva považována za prošlou. Tato hodnota se měří v milisekundách.</p> <p>Stáří stavové zprávy je založeno na čase, kdy byla publikována v koordinačním správci front. Zpráva je však vyslána agentem určitou dobu před jejím přijetím koordinačním správcem front, aby byla zajištěna doba potřebná k cestování po síti IBM MQ . Pokud tento přenos trvá vždy stejné množství času, zprávy vytvořené od sebe 60 sekund jsou publikovány 60 sekund od sebe, bez ohledu na skutečný čas v přenosu. Pokud se však doba přenosu mezi zprávami liší, mohou být vytvořeny v 60sekundových intervalech, ale publikovány v intervalech, například 61, 59, 58 a 62 sekund. Maximální odchylka od 60, 2 sekundy v tomto příkladu je kolísání. Tato vlastnost určuje maximální prodlevu kvůli kolísání před tím, než je zpráva považována za prošlé.</p>	3000

Tabulka 97. Rozšířené vlastnosti koordinace: Kódová stránka		
Název vlastnosti	Popis	Výchozí hodnota
coordinationCcsid	Kódová stránka, se kterou se příkazy připojují ke koordinačnímu správci front. Také veškerá publikování do koordinačního správce front provedená agentem jsou prováděna s touto kódovou stránkou. Pokud zadáte hodnotu pro coordinationCcsid, musíte také zadat hodnotu pro název coordinationCcsid.	1208
coordinationCcsidNázev	Java reprezentace coordinationCcsid. Pokud zadáte hodnotu pro název coordinationCcsid, musíte také zadat hodnotu pro coordinationCcsid.	UTF8



Tabulka 98. Rozšířené koordinační vlastnosti: Připojení		
Název vlastnosti	Popis	Výchozí hodnota
Cesta javaLibrary	Při připojování ke správci front v režimu vazeb Managed File Transfer musí mít přístup ke knihovnám vazeb produktu IBM MQ Java. Standardně produkt Managed File Transfer vyhledává knihovny vazeb ve výchozím umístění definovaném pomocí IBM MQ. Pokud se knihovny vazeb nacházejí v jiném umístění, použijte tuto vlastnost k určení umístění knihoven vazeb.	MQ_INSTALLATION_PATH/ java/lib

Tabulka 99. Rozšířené vlastnosti koordinace: Správce front pro více instancí		
Název vlastnosti	Popis	Výchozí hodnota
coordinationQMgrPohotovost	Název hostitele a číslo portu použité pro připojení klienta ve formátu IBM MQ CONNAME pro rezervní instanci koordinačního správce front s více instancemi definovaného vlastností coordinationQMgr. Například <i>host_name(port_number)</i>	Bez výchozí hodnoty

Tabulka 100. Rozšířené vlastnosti koordinace: Fronta		
Název vlastnosti	Popis	Výchozí hodnota
dynamicQueuePředpona	Tato vlastnost definuje předponu IBM MQ, která se má použít pro generování dočasných názvů fronty. Formát vlastnosti předpony dynamicQueue odpovídá formátu pole DynamicQName struktury IBM MQ MQOD. Další informace naleznete v tématu Vytvoření dynamických front . Tuto vlastnost můžete také definovat v souboru <code>command.properties</code> , chcete-li použít specifickou předponu IBM MQ pro dočasné fronty odpovědí generované příkazy, které vyžadují odezvu od agenta.	WMQFTE.*
modelQueueNázev	Tato vlastnost definuje modelovou frontu IBM MQ, která se má použít pro generování dočasných fronty. Tuto vlastnost můžete také definovat v souboru <code>command.properties</code> , pokud chcete použít specifickou modelovou frontu IBM MQ pro dočasné fronty odpovědí generované příkazy, které vyžadují odpověď od agenta. Další informace viz téma "Soubor MFT <code>command.properties</code> " na stránce 195.	SYSTEM.DEFAULT.MODEL.QUEUE

Tabulka 101. Rozšířené koordinační vlastnosti: Zabezpečení		
Název vlastnosti	Popis	Výchozí hodnota
userIdForClientConnect	ID uživatele, které je protékáno přes připojení klienta k produktu IBM MQ. Je-li zadáno <i>java</i> , bude jméno uživatele hlášené prostředím JVM zadáno jako součást požadavku na připojení IBM MQ. Hodnota této vlastnosti může být žádná nebo <i>java</i> .	Není
coordinationQMgrAuthenticationCredentials	Cesta k souboru, který obsahuje pověření připojení produktu MQ pro připojení ke koordinačnímu správci front.	 Podrobnosti o vytvoření souboru ověřovacích pověření viz Konfigurace MQMFTCredentials.xml na webu z/OS .  Informace o umístění a oprávněních tohoto souboru viz Konfigurace MQMFTCredentials.xml.  Další podrobnosti o vytvoření souboru ověřovacích pověření jsou v adresáři MFT a IBM MQ ověření připojení .

Tabulka 102. Rozšířené koordinační vlastnosti: SSL/TLS

Název vlastnosti	Popis	Výchozí hodnota
coordinationSslCipherSpec	<p>Určuje použitý protokol, hašovací algoritmus a šifrovací algoritmus a počet bitů použitých v šifrovacím klíči při výměně dat mezi příkazy a koordinačním správcem front.</p> <p>Hodnota <code>coordinationSslCipherSpec</code> je název <code>CipherSpec</code>. Tento název <code>CipherSpec</code> je stejný jako název <code>CipherSpec</code> používaný v kanálu koordinačního správce front. Seznam platných názvů <code>CipherSpec</code> je obsažen v specifikacích SSL/TLS CipherSpecs a CipherSuites ve třídách IBM MQ pro specifikace Java a SSL/TLS CipherSpecs a CipherSuites ve třídách IBM MQ pro JMS.</p> <p><code>coordinationSslCipherSpec</code> je podobná položce <code>coordinationSslCipherSuite</code>. Pokud jsou zadány oba parametry <code>coordinationSslCipherSuite</code> a <code>coordinationSslCipherSpec</code>, použije se hodnota <code>coordinationSslCipherSpec</code>.</p>	Není
coordinationSslCipherSuite	<p>Určuje aspekty zabezpečení SSL týkající se způsobu, jakým si příkazy a koordinační správce front vyměňují data.</p> <p>Hodnota <code>coordinationSslCipherSuite</code> je název <code>CipherSuite</code>. Název <code>CipherSuite</code> se mapuje na název <code>CipherSpec</code> použitý v kanálu správce front agenta. Další informace viz CipherSuite a CipherSpec mapování názvů.</p> <p><code>coordinationSslCipherSuite</code> je podobná položce <code>coordinationSslCipherSpec</code>. Pokud jsou zadány oba parametry <code>coordinationSslCipherSuite</code> a <code>coordinationSslCipherSpec</code>, použije se hodnota <code>coordinationSslCipherSpec</code>.</p>	Není
coordinationSslPeerName	<p>Určuje kostru rozlišujícího názvu, která se musí shodovat s názvem poskytovaným koordinačním správcem front. Rozlišující název se používá ke kontrole identifikačního certifikátu, který je prezentován koordinačním správcem front při připojení.</p>	Není
coordinationSslTrustStore	<p>Určuje umístění certifikátů, kterým příkazy důvěřují. Hodnota <code>coordinationSslTrustStore</code> je cesta k souboru. Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\).</p> <p> Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/). Tato vlastnost je vyžadována pouze v případě, že koordinační správce front vyžaduje ověřování klienta.</p> <p>V produktu IBM WebSphere MQ 7.5 nebo novějším může hodnota této vlastnosti obsahovat proměnné prostředí.</p>	Není
coordinationSslTrustStore	<p>Typ úložiště klíčů SSL, které chcete použít. Úložiště klíčů JKS a PKCS#12 jsou podporována. Hodnota této vlastnosti může být buď <code>jks</code>, nebo <code>pkcs12</code>.</p>	JKS
coordinationSslTrustStoreCredentialsFile	<p>Cesta k souboru, který obsahuje pověření <code>coordinationSslTrustStore</code>. Hodnota této vlastnosti může obsahovat proměnné prostředí.</p>	Výchozí hodnota této vlastnosti je <code>%USERPROFILE%/MQMFTcredentials.xml</code> na systému Windows a <code>\$HOME/MQMFTcredentials.xml</code> na jiných platformách.
coordinationSslKeyStore	<p>Určuje umístění soukromého klíče příkazů. Hodnota <code>coordinationSslKeyStore</code> je cesta k souboru. Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\).</p> <p> Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/). Tato vlastnost je vyžadována pouze v případě, že koordinační správce front vyžaduje ověřování klienta.</p> <p>Hodnota této vlastnosti může obsahovat proměnné prostředí.</p>	Není
coordinationSslKeyStore	<p>Typ úložiště klíčů SSL, které chcete použít. Úložiště klíčů JKS a PKCS#12 jsou podporována. Hodnota této vlastnosti může být buď <code>jks</code>, nebo <code>pkcs12</code>.</p>	JKS
coordinationSslKeyStoreCredentialsFile	<p>Cesta k souboru, který obsahuje pověření <code>coordinationSslKeyStore</code>. Hodnota této vlastnosti může obsahovat proměnné prostředí.</p>	Výchozí hodnota této vlastnosti je <code>%USERPROFILE%/MQMFTcredentials.xml</code> na systému Windows a <code>\$HOME/MQMFTcredentials.xml</code> na jiných platformách.
coordinationSslFipsRequired	<p>Určuje, že chcete povolit podporu FIPS na úrovni koordinačního správce front. Hodnota této vlastnosti může být <code>true</code> nebo <code>false</code>. Další informace viz Podpora FIPS v MFT.</p>	ne

Tabulka 103. Rozšířené koordinační vlastnosti: Předplatné

Název vlastnosti	Popis	Výchozí hodnota
Téma coordinationSubscription	Pomocí této vlastnosti lze určit jiné téma než SYSTEM.FTE , který se má přihlásit k odběru, aby získal publikování o stavu sítě IBM MQ . Všechny nástroje se stále publikují do SYSTEM.FTE , ale můžete změnit topologii produktu IBM MQ , abyste distribuovali tyto publikace do různých témat na základě jejich obsahu. Poté můžete pomocí této funkce vynutit, aby se nástroje přihlásili k odběru jednoho z těchto dalších témat.	SYSTEM.FTE

Související pojmy

Volby konfigurace MFT na platformě Multiplatforms

Související odkazy

[fteSetupKoordinace](#)

[Vlastnosti SSL/TLS pro MFT](#)

[“Soubor MFT agent.properties” na stránce 169](#)

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.

[“Soubor MFT command.properties” na stránce 195](#)

Soubor command . properties uvádí správce front příkazů, ke kterému se chcete připojit při zadávání příkazů, a informace, které produkt Managed File Transfer vyžaduje pro kontaktování tohoto správce front.

[“Soubor MFT logger.properties” na stránce 199](#)

Modul protokolování Managed File Transfer má sadu vlastností konfigurace. Tyto vlastnosti zadejte v souboru logger . properties , který se nachází v adresáři MQ_DATA_PATH/mqft/config/coordination_qmgr_name/loggers/logger_name .

Soubor MFT command.properties

Soubor command . properties uvádí správce front příkazů, ke kterému se chcete připojit při zadávání příkazů, a informace, které produkt Managed File Transfer vyžaduje pro kontaktování tohoto správce front.

Soubor command . properties je vytvořen instalačním programem nebo příkazem **fteSetupCommands** . Pomocí příkazu **fteSetupCommands** s příznakem **-f** můžete změnit základní vlastnosti správce front příkazů v tomto souboru. Chcete-li změnit nebo přidat rozšířené vlastnosti správce front příkazů, musíte upravit soubor v textovém editoru.

Některé příkazy Managed File Transfer se připojují ke správci front agenta nebo koordinačnímu správci front místo ke správci front příkazů. Informace o tom, které příkazy se připojují ke kterému správci front, naleznete v tématu [Které MFT příkazy se připojují ke kterému správci front.](#)

Soubor command . properties je umístěn v adresáři MQ_DATA_PATH/mqft/config/coordination_qmgr_name .

Soubor MFT command . properties obsahuje následující hodnoty:

Tabulka 104. Základní vlastnosti správce front příkazů

Název vlastnosti	Popis	Výchozí hodnota
connectionCredentialsKeyFile	Název souboru obsahujícího klíč pověření použitý při šifrování pověření.	Vlastnost řetězce bez výchozí hodnoty.
connectionQMGr	Název správce front použitého pro připojení k síti IBM MQ .	Bez výchozí hodnoty
connectionQMGrHostitel	Název hostitele nebo adresa IP správce front připojení.	Bez výchozí hodnoty
Port connectionQMGr	Číslo portu použité pro připojení ke správci front připojení v režimu klienta.	1414
Kanál connectionQMGr	Název kanálu SVRCONN použitý pro připojení ke správci front připojení.	SYSTEM.DEF.SVRCONN

Pokud nezádáte hodnotu pro vlastnost hostitele connectionQMGr, použije se standardně režim vazeb.

Pokud zadáte hodnotu pro vlastnost hostitele connectionQMGr, ale nezádáte hodnoty pro vlastnosti kanálu connectionQMGrPort a connectionQMGr, číslo portu 1414 a kanál SYSTEM.DEF.SVRCONN .


Zde je příklad obsahu souboru `command.properties` :

```
connectionQMGr=PLUTO
connectionQMGrHost=kuiper.example.com
connectionQMGrPort=1930
connectionQMGrChannel=SYSTEM.DEF.SVRCONN
```

V tomto příkladu je PLUTO název IBM MQ správce front, který je umístěn v systému `kuiper.example.com`. Správce front PLUTO je správce front, ke kterému se připojují příkazy Managed File Transfer .

Rozšířené vlastnosti příkazu

Produkt Managed File Transfer také poskytuje rozšířené vlastnosti příkazu. Chcete-li použít některou z následujících vlastností, ručně upravte soubor `command.properties` a přidejte požadované rozšířené vlastnosti. Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být

uvozeny zpětným lomítkem (\).  Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/). Další informace o řídicím znaku v souborech vlastností Java naleznete v dokumentaci Oracle [Javadoc pro třídu vlastností](#).

- [Vlastnosti agenta](#)
- [Vlastnosti kódové stránky](#)
- [Vlastnosti správce front pro více instancí](#)
- [Vlastnosti fronty](#)
- [Vlastnosti zabezpečení](#)
- [Vlastnosti SSL](#)

Tabulka 105. Rozšířené vlastnosti příkazu: Agent


Název vlastnosti	Popis	Výchozí hodnota
<code>failCleanAgentWithNoArguments</code>	Standardně je hodnota této vlastnosti <code>true</code> , což znamená, že příkaz <code>fteCleanAgent</code> se nezdaří spustit, pokud je uveden pouze parametr názvu agenta. Nastavení vlastnosti na hodnotu <code>false</code> znamená, že pokud je nastaven pouze parametr názvu agenta, je chování příkazu <code>fteCleanAgent</code> ekvivalentní zadání parametru <code>-all</code> .	ano

Tabulka 106. Rozšířené vlastnosti příkazu: Kódová stránka

Název vlastnosti	Popis	Výchozí hodnota
<code>connectionCcsid</code>	Kódová stránka, se kterou se příkazy připojují ke správci front příkazů. Pokud uvedete hodnotu pro <code>connectionCcsid</code> , musíte také uvést hodnotu pro název <code>connectionCcsid</code> .	1208
Název <code>connectionCcsid</code>	Java reprezentace <code>connectionCcsid</code> . Pokud uvedete hodnotu pro název <code>connectionCcsid</code> , musíte také uvést hodnotu pro <code>connectionCcsid</code> .	UTF8

Tabulka 107. Rozšířené vlastnosti připojení: Správce front s více instancemi

Název vlastnosti	Popis	Výchozí hodnota
<code>connectionQMGrPohotovost</code>	Název hostitele a číslo portu použité pro připojení klienta ve formátu IBM MQ CONNAME pro rezervní instanci správce front příkazů s více instancemi definovanou vlastností <code>connectionQMGr</code> . Například <code>host_name(port_number)</code>	Bez výchozí hodnoty

Tabulka 108. Rozšířené vlastnosti příkazu: Fronta		
Název vlastnosti	Popis	Výchozí hodnota
dynamicQueuePředpona	Pro příkazy, které vyžadují odezvu od agenta, tato vlastnost definuje předponu IBM MQ , která se má použít pro generování názvu dočasně fronty odpovědí. Formát vlastnosti předpony dynamicQueueodpovídá formátu pole DynamicQName struktury IBM MQ MQOD. Další informace naleznete v tématu Vytvoření dynamických front . Tuto vlastnost můžete také definovat v souboru <code>coordination.properties</code> , chcete-li použít specifickou předponu IBM MQ pro dočasně fronty generované produktem WMQFTE.	WMQFTE.*
modelQueueNázev	Pro příkazy, které vyžadují odezvu od agenta, tato vlastnost definuje frontu modelu IBM MQ , která se má použít pro generování dočasně fronty odpovědí. Tuto vlastnost můžete také definovat v souboru <code>coordination.properties</code> , chcete-li použít specifickou modelovou frontu IBM MQ pro dočasně fronty generované produktem WMQFTE. Další informace viz téma "Soubor MFT coordination.properties" na stránce 191.	SYSTEM.DEFAULT.MODEL.QUEUE
Vlastnosti připojení:		
Cesta javaLibrary	Při připojování ke správci front v režimu vazeb Managed File Transfer musí mít přístup ke knihovnám vazeb produktu IBM MQ Java . Standardně produkt Managed File Transfer vyhledává knihovny vazeb ve výchozím umístění definovaném pomocí IBM MQ . Pokud se knihovny vazeb nacházejí v jiném umístění, použijte tuto vlastnost k určení umístění knihoven vazeb.	/opt/mqm/java/lib
 legacyXMLMessageFormát MQMDFormat	Zprávy XML příkazu Managed File Transfer jsou nyní odesílány do fronty s prázdným polem formátu MQMD. Předchozí verze produktu nastavily pole formátu MQMD na hodnotu MQSTR (textový řetězec zprávy). Nastavení této vlastnosti na hodnotu true povolí odesílání zpráv XML příkazu Managed File Transfer do fronty s polem formátu MQMD MQSTR. Je-li pole formátu MQMD nastaveno na hodnotu MQSTR, může dojít k poškození zpráv XML příkazu Managed File Transfer , pokud jsou v síti produktu MQ kanály s povoleným převodem dat.	ne

Tabulka 109. Rozšířené vlastnosti příkazu: Zabezpečení		
Název vlastnosti	Popis	Výchozí hodnota
userIdForClientConnect	ID uživatele, které je protékáno přes připojení klienta k produktu IBM MQ . Je-li zadáno <code>java</code> , bude jméno uživatele hlášené prostředím JVM zadáno jako součást požadavku na připojení IBM MQ . Hodnota této vlastnosti může být žádná nebo <code>java</code> .	Není
connectionQMGrAuthenticationCredentialsSoubor	Cesta k souboru, který obsahuje pověření připojení produktu MQ pro připojení ke správci front příkazů.	Viz MFT a IBM MQ ověření připojení a jeho podřízená témata.

Tabulka 110. Rozšířené vlastnosti příkazu: SSL/TLS		
Název vlastnosti	Popis	Výchozí hodnota
connectionSslCipherSpec	Určuje použitý protokol, hašovací algoritmus a šifrovací algoritmus a počet bitů použitých v šifrovacím klíči při výměně dat mezi příkazy a správcem front příkazů. Hodnota <code>connectionSslCipherSpec</code> je název <code>CipherSpec</code> . Tento název <code>CipherSpec</code> je stejný jako název <code>CipherSpec</code> použitý v kanálu správce front příkazů. Seznam platných názvů <code>CipherSpec</code> je obsažen v specifikacích SSL/TLS CipherSpecs a CipherSuites ve třídách IBM MQ pro produkt Java a SSL/TLS CipherSpecs a CipherSuites ve třídách IBM MQ pro JMS . <code>connectionSslCipherSpec</code> je podobná položce <code>connectionSslCipherSuite</code> . Pokud jsou zadány oba parametry <code>connectionSslCipherSuite</code> a <code>connectionSslCipherSpec</code> , použije se hodnota <code>connectionSslCipherSpec</code> .	Není
connectionSslCipherSuite	Určuje aspekty zabezpečení SSL týkající se způsobu výměny dat mezi příkazy a správcem front příkazů. Hodnota <code>connectionSslCipherSuite</code> je název <code>CipherSuite</code> . Název <code>CipherSuite</code> se mapuje na název <code>CipherSpec</code> použitý v kanálu správce front agenta. Další informace viz CipherSuite a CipherSpec mapování názvů. <code>connectionSslCipherSuite</code> je podobná položce <code>connectionSslCipherSpec</code> . Pokud jsou zadány oba parametry <code>connectionSslCipherSuite</code> a <code>connectionSslCipherSpec</code> , použije se hodnota <code>connectionSslCipherSpec</code> .	Není

Tabulka 110. Rozšířené vlastnosti příkazu: SSL/TLS (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
connectionSslPeerName	Určuje kostru rozlišujícího názvu, která se musí shodovat s názvem poskytnutým správcem front příkazů. Rozlišující název se používá ke kontrole identifikačního certifikátu, který je prezentován správcem front příkazů při připojení.	Není
connectionSslTrustStore	Určuje umístění certifikátů, kterým příkazy důvěřují. Hodnota connectionSslTrustStore je cesta k souboru. Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\). Windows Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/). Hodnota této vlastnosti může obsahovat proměnné prostředí.	Není
connectionSslTrustStore	Typ úložiště údajů o důvěryhodnosti SSL, které chcete použít. Úložiště klíčů JKS a PKCS#12 jsou podporována. Hodnota této vlastnosti může být buď jks , nebo pkcs12.	JKS
connectionSslTrustStoreCredentialsFile	Cesta k souboru, který obsahuje pověření connectionSslTrustStore . Hodnota této vlastnosti může obsahovat proměnné prostředí.	Výchozí hodnota této vlastnosti je %USERPROFILE%/MQMFTcredentials.xml na systému Windows a \$HOME/MQMFTcredentials.xml na jiných platformách.
connectionSslKeyStore	Určuje umístění soukromého klíče příkazů. Hodnota connectionSslKeyStore je cesta k souboru. Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\). Windows Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/). Tato vlastnost je vyžadována pouze v případě, že správce front příkazů vyžaduje ověřování klienta. Hodnota této vlastnosti může obsahovat proměnné prostředí.	Není
connectionSslKeyStore	Typ úložiště klíčů SSL, které chcete použít. Úložiště klíčů JKS a PKCS#12 jsou podporována. Hodnota této vlastnosti může být buď jks , nebo pkcs12. Hodnota této vlastnosti může obsahovat proměnné prostředí.	JKS
connectionSslKeyStoreCredentialsFile	Cesta k souboru, který obsahuje pověření connectionSslKeyStore . Hodnota této vlastnosti může obsahovat proměnné prostředí.	Výchozí hodnota této vlastnosti je %USERPROFILE%/MQMFTcredentials.xml na systému Windows a \$HOME/MQMFTcredentials.xml na jiných platformách.
connectionSslFipsRequired	Určuje, že chcete povolit podporu FIPS na úrovni správce front příkazů. Hodnota této vlastnosti může být true nebo false. Další informace viz Podpora FIPS v MFT .	ne

Související pojmy

[Volby konfigurace MFT na platformě Multiplatforms](#)

Související odkazy

“Java systémové vlastnosti pro MFT” na stránce 212

Řada vlastností příkazu Managed File Transfer a agenta musí být definována jako systémové vlastnosti Java , protože definují konfiguraci pro funkci typu early (dřívější), která nemůže používat mechanismus vlastností příkazu nebo agenta.

Vlastnosti SSL/TLS pro MFT

“Soubor MFT agent.properties” na stránce 169

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.

“Soubor MFT coordination.properties” na stránce 191

Soubor coordination.properties uvádí podrobnosti připojení ke koordinačnímu správci front. Vzhledem k tomu, že několik instalací produktu Managed File Transfer může sdílet stejného koordinačního správce front, můžete použít symbolický odkaz na společný soubor coordination.properties na sdílené jednotce.

[“Soubor MFT logger.properties” na stránce 199](#)

Modul protokolování Managed File Transfer má sadu vlastností konfigurace. Tyto vlastnosti zadejte v souboru `logger.properties`, který se nachází v adresáři `MQ_DATA_PATH/mqft/config/coordination_qmgr_name/loggers/logger_name`.

[Příkazy fteSetup](#): Vytvořte soubor `MFT command.properties`.


[fteCleanAgent](#): vyčištění agenta MFT

Soubor MFT logger.properties

Modul protokolování Managed File Transfer má sadu vlastností konfigurace. Tyto vlastnosti zadejte v souboru `logger.properties`, který se nachází v adresáři `MQ_DATA_PATH/mqft/config/coordination_qmgr_name/loggers/logger_name`.

Můžete použít proměnné prostředí v některých vlastnostech Managed File Transfer, které představují umístění souborů nebo adresářů. To umožňuje, aby se umístění souborů nebo adresářů, které se používají při spouštění částí produktu, lišila v závislosti na změnách prostředí, například na tom, který uživatel spouští proces. Další informace viz téma [“Použití proměnných prostředí ve vlastnostech MFT” na stránce 163](#).

Poznámka: Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být




uvozeny zpětným lomítkem (\).  Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/). Další informace o řídicím znaku v souborech vlastností Java v databázi Oracle viz [Javadoc pro třídu vlastností](#).

Soubor `MFT logger.properties` obsahuje následující hodnoty:

- [“Vlastnosti připojení režimu vazeb” na stránce 199](#)
- [“Vlastnosti připojení SSL/TLS v režimu klienta” na stránce 207](#)

Vlastnosti připojení režimu vazeb


Název vlastnosti	Popis	Výchozí hodnota
<code>wmqfte.logger.type</code>	Používaný typ modulu protokolování: soubor nebo databáze. Nastavte tuto hodnotu na <code>FILE</code> nebo <code>DATABASE</code> .	Bez výchozí hodnoty
<code>wmqfte.max.transaction.messages</code>	Maximální počet zpráv, které jsou zpracovány v transakci před potvrzením transakce. V kruhovém režimu transakčního protokolování má správce front k dispozici pevné množství prostoru pro průřezová data. Ujistěte se, že jste nastavili tuto vlastnost s dostatečně nízkou hodnotou, aby nedošlo k nedostatku dostupného prostoru.	50
<code>wmqfte.max.transaction.time</code>	Maximální doba v milisekundách, která uplyne mezi potvrzeními transakce.	5000
<code>wmqfte.max.consecutive.reject</code>	Maximální počet zpráv, které mohou být postupně odmítnuty (tj. bez zjištění platné zprávy). Pokud je tento počet překročen, zapisovač protokolu dojde k závěru, že problém není se zprávami samotnými, ale s konfigurací. Pokud například učiníte sloupec <code>název_agenta</code> v databázi užším než všechny názvy agentů, všechny zprávy odkazující na agenty budou odmítnuty.	50
<code>wmqfte.reject.queue.name</code>	Název fronty, do které modul protokolování vkládá zprávy, které modul protokolování nemůže zpracovat. Máte-li modul pro protokolování databáze, naleznete podrobné informace o tom, které zprávy mohou být vloženy do této fronty, v tématu MFT Zpracování a odmítnutí chyb modulu pro protokolování .	<code>SYSTEM.FTE.LOG.RJCT.název_protokolu</code>

Tabulka 111. Vlastnosti připojení režimu vazeb pro soubor <i>logger.properties</i> (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
wmqfte.command.queue.name	Název fronty, ze které modul protokolování čte zprávy příkazů, které řídí jeho chování.	SYSTEM.FTE.LOG.CMD.název_logger_name
wmqfte.queue.manager	Správce front, ke kterému se modul protokolování připojuje. Tento parametr je povinný a je vše, co je zapotřebí pro připojení v režimu vazeb ke správci front. (Vlastnosti pro připojení ke vzdálenému správci front viz Tabulka 112 na stránce 207.)	Bez výchozí hodnoty
wmqfte.message.source.type	Jedna z následujících hodnot: automatické předplatné Výchozí hodnota. Modul protokolování vytváří a používá vlastní trvalý spravovaný odběr ve správci front, který je definován v SYSTEM.FTE/Log/#. Jedná se o vhodnou hodnotu pro většinu scénářů. administrativní odběr Pokud automatický odběr není vhodný, můžete definovat jiný odběr (například pomocí IBM MQ Explorer, MQSC nebo PCF) a instruovat modul protokolování, aby tento odběr používal. Tuto hodnotu použijte například k rozdělení protokolovacího prostoru tak, aby jeden modul protokolování obsluhuje agenty z A-H, jiný modul protokolování obsluhuje I-P a třetí modul protokolování z Q-Z. fronta Pokud topologie IBM MQ znamená, že vytvoření odběru pro modul protokolování není vhodné, můžete místo toho použít frontu. Nakonfigurujte produkt IBM MQ tak, aby fronta přijímala zprávy, které jsou obvykle přijímány prostřednictvím odběru systému SYSTEM.FTE/Log/# v koordinačním správci front.	automatický odběr
wmqfte.message.source.name	Pokud je typ zdroje zpráv administrativní odběr nebo fronta, jedná se o název odběru nebo fronty, která má být použita. Tato vlastnost je ignorována, pokud je typ zdroje automatický odběr.	Bez výchozí hodnoty
wmqfte.database.credentials.file	Soubor, který obsahuje jméno uživatele a heslo pro připojení k databázi. Hodnota této vlastnosti může obsahovat proměnné prostředí. Další informace viz Formát souboru pověření MFT .	<p> Informace o vytvoření souboru ověřovacích pověření naleznete v tématu Konfigurace souboru MQMFTCredentials.xml na webu z/OS.</p> <p> Informace o umístění a oprávněních tohoto souboru naleznete v tématu Konfigurace souboru MQMFTCredentials.xml.</p> <p> Viz také MFT a IBM MQ ověření připojení.</p>

Tabulka 111. Vlastnosti připojení režimu vazeb pro soubor `logger.properties` (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
<p><code>wmqfte.database.driver</code></p>	<p>Umístění tříd ovladače JDBC pro databázi. Toto je obvykle cesta a název souboru JAR.</p> <p>AIX Například ovladač typu 2 pro systém Db2 na systému AIX vyžaduje soubor <code>/opt/IBM/db2/V9.5/java/db2jcc.jar</code>.</p> <p>Windows V systémech Windows zadejte oddělovač cesty jako dopředné lomítko (<code>/</code>), například <code>C:/Program Files/IBM/SQLLIB/java/db2jcc.jar</code>.</p> <p>z/OS V systému z/OS zadejte úplnou cestu k souboru <code>db2jcc.jar</code>. Například <code>wmqfte.database.driver=/db2/db2v10/jdbc/classes/db2jcc.jar</code>.</p> <p>z/OS Na systémech z/OS musíte odkazovat na všechny následující soubory JAR:</p> <ul style="list-style-type: none"> • <code>db2jcc.jar</code> • <code>db2jcc_license_cisuz.jar</code> • <code>db2jcc_javax.jar</code> <p>Pokud váš ovladač databáze sestává z více souborů JAR (například Db2 V9.1 vyžaduje soubor JAR ovladače a soubor JAR licence), zahrňte všechny tyto soubory JAR do této vlastnosti. Oddělte více názvů souborů pomocí oddělovače cesty ke třídě pro vaši platformu, tj. středníkem (<code>:</code>) na systémech Windows a dvojtečkou (<code>:</code>) na jiných platformách.</p>	<p>Bez výchozí hodnoty</p>
<p><code>wmqfte.database.exclude.metadata</code></p>	<p>Řídí, zda jsou položky uloženy v tabulce metadat, která obsahuje informace, které lze nalézt v jiných tabulkách v rámci schématu modulu pro protokolování databáze. Nastavte tuto hodnotu na <code>true</code> nebo <code>false</code>. Tyto položky metadat se již standardně neukládají, protože se jedná o duplikaci existujících dat a ztrátu kapacity databázového úložiště. Položky vlastností a tabulky, kde se zobrazují stejná data, jsou následující:</p> <ul style="list-style-type: none"> • <code>com.ibm.wmqfte.SourceAgent TRANSFER_EVENT</code> nebo <code>CALL_REQUEST</code> • <code>com.ibm.wmqfte.DestinationAgent TRANSFER_EVENT</code> • <code>com.ibm.wmqfte.MqmdUser TRANSFER_EVENT</code> nebo <code>CALL_REQUEST</code> • <code>com.ibm.wmqfte.OriginatingUser TRANSFER_EVENT</code> nebo <code>CALL_REQUEST</code> • <code>com.ibm.wmqfte.OriginatingHost TRANSFER_EVENT</code> nebo <code>CALL_REQUEST</code> • <code>com.ibm.wmqfte.TransferId TRANSFER</code> nebo <code>CALL_REQUEST</code> • <code>com.ibm.wmqfte.JobName TRANSFER</code> nebo <code>CALL_REQUEST</code> <p>Nastavení této vlastnosti na hodnotu <code>false</code> způsobí, že tyto položky metadat budou uloženy v tabulce metadat.</p>	<p>ano</p>

Tabulka 111. Vlastnosti připojení režimu vazeb pro soubor `logger.properties` (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
<code>wmqfte.database.host</code>	<p>Db2 pouze:</p> <p>Název hostitele databázového serveru, ke kterému se chcete připojit pomocí ovladače JDBC typu 4. Je-li zadána hodnota této vlastnosti, musí být zadána také hodnota <code>wmqfte.database.port</code>. Pokud nejsou definovány obě vlastnosti, modul pro protokolování databáze se připojí pomocí výchozího ovladače JDBC typu 2.</p> <p>Pokud je zadána hodnota této vlastnosti, musí existovat soubor pověření pro tento modul protokolování (cesta k souboru definovaná vlastností <code>wmqfte.database.credentials.file</code>) a musí být přístupný pro definování jména uživatele a hesla pro připojení k databázi, a to i v případě, že se databáze nachází na lokálním systému.</p>	Bez výchozí hodnoty
<code>wmqfte.database.name</code>	Název instance databáze (nebo subsystému při použití Db2 pro z/OS), která obsahuje tabulky protokolu Managed File Transfer.	Bez výchozí hodnoty
<code>wmqfte.database.type</code>	Používaný systém správy databází: Db2 nebo Oracle. Nastavte tuto hodnotu na <code>db2</code> nebo <code>oracle</code> .	<code>db2</code>
<code>wmqfte.database.port</code>	<p>Db2 pouze:</p> <p>Číslo portu databázového serveru, ke kterému se chcete připojit pomocí ovladače JDBC typu 4. Je-li zadána hodnota této vlastnosti, musí být zadána také hodnota <code>wmqfte.database.host</code>. Pokud nejsou definovány obě vlastnosti, modul pro protokolování databáze se připojí pomocí výchozího ovladače JDBC typu 2.</p> <p>Pokud je zadána hodnota této vlastnosti, musí existovat soubor pověření pro tento modul protokolování (cesta k souboru definovaná vlastností <code>wmqfte.database.credentials.file</code>) a musí být přístupný pro definování jména uživatele a hesla pro připojení k databázi, a to i v případě, že se databáze nachází na lokálním systému.</p>	Bez výchozí hodnoty
<code>wmqfte.database.schema</code>	<p>Db2 pouze:</p> <p>Schéma databáze, které obsahuje tabulky protokolování Managed File Transfer. Ve většině případů je výchozí hodnota vhodná, ale možná budete muset zadat alternativní hodnotu v závislosti na vašich vlastních aspektech databáze specifických pro organizační jednotku.</p>	FTELOG
<code>wmqfte.database.native.library.path</code>	<p>Cesta, která obsahuje nativní knihovny potřebné pro vybraný ovladač databáze (je-li k dispozici).</p> <p> Například ovladač typu 2 pro systém Db2 na systému AIX vyžaduje knihovny z produktu <code>/opt/IBM/db2/V9.5/11b32/</code>. Jako alternativu k této vlastnosti můžete nastavit systémovou vlastnost <code>java.library.path</code> pomocí jiných metod.</p>	Bez výchozí hodnoty
<code>wmqfte.file.logger.fileDirectory</code>	Adresář, kde jsou umístěny soubory protokolu modulu protokolování souborů.	<code>mqft/logs/coordination_dir/loggers/logger_name/logs</code>

Tabulka 111. Vlastnosti připojení režimu vazeb pro soubor *logger.properties* (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
wmqfte.file.logger.fileSize	<p>Maximální velikost, na kterou může soubor protokolu růst. Hodnota velikosti je kladné celé číslo, větší než nula, následované jednou z následujících jednotek: KB, MB, GB, m (minuty), h (hodiny), d (dny), w (týdny). Například <code>wmqfte.file.logger.fileSize=5MB</code> uvádí maximální velikost souboru 5MBa <code>wmqfte.file.logger.fileSize=2d</code> uvádí maximální velikost souboru 2 dny dat.</p>	10MB
wmqfte.file.logger.fileCount	<p>Maximální počet souborů protokolu, které se mají vytvořit. Když množství dat překročí maximální množství, které lze uložit v tomto počtu souborů, nejstarší soubor se odstraní, takže počet souborů nikdy nepřekročí zadanou hodnotu.</p>	3




Tabulka 111. Vlastnosti připojení režimu vazeb pro soubor *logger.properties* (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
wmqfte.file.logger.mode	<p>Používaný režim zapisovače protokolu: kruhový nebo lineární. Nastavte tuto hodnotu na CIRCULARnebo LINEAR.</p> <p>CIRCULAR-Modul protokolování souborů zapisuje informace do souboru, dokud tento soubor nedosáhne maximální velikosti definované pomocí vlastnosti wmqfte.file.logger.fileSize . Po dosažení maximální velikosti modul protokolování souborů spustí nový soubor. Maximální počet souborů zapsaných v tomto režimu je řízen hodnotou, která je definována pomocí vlastnosti wmqfte.file.logger.fileCount . Po dosažení tohoto maximálního počtu souborů modul protokolování odstraní první soubor a znovu jej vytvoří pro použití jako aktuálně aktivní soubor. Pokud je hodnota definovaná ve vlastnosti wmqfte.file.logger.fileSize jednotkou bajtů pevné velikosti (například KB, MB nebo GB), pak se horní limit prostoru na disku, který se používá v tomto režimu, rovná fileSize vynásobený fileCount. Pokud je hodnota definovaná ve vlastnosti wmqfte.file.logger.fileSize jednotkou času (například m, h, dnebo w), pak maximální velikost závisí na propustnosti zpráv protokolu v systému v těchto časových obdobích. Konvence pojmenování souboru protokolu, která se používá při spuštění v tomto režimu, je: <i>logger_namenumbertimestamp</i> .log , kde:</p> <ul style="list-style-type: none"> • <i>logger_name</i> je název, který je dán modulu protokolování v příkazu fteCreateLogger . • <i>number</i> je číslo souboru v sadě. • <i>timestamp</i> je časové razítko, kdy byl soubor vytvořen. <p>Například: LOGGER1-20111216123430147.log</p> <p>LINEAR-Modul protokolování souborů zapisuje informace do souboru, dokud tento soubor nedosáhne maximální velikosti definované pomocí vlastnosti wmqfte.file.logger.fileSize . Po dosažení maximální velikosti modul protokolování spustí nový soubor. Dříve zapsané soubory nejsou odstraněny, což jim umožňuje uchovávat je jako historický záznam zpráv protokolu. Soubory se při spuštění v lineárním režimu neodstraní, takže se vlastnost wmqfte.file.logger.fileCount ignoruje, protože neexistuje žádný horní limit počtu souborů, které lze vytvořit. Vzhledem k tomu, že při spuštění v tomto režimu neexistuje žádný horní limit, je nutné sledovat množství místa na disku, které soubory protokolu využívají, aby se zabránilo nedostatku místa na disku. Konvence pojmenování souboru protokolu, která se používá při spuštění v tomto režimu, je: <i>logger_name-timestamp</i> .log , kde:</p> <ul style="list-style-type: none"> • <i>logger_name</i> je název, který je dán modulu protokolování v příkazu fteCreateLogger . • <i>timestamp</i> je časové razítko, kdy byl soubor vytvořen. <p>Například: LOGGER-20111216123430147.log</p>	Bez výchozí hodnoty

Tabulka 111. Vlastnosti připojení režimu vazeb pro soubor `logger.properties` (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
<code>wmqfte.max.retry.interval</code>	<p>Maximální doba, v sekundách, mezi opakovanými pokusy, když modul protokolování zjistí trvalou chybu.</p> <p>Některé chybové stavy (například ztráta databázového připojení) brání v pokračování modulu protokolování. Dojde-li k tomuto typu podmínky, modul protokolování odvolá aktuální transakci, počká po určitou dobu a poté zopakuje pokus. Doba, po kterou modul protokolování čeká, je zpočátku velmi krátká, takže přechodné chyby lze rychle překonat. Avšak pokaždé, když se modul protokolování pokusí o opakování, doba, po kterou čeká, se zvýší. To zabraňuje tomu, aby se prováděla zbytečná práce, když je chybový stav delší, například když je databáze vypnutá kvůli údržbě.</p> <p>Pomocí této vlastnosti lze nastavit omezení délky čekání tak, aby se opakovaný pokus vyskytoval v přiměřeném čase vyřešení chybového stavu.</p>	600
<code>immediateShutdownvypršení časového limitu</code>	<p>Doba, v sekundách, po kterou modul protokolování čeká na dokončení všech neprovedených operací, a která se postupně vypne. Standardně modul protokolování čeká na dokončení operací po dobu 10 sekund. Pokud nejsou operace dokončeny před vypršením časového limitu, zapisovač protokolu запиše následující zprávu události do souboru <code>output0.log</code> a ukončí se.</p> <p><code>BFGDB0082I: The logger is ending immediately.</code></p> <p>Zadáte-li hodnotu nula, modul protokolování bude čekat na dokončení aktuálních operací.</p> <p>Výchozí hodnota se použije, pokud je hodnota <code>immediateShutdownTimeout</code> nastavena na menší než nula.</p> <p>Tato vlastnost se vztahuje jak na modul protokolování samostatné databáze, tak na modul protokolování typu souboru.</p>	10
<code>loggerCredentialsKeyFile</code>	Název souboru obsahujícího klíč pověření použitý při šifrování pověření.	Vlastnost řetězce bez výchozí hodnoty.
<code>loggerQMGrRetryInterval</code>	Interval v sekundách mezi kontrolami dostupnosti správce front řadičem procesů modulu protokolování.	30
Počet <code>maxRestart</code>	Maximální počet restartů, ke kterým může dojít v časovém intervalu určeném hodnotou vlastnosti <code>maxRestartInterval</code> . Když je tato hodnota překročena, řadič procesů modulu protokolování zastaví restartování modulu protokolování a místo toho provede akci, která je založena na hodnotě vlastnosti <code>maxRestartDelay</code> .	4
<code>maxRestartInterval</code>	Interval v sekundách, po který řadič procesů modulu protokolování měří, zda se má modul protokolování znovu spustit. Pokud počet restartů v tomto intervalu překročí hodnotu vlastnosti <code>maxRestartCount</code> , řadič procesů modulu protokolování zastaví restartování modulu protokolování. Místo toho řadič procesů modulu protokolování provede akci, která je založena na hodnotě vlastnosti prodlevy <code>maxRestart</code> .	120

Tabulka 111. Vlastnosti připojení režimu vazeb pro soubor `logger.properties` (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
<code>Prodleva maxRestart</code>	Určuje chování řadiče procesů modulu protokolování, když rychlost restartů modulu protokolování překročí hodnotu vlastností intervalu <code>maxRestartCount</code> a <code>maxRestart</code> . Zadáte-li hodnotu menší nebo rovnou nule, řadič procesů modulu protokolování se zastaví. Zadáte-li hodnotu větší než nula, jedná se o počet sekund, po který se má čekat, než se informace o historii restartování, které obsahuje řadič procesů modulu protokolování, vynulují a modul protokolování se restartuje.	-1
<code>wmqfte.oracle.port</code>	Port, který modul protokolování používá pro připojení k instanci Oracle. Tento port je také známý jako modul listener TNS.	1521
<code>wmqfte.oracle.host</code>	Hostitel, kterého modul protokolování používá pro připojení k instanci Oracle.	lokální hostitel
<code>armELEMTYPE</code>	Volitelná vlastnost. Je-li modul protokolování konfigurován pro restartování správcem ARM (Automatic Restart Manager), nastavte tuto vlastnost na hodnotu parametru ARM ELEMTYPE určenou v přidružené zásadě ARM. Pro modul protokolování nastavte ELEMTYPE na SYSBFGLG.	Nenastaveno
<code>armELEMENT</code>	Volitelná vlastnost. Je-li modul protokolování konfigurován pro restartování správcem ARM (Automatic Restart Manager), nastavte tuto vlastnost na hodnotu parametru ARM ELEMENT určenou v přidružené zásadě ARM. Hodnotu ELEMENT můžete nastavit tak, aby odpovídala názvu modulu protokolování.	Nenastaveno
<code>loggerQMGrAuthenticationCredentials</code>	Cesta k souboru, který obsahuje pověření připojení produktu MQ pro připojení ke koordinačnímu správci front modulu protokolování.	<p> z/OS Informace o vytvoření souboru ověřovacích pověření naleznete v tématu Konfigurace souboru MQMFTCredentials.xml na webu z/OS.</p> <p> ALW Informace o umístění a oprávněních pro tento soubor naleznete v tématu Konfigurace souboru MQMFTCredentials.xml.</p> <p> ALW Viz také MFT a IBM MQ ověření připojení.</p>
<code>trasování</code>	Volitelná vlastnost. Specifikace trasování, když má být modul protokolování spuštěn s povoleným trasováním při spuštění modulu protokolování. Specifikace trasování je seznam tříd oddělených čárkami, znak rovná se a úroveň trasování. Například <code>com.ibm.wmqfte.databaselogger.com.ibm.wmqfte.databaselogger.operation=all</code> V seznamu odděleném dvojtečkami můžete zadat více specifikací trasování. Například: <code>com.ibm.wmqfte.databaselogger=moderate:com.ibm.wmqfte.databaselogger.operation=all</code>	Není
<code>traceFiles</code>	Volitelná vlastnost. Celkový počet trasovacích souborů, které se mají uchovat. Tato hodnota platí pro řadič procesů modulu protokolování i pro samotný modul protokolování.	5

Tabulka 111. Vlastnosti připojení režimu vazeb pro soubor <i>logger.properties</i> (pokračování)		
Název vlastnosti	Popis	Výchozí hodnota
traceSize	Volitelná vlastnost. Maximální velikost každého trasovacího souboru v MB před tím, než se trasování přetočí na další soubor. Tato hodnota platí pro řadič procesů modulu protokolování a pro samotný modul protokolování.	20
wmqfte.file.logger.filePermissions	<p>Volitelná vlastnost. Slouží k určení, jaký druh oprávnění je vyžadován pro soubor protokolu modulu protokolování.</p> <p>Vlastnost platí pro lineární i kruhové protokoly a může nabývat hodnot <i>UserReadWriteOnly</i> nebo <i>UserReadWriteAllRead</i>.</p> <p>Hodnota <i>UserReadWriteOnly</i> má existující ekvivalentní oprávnění 600 a hodnota <i>UserReadWriteAllRead</i> má ekvivalentní oprávnění 644.</p> <p>Jakákoli změna oprávnění je použitelná pro nově vytvořené soubory modulu protokolování.</p> <p>Pokud zadáte neplatnou hodnotu vlastnosti, modul protokolování vezme výchozí hodnotu a vydá zprávu BFGDB0083W do výstupního protokolu.</p>	UserReadWriteOnly

Vlastnosti připojení SSL/TLS v režimu klienta

Vlastnosti nezbytné pro podporu připojení v režimu klienta ke správci front modulu protokolování pomocí SSL/TLS.

Tabulka 112. Vlastnosti připojení SSL/TLS v režimu klienta pro soubor <i>logger.properties</i>		
Název vlastnosti	Popis	Výchozí hodnota
wmqfte.queue.manager.host	Název hostitele nebo adresa IP správce front modulu protokolování.	Bez výchozí hodnoty
wmqfte.queue.manager.port	Port, na kterém naslouchá správce front modulu protokolování.	1414
wmqfte.queue.manager.channel	Název kanálu připojení serveru ve správci front modulu protokolování.	SYSTEM.DEF.SVRCONN
wmqfte.Ssl.CipherSuite	<p>Určuje aspekty protokolu TLS týkající se způsobu výměny dat mezi modulem protokolování a správcem front modulu protokolování.</p> <p>Hodnota wmqfte.Ssl.CipherSuite je název CipherSuite . Název CipherSuite se mapuje na název CipherSpec použitý v kanálu správce front modulu protokolování.</p> <p>Další informace viz CipherSuite a CipherSpec mapování názvů.</p>	Bez výchozí hodnoty
wmqfte.Ssl.PeerName	Určuje kostru rozlišujícího názvu, která se musí shodovat s názvem poskytnutým správcem front modulu protokolování. Rozlišující název se používá ke kontrole identifikačního certifikátu předloženého správcem front při připojení.	Bez výchozí hodnoty

Tabulka 112. Vlastnosti připojení SSL/TLS v režimu klienta pro soubor `logger.properties` (pokračování)

Název vlastnosti	Popis	Výchozí hodnota
<code>wmqfte.Ssl.TrustStore</code>	<p>Určuje umístění certifikátů, kterým modul protokolování důvěřuje. Hodnota wmqfte.Ssl.TrustStore je cesta k souboru.</p> <p>Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\).</p> <p>Windows Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/).</p> <p>Všimněte si, že hodnota této vlastnosti může obsahovat proměnné prostředí.</p>	Bez výchozí hodnoty
<code>wmqfte.Ssl.TrustStoreCredentialsFile</code>	<p>Cesta k souboru, který obsahuje pověření wmqfte.Ssl.TrustStore.</p> <p>Všimněte si, že hodnota této vlastnosti může obsahovat proměnné prostředí.</p>	Bez výchozí hodnoty
<code>wmqfte.Ssl.TrustStoreType</code>	<p>Typ úložiště klíčů SSL, které chcete použít. Úložiště klíčů JKS a PKCS#12 jsou podporována. Hodnota této vlastnosti může být buď <code>jks</code>, nebo <code>pkcs12</code>.</p>	JKS
<code>wmqfte.Ssl.KeyStore</code>	<p>Určuje umístění soukromého klíče modulu protokolování. Hodnota wmqfte.Ssl.KeyStore je cesta k souboru.</p> <p>Závorky, čárky (,) a zpětná lomítka (\) jsou speciální znaky v příkazech MFT a musí být uvozeny zpětným lomítkem (\).</p> <p>Windows Cesty k souborům v systému Windows lze zadat buď pomocí dvojitých zpětných lomítek (\\) jako oddělovače, nebo pomocí jednoduchých dopředných lomítek (/).</p> <p>Všimněte si, že hodnota této vlastnosti může obsahovat proměnné prostředí.</p>	Bez výchozí hodnoty
<code>wmqfte.Ssl.KeyStore.CredentialsFile</code>	<p>Cesta k souboru, který obsahuje pověření wmqfte.Ssl.KeyStore.</p> <p>Všimněte si, že hodnota této vlastnosti může obsahovat proměnné prostředí.</p>	Bez výchozí hodnoty
<code>wmqfte.Ssl.KeyStoreType</code>	<p>Typ úložiště klíčů SSL, které chcete použít. Úložiště klíčů JKS a PKCS#12 jsou podporována. Hodnota této vlastnosti může být buď <code>jks</code>, nebo <code>pkcs12</code>.</p>	JKS
<code>wmqfte.Ssl.FipsRequired</code>	<p>Určuje, že chcete povolit podporu FIPS na úrovni modulu protokolování. Hodnota této vlastnosti může být <code>true</code> nebo <code>false</code>. Další informace viz Podpora FIPS v MFT.</p>	ne

Související pojmy

Vlastnosti SSL/TLS pro MFT

Související odkazy

“Použití proměnných prostředí ve vlastnostech MFT” na stránce 163

Je možné, aby se proměnné prostředí používaly ve vlastnostech Managed File Transfer, které představují umístění souborů nebo adresářů. To umožňuje, aby se umístění souborů nebo adresářů používaných při spouštění částí produktu lišila v závislosti na aktuálním prostředí (například uživatel spouštějící příkaz).

[“Soubor MFT agent.properties” na stránce 169](#)

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.

[“Soubor MFT command.properties” na stránce 195](#)

Soubor `command.properties` uvádí správce front příkazů, ke kterému se chcete připojit při zadávání příkazů, a informace, které produkt Managed File Transfer vyžaduje pro kontaktování tohoto správce front.

[“Soubor MFT coordination.properties” na stránce 191](#)

Soubor `coordination.properties` uvádí podrobnosti připojení ke koordinačnímu správci front. Vzhledem k tomu, že několik instalací produktu Managed File Transfer může sdílet stejného koordinačního správce front, můžete použít symbolický odkaz na společný soubor `coordination.properties` na sdílené jednotce.

V 9.3.0 Výstup vytvořený funkcí LogTransfer

Události protokolu přenosu zachycují podrobnosti průběhu přenosu od okamžiku odeslání přenosu až do jeho dokončení. Informace o přenosu do resynchronizace jsou také zachyceny, aby vám pomohly pochopit průběh přenosu.

Formát události přenosu

Události přenosu jsou ve formátu JSON a jsou zapsány do souboru `transferlogN.json`, který je vytvořen v adresáři protokolu agenta, kde N je číslo s výchozím 0. Každá událost obsahuje následující společné atributy:

- Datum a čas (v UTC)
- Jedinečné ID

Do zapisovaných informací o události jsou zahrnuty další atributy v závislosti na typu události a úrovni protokolu přenosu. Zatímco úroveň protokolu přenosu *info* zapisuje minimální informace, úroveň *verbose* obsahuje podrobnější informace. Následující část [“Ukázkové události” na stránce 209](#) popisuje několik příkladů událostí přenosu zaprotokolovaných agentem.

Jedinečné ID

Součástí je jedinečné ID, které vám pomůže snadno identifikovat různé fáze průběhu přenosu, například BFGTL0001. Jedinečné ID je součástí atributu **eventDescription** a skládá se ze dvou částí:

BFGTL

Předpona použitá pro všechny identifikátory, kde BFG je standardní přípona použitá v produktu Managed File Transfer a TL označuje, že se jedná o protokol přenosu.

Číslo

Jedinečné číslo začínající na 1. Příklad:

```
{
  "eventDescription": "BFGTL0001: New transfer request submitted"
}
```

Ukázkové události

Následující tabulka popisuje některé události jako příklady informací zaprotokolovaných přídatnou funkcí. Druhý sloupec tabulky *Úroveň protokolování* označuje úroveň, na které je událost protokolována.

Důležité: Následující atributy jsou zahrnuty v informacích o události, pokud je úroveň **logTransfer** nastavena na *verbose* nebo *střední*:

- **sourceAgent**
- **destinationAgent**
- **threadId**

Událost	Úroveň protokolování	Popis
Seznam položek k převodu	Podrobně	<pre> { "dateTime": "<Data time in UTC>", "eventDescription": "BFGTL0002I: Generated detailed transfer item list.", "destinationAgent": "<Name of destination agent>", "sourceAgent": "<Name of source agent>", "threadId": "0000001d", "totalItemsInTransfer": <Number of items in the transfer>, "transferId": "<Transfer Identifier>", "transferItemsList": [{"source": "source item name", "destination": "destination item name"}] } Example: { "dateTime": "2022-01-14T12:56:54.219Z UTC", "eventDescription": "BFGTL0002I: Generated detailed transfer item list.", "destinationAgent": "QMBAGQ", "sourceAgent": "QMBAG1", "threadId": "0000001d", "totalItems": 1, "transferId": "414d5120514d412020202020202020202063bd17610a390040", "transferItems": [{ "destination": "/results/rts/target/destFile.txt", "source": "DESTINATIONQ@QMB" }] } </pre>

Událost	Úroveň protokolování	Popis
Seznam přenosů, které mají být obnoveny na začátku agenta	Podrobně	<pre>{ "dateTime": "<Date and time in UTC>", "eventDescription": "The list of transfers being recovered as part of agent recovery process.", "agentName": "<Agent name>", "transfers": [{ "transferId": "<transfer state>" }] "threadId": "<Thread Id>", }</pre> <p>Example:</p> <pre>{ "dateTime": "2022-01-14T14:42:24.902Z UTC", "eventDescription": "The list of transfers being recovered as part of agent recovery process.", "agentName": "CQMXX01AG1", "transfers": [{ "414D512043514D485830312020202020B0D4176101370040": "completeReceived" }, { "414D512043514D485830312020202020B0D4176101370050": "resynchronizing" }] "threadId": "0000001c", }</pre>

Související odkazy

[“Java systémové vlastnosti pro MFT” na stránce 212](#)

Řada vlastností příkazu Managed File Transfer a agenta musí být definována jako systémové vlastnosti Java , protože definují konfiguraci pro funkci typu early (dřívější), která nemůže používat mechanismus vlastností příkazu nebo agenta.

[fteCreateAgent](#)

[“Použití proměnných prostředí ve vlastnostech MFT” na stránce 163](#)

Je možné, aby se proměnné prostředí používaly ve vlastnostech Managed File Transfer , které představují umístění souborů nebo adresářů. To umožňuje, aby se umístění souborů nebo adresářů používaných při spouštění částí produktu lišila v závislosti na aktuálním prostředí (například uživatel spouštějící příkaz).




Java systémové vlastnosti pro MFT

Řada vlastností příkazu Managed File Transfer a agenta musí být definována jako systémové vlastnosti Java , protože definují konfiguraci pro funkci typu early (dřívější), která nemůže používat mechanismus vlastností příkazu nebo agenta.

Definujte systémové vlastnosti a další volby prostředí JVM pro spuštění příkazů Managed File Transfer definováním proměnné prostředí BFG_JVM_PROPERTIES. Chcete-li například nastavit vlastnost `com.ibm.wmqfte.maxConsoleLineLength` na platformě typu UNIX, definujte proměnnou následujícím způsobem:

```
export BFG_JVM_PROPERTIES="-Dcom.ibm.wmqfte.maxConsoleLineLength=132"
```

Pokud spouštíte agenta jako službu Windows , můžete upravit systémové vlastnosti Java agenta zadáním parametru `-sj` v příkazu **fteModifyAgent** .

Název vlastnosti	Popis	Hodnota
<code>com.ibm.wmqfte.maxConsoleLineLength</code>	Maximální délka řádku, který lze zapsat na konzolu. Řádky, které přesahují tuto délku, jsou zalomené. Tato hodnota je vyjádřena v bajtech (nikoli ve znacích).	 Výchozí délka pro systém IBM i je 132 bajtů.   Pro z/OS, AIX, Linux, and Windows je délka neomezená.

Tabulka 113. Java Systémové vlastnosti (pokračování)

Název vlastnosti	Popis	Hodnota
com.ibm.wmqfte.daemon.windows.windowsServiceLogFilesm	(Pouze Windows .) Určuje maximální počet souborů protokolu služby Windows , které mají být uchovány. Soubory protokolu služby systému Windows jsou vytvořeny v adresářích protokolů agenta a modulu protokolování databáze, pokud jsou tyto aplikace spuštěny jako služba systému Windows . Soubory protokolu služby Windows jsou pojmenovány s předponou <i>servicea</i> obsahují zprávy o spuštění a zastavení služby.	5

Související pojmy

[Volby konfigurace MFT na platformě Multiplatforms](#)

[Rady a tipy pro použití MFT](#)

SHA-2 CipherSpecs a CipherSuites pro MFT

Produkt Managed File Transfer podporuje specifikace SHA-2 CipherSpecs a CipherSuites.

Další informace o specifikacích CipherSpecs a CipherSuites , které jsou k dispozici pro připojení mezi agenty a správci front IBM MQ , naleznete v části [Specifikace TLS CipherSpecs a CipherSuites](#) v části [IBM MQ classes for Java](#) a v části [Specifikace SSL/TLS CipherSpecs a CipherSuites](#) ve třídách IBM MQ pro platformu JMS.

Další informace o konfiguraci specifikací CipherSpecs a CipherSuites pro použití s agenty mostu protokolů (PBA) a servery FTPS naleznete v tématu [Podpora serveru FTPS mostem protokolů](#) a [Formát souboru vlastností mostu protokolů](#).

Chcete-li vyhovět požadavkům SP 800-131A, musíte splnit následující požadavky:

- Musíte použít FTPS, který jste správně nakonfigurovali; SFTP není podporován.
- Vzdálený server musí odeslat pouze šifrovací sady SP 800-131A-compliant .

Související pojmy

[Vlastnosti SSL/TLS pro MFT](#)

Konfigurační soubory modulu protokolování souborů MFT

Kromě souboru `logger.properties` má samostatný modul protokolování souborů Managed File Transfer ve svém konfiguračním adresáři také konfigurační soubor XML. Tento konfigurační soubor se nazývá `FileLoggerFormat.xml` a definuje formát používaný modulem protokolování souborů pro zápis zpráv do souboru protokolu. Obsah tohoto souboru musí odpovídat schématu XML definovanému v souboru `FileLoggerFormat.xsd`.

Související pojmy

[Formát samostatného modulu protokolování souborů MFT](#)

Související odkazy

[“Soubor MFT logger.properties” na stránce 199](#)

Modul protokolování Managed File Transfer má sadu vlastností konfigurace. Tyto vlastnosti zadejte v souboru `logger.properties` , který se nachází v adresáři `MQ_DATA_PATH/mqft/config/coordination_qmgr_name/loggers/logger_name` .

[“Výchozí formát protokolu samostatného modulu protokolování souborů MFT” na stránce 214](#)

Výchozí definice formátu souboru protokolu pro samostatný modul protokolování souborů Managed File Transfer .

[“XSD formátu samostatného modulu protokolování souborů” na stránce 218](#)

Schéma pro samostatný formát souboru.

Výchozí formát protokolu samostatného modulu protokolování souborů MFT

Výchozí definice formátu souboru protokolu pro samostatný modul protokolování souborů Managed File Transfer .

```
<?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>
    <callCompleted>
      <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="false">/transaction/status/@resultCode</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>
          <insert type="user" width="0" ignoreNull="true">/transaction/transferSet/call/callResult/
@outcome</insert>
          <insert type="user" width="0" ignoreNull="true">/transaction/transferSet/call/callResult/
result/error</insert>
        </inserts>
        <separator>;</separator>
      </format>
    </callCompleted>
    <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>
    <monitorAction>
      <format>
        <inserts>
          <insert type="user" width="19" ignoreNull="false"/>/monitorLog/action/@time</insert>
          <insert type="user" width="48" ignoreNull="false"/>/monitorLog/@referenceId</insert>
          <insert type="system" width="6" ignoreNull="false">type</insert>
          <insert type="user" width="3" ignoreNull="false">/monitorLog/status/@resultCode</insert>
          <insert type="user" width="0" ignoreNull="false">/monitorLog/@monitorName</insert>
          <insert type="user" width="0" ignoreNull="false">/monitorLog/monitorAgent/@agent</insert>
          <insert type="user" width="0" ignoreNull="false">/monitorLog/monitorAgent/@QMgr</insert>
          <insert type="user" width="0" ignoreNull="false">/monitorLog/action</insert>
        </inserts>
        <separator>;</separator>
      </format>
    </monitorAction>
    <monitorCreate>
      <format>
        <inserts>
          <insert type="user" width="19" ignoreNull="false"/>/monitorLog/action/@time</insert>
          <insert type="user" width="48" ignoreNull="false"/>/monitorLog/@referenceId</insert>
          <insert type="system" width="6" ignoreNull="false">type</insert>
          <insert type="user" width="0" ignoreNull="false">/monitorLog/@monitorName</insert>
          <insert type="user" width="0" ignoreNull="false">/monitorLog/monitorAgent/@agent</insert>
          <insert type="user" width="0" ignoreNull="false">/monitorLog/monitorAgent/@QMgr</insert>
          <insert type="user" width="0" ignoreNull="false">/monitorLog/action</insert>
        </inserts>
        <separator>;</separator>
      </format>
    </monitorCreate>
    <monitorFired>
```

```

<format>
  <inserts>
    <insert type="user" width="19" ignoreNull="false">/monitorLog/action/@time</insert>
    <insert type="user" width="48" ignoreNull="false">/monitorLog/@referenceId</insert>
    <insert type="system" width="6" ignoreNull="false">type</insert>
    <insert type="user" width="3" ignoreNull="false">/monitorLog/status/@resultCode</insert>
    <insert type="user" width="0" ignoreNull="false">/monitorLog/@monitorName</insert>
    <insert type="user" width="0" ignoreNull="false">/monitorLog/monitorAgent/@agent</insert>
    <insert type="user" width="0" ignoreNull="false">/monitorLog/monitorAgent/@QMgr</insert>
    <insert type="user" width="0" ignoreNull="false">/monitorLog/action</insert>
    <insert type="user" width="48" ignoreNull="false">/monitorLog/references/taskRequest</insert>
  </inserts>
  <separator>;</separator>
</format>
</monitorFired>
<notAuthorized>
  <format>
    <inserts>
      <insert type="user" width="19" ignoreNull="false">/notAuthorized/action/@time</insert>
      <insert type="user" width="48" ignoreNull="false">/notAuthorized/@ID</insert>
      <insert type="system" width="6" ignoreNull="false">type</insert>
      <insert type="user" width="3" ignoreNull="false">/notAuthorized/status/@resultCode</insert>
      <insert type="user" width="12" ignoreNull="false">/notAuthorized/authority</insert>
      <insert type="user" width="0" ignoreNull="false">/notAuthorized/originator/userID</insert>
      <insert type="user" width="0" ignoreNull="false">/notAuthorized/status/supplement</insert>
    </inserts>
    <separator>;</separator>
  </format>
</notAuthorized>
<scheduleDelete>
  <format>
    <inserts>
      <insert type="user" width="19" ignoreNull="false">/schedulelog/action/@time</insert>
      <insert type="user" width="48" ignoreNull="false">/schedulelog/@ID</insert>
      <insert type="system" width="6" ignoreNull="false">type</insert>
      <insert type="user" width="3" ignoreNull="false">/schedulelog/status/@resultCode</insert>
      <insert type="user" width="0" ignoreNull="false">/schedulelog/sourceAgent/@agent</insert>
      <insert type="user" width="12" ignoreNull="false">/schedulelog/action</insert>
      <insert type="user" width="0" ignoreNull="false">/schedulelog/originator/userID</insert>
      <insert type="user" width="0" ignoreNull="true">/schedulelog/status/supplement</insert>
    </inserts>
    <separator>;</separator>
  </format>
</scheduleDelete>
<scheduleExpire>
  <format>
    <inserts>
      <insert type="user" width="19" ignoreNull="false">/schedulelog/action/@time</insert>
      <insert type="user" width="48" ignoreNull="false">/schedulelog/@ID</insert>
      <insert type="system" width="6" ignoreNull="false">type</insert>
      <insert type="user" width="3" ignoreNull="false">/schedulelog/status/@resultCode</insert>
      <insert type="user" width="0" ignoreNull="false">/schedulelog/sourceAgent/@agent</insert>
      <insert type="user" width="12" ignoreNull="false">/schedulelog/action</insert>
      <insert type="user" width="0" ignoreNull="false">/schedulelog/originator/userID</insert>
      <insert type="user" width="0" ignoreNull="true">/schedulelog/status/supplement</insert>
    </inserts>
    <separator>;</separator>
  </format>
</scheduleExpire>
<scheduleSkipped>
  <format>
    <inserts>
      <insert type="user" width="19" ignoreNull="false">/schedulelog/action/@time</insert>
      <insert type="user" width="48" ignoreNull="false">/schedulelog/@ID</insert>
      <insert type="system" width="6" ignoreNull="false">type</insert>
      <insert type="user" width="3" ignoreNull="false">/schedulelog/status/@resultCode</insert>
      <insert type="user" width="0" ignoreNull="false">/schedulelog/sourceAgent/@agent</insert>
      <insert type="user" width="12" ignoreNull="false">/schedulelog/action</insert>
      <insert type="user" width="0" ignoreNull="false">/schedulelog/originator/userID</insert>
      <insert type="user" width="0" ignoreNull="true">/schedulelog/status/supplement</insert>
    </inserts>
    <separator>;</separator>
  </format>
</scheduleSkipped>
<scheduleSubmitInfo>
  <format>
    <inserts>
      <insert type="user" width="19" ignoreNull="false">/schedulelog/action/@time</insert>
      <insert type="user" width="48" ignoreNull="false">/schedulelog/@ID</insert>
      <insert type="system" width="6" ignoreNull="false">type</insert>
      <insert type="user" width="3" ignoreNull="false">/schedulelog/status/@resultCode</insert>

```

```

        <insert type="user" width="0" ignoreNull="false">/schedulelog/sourceAgent/@agent</insert>
        <insert type="user" width="12" ignoreNull="false">/schedulelog/action</insert>
        <insert type="user" width="0" ignoreNull="false">/schedulelog/originator/userID</insert>
        <insert type="user" width="0" ignoreNull="true">/schedulelog/schedule/submit</insert>
        <insert type="user" width="0" ignoreNull="true">/schedulelog/schedule/submit/@timezone</
insert>
        <insert type="user" width="3" ignoreNull="true">/schedulelog/schedule/repeat/frequency</
insert>
        <insert type="user" width="12" ignoreNull="true">/schedulelog/schedule/repeat/frequency/
@interval</insert>
        <insert type="user" width="3" ignoreNull="true">/schedulelog/schedule/repeat/expireCount</
insert>
        <insert type="user" width="0" ignoreNull="true">/schedulelog/status/supplement</insert>
    </inserts>
    <separator>;</separator>
</format>
</scheduleSubmitInfo>
<scheduleSubmitTransfer>
    <format>
        <inserts>
            <insert type="user" width="19" ignoreNull="false">/schedulelog/action/@time</insert>
            <insert type="user" width="48" ignoreNull="false">/schedulelog/@ID</insert>
            <insert type="system" width="10" ignoreNull="false">type</insert>
            <insert type="user" width="0" ignoreNull="false">/transaction/sourceAgent/@agent |
            /transaction/sourceWebUser/@webGatewayAgentName |
            /transaction/sourceWebGateway/@webGatewayAgentName</insert>
            <insert type="user" width="0" ignoreNull="false">/transaction/sourceAgent/@QMgr |
            /transaction/sourceWebUser/@webGatewayAgentQMgr |
            /transaction/sourceWebGateway/@webGatewayAgentQMgr</insert>
            <insert type="user" width="0" ignoreNull="false">/transaction/destinationAgent/@agent |
            /transaction/destinationWebUser/@webGatewayAgentName |
            /transaction/destinationWebGateway/@webGatewayAgentName</insert>
            <insert type="user" width="0" ignoreNull="false">/transaction/destinationAgent/@QMgr |
            /transaction/destinationWebUser/@webGatewayAgentQMgr |
            /transaction/destinationWebGateway/@webGatewayAgentQMgr</insert>
        </inserts>
        <separator>;</separator>
    </format>
</scheduleSubmitTransfer>
<scheduleSubmitTransferSet>
    <format>
        <inserts>
            <insert type="user" width="19" ignoreNull="false">/schedulelog/action/@time</insert>
            <insert type="user" width="48" ignoreNull="false">/schedulelog/@ID</insert>
            <insert type="system" width="10" ignoreNull="false">type</insert>
            <insert type="user" width="0" ignoreNull="false">source/file | source/queue</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="5" ignoreNull="true">destination/@type</insert>
            <insert type="user" width="9" ignoreNull="true">destination/@exist</insert>
        </inserts>
        <separator>;</separator>
    </format>
</scheduleSubmitTransferSet>
<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="3" ignoreNull="true">/transaction/status/@resultCode</insert>
            <insert type="user" width="0" ignoreNull="false">/transaction/sourceAgent/@agent |
            /transaction/sourceWebUser/@webGatewayAgentName |
            /transaction/sourceWebGateway/@webGatewayAgentName</insert>
            <insert type="user" width="0" ignoreNull="true">/transaction/sourceAgent/@QMgr |
            /transaction/sourceWebUser/@webGatewayAgentQMgr |
            /transaction/sourceWebGateway/@webGatewayAgentQMgr</insert>
            <insert type="user" width="0" ignoreNull="true">/transaction/sourceAgent/@agentType |
            /transaction/sourceWebUser/@webGatewayAgentType |
            /transaction/sourceWebGateway/@webGatewayAgentType</insert>
            <insert type="user" width="0" ignoreNull="false">/transaction/destinationAgent/@agent |
            /transaction/destinationWebUser/@webGatewayAgentName |
            /transaction/destinationWebGateway/@webGatewayAgentName</insert>
            <insert type="user" width="0" ignoreNull="true">/transaction/destinationAgent/@QMgr |
            /transaction/destinationWebUser/@webGatewayAgentQMgr |
            /transaction/destinationWebGateway/@webGatewayAgentQMgr</insert>
            <insert type="user" width="0" ignoreNull="true">/transaction/originator/userID</insert>
            <insert type="user" width="0" ignoreNull="true">/transaction/job/name</insert>
            <insert type="user" width="0" ignoreNull="true">/transaction/scheduleLog/@ID</insert>
        </inserts>

```



```

/transaction/sourceWebGateway/@webGatewayAgentType</insert>
<insert type="user" width="0" ignoreNull="false">/transaction/destinationAgent/@agent |
/transaction/destinationWebUser/@webGatewayAgentName |
/transaction/destinationWebGateway/@webGatewayAgentName</insert>
<insert type="user" width="0" ignoreNull="true">/transaction/destinationAgent/@QMgr |
/transaction/destinationWebUser/@webGatewayAgentQMgr |
/transaction/destinationWebGateway/@webGatewayAgentQMgr</insert>
<insert type="user" width="0" ignoreNull="true">/transaction/destinationAgent/@agentType |
/transaction/destinationWebUser/@webGatewayAgentType |
/transaction/destinationWebGateway/@webGatewayAgentType</insert>
<insert type="user" width="0" ignoreNull="true">/transaction/originator/userID</insert>
<insert type="user" width="0" ignoreNull="true">/transaction/job/name</insert>
<insert type="user" width="0" ignoreNull="true">/transaction/status/supplement</insert>
</inserts>
<separator>;</separator>
</format>
</transferDelete>
<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="true">source/file/@alias | source/queue/@alias</
insert>
<insert type="user" width="0" ignoreNull="true">source/file/@filesystem | source/queue/
@filesystem</insert>
<insert type="user" width="0" ignoreNull="true">source/@correlationBoolean1</insert>
<insert type="user" width="0" ignoreNull="true">source/@correlationNum1</insert>
<insert type="user" width="0" ignoreNull="true">source/@correlationString1</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">destination/file/@alias | destination/queue/
@alias</insert>
<insert type="user" width="0" ignoreNull="true">destination/file/@filesystem | destination/
queue/@filesystem</insert>
<insert type="user" width="0" ignoreNull="true">destination/file/@truncateRecords</insert>
<insert type="user" width="0" ignoreNull="true">destination/@correlationBoolean1</insert>
<insert type="user" width="0" ignoreNull="true">destination/@correlationNum1</insert>
<insert type="user" width="0" ignoreNull="true">destination/@correlationString1</insert>
<insert type="user" width="0" ignoreNull="true">status/supplement</insert>
</inserts>
<separator>;</separator>
</format>
</transferProgress>
</messageTypes>
</logFormatDefinition>

```

Související odkazy

[Formát samostatného modulu protokolování souborů MFT](#)

[“XSD formátu samostatného modulu protokolování souborů” na stránce 218](#)

Schéma pro samostatný formát souboru.

XSD formátu samostatného modulu protokolování souborů

Schéma pro samostatný formát souboru.

Schéma

```

<?xml version="1.0" encoding="UTF-8"?>
<!--
@start_non_restricted_prolog@
Version: %Z% %I% %W% %E% %U% [%H% %T%]

Licensed Materials - Property of IBM

```

Copyright IBM Corp. 2011, 2024. All Rights Reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

@end_non_restricted_prolog@

-->

<!--

This schema defines the format of the FileLoggerFormat XML file that contains the definition of the format to use when logging FTE log messages to a file. When an XML file that conforms to this schema is processed by a file logger it can contain definitions for one or more message type(s) that define how log messages of those types are output to the file log.

-->

<xsd:schema xmlns:xsd="https://www.w3.org/2001/XMLSchema">

<xsd:include schemaLocation="fteutils.xsd"/>

<!--

Defines the logFileDefinition and version number
<logFileDefinition version="1.00" ...
 <messageTypes>

 ...

 </messageTypes>

</logFileDefinition>

-->

<xsd:element name="logFileDefinition">

 <xsd:complexType>

 <xsd:sequence>

 <xsd:element name="messageTypes" type="messageTypesType" maxOccurs="1" minOccurs="1"/>

 </xsd:sequence>

 <xsd:attribute name="version" type="versionType" use="required"/>

 </xsd:complexType>

</xsd:element>

<!--

Defines the set of accepted message types. The definition of individual message types is optional. If a particular types element is present but empty then no line will be output for messages of that type. If a particular types element is not present then the default format will be used to format messages of that type.

-->

<xsd:complexType name="messageTypesType">

 <xsd:sequence>

 <xsd:element name="callCompleted" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="callStarted" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="monitorAction" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="monitorCreate" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="monitorFired" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="notAuthorized" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="scheduleDelete" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="scheduleExpire" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="scheduleSkipped" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="scheduleSubmitInfo" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="scheduleSubmitTransfer" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="scheduleSubmitTransferSet" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="transferStarted" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="transferCancelled" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="transferComplete" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="transferDelete" type="messageType" maxOccurs="1" minOccurs="0"/>

 <xsd:element name="transferProgress" type="messageType" maxOccurs="1" minOccurs="0"/>

 </xsd:sequence>

</xsd:complexType>

```

<!--
  Defines the content of a message type definition e.g.

  <callStarted>
  <format>
  ...
  </format>
  <callStarted>
-->
<xsd:complexType name="messageType">
  <xsd:sequence>
    <xsd:element name="format" type="messageFormatType" maxOccurs="1" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<!--
  Defines the content of a message format definition e.g.

  <format>
  <inserts>
  ...
  </inserts>
  <separator>;</separator>
  </format>
-->
<xsd:complexType name="messageFormatType">
  <xsd:sequence>
    <xsd:element name="inserts" type="insertsType" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="separator" type="scheduleType" maxOccurs="1" minOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>

<!--
  Defines the content of the inserts element e.g.

  <inserts>
  <insert ...>
  <insert ...>
  ...
  </inserts>
-->
<xsd:complexType name="insertsType">
  <xsd:sequence>
    <xsd:element name="insert" type="insertType" maxOccurs="unbounded" minOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>

<!--
  Defines the content of an insert definition e.g.

  <insert type="user" width="0" ignoreNull="true">/transaction/@ID</insert>
-->
<xsd:complexType name="insertType">
  <xsd:attribute name="type" type="insertTypeType" use="required"/>
  <xsd:attribute name="width" type="xsd:nonNegativeInteger" use="required"/>
  <xsd:attribute name="ignoreNull" type="xsd:boolean" use="required"/>
</xsd:complexType>

<!--
  Defines the accepted choices for the insert type attribute.
-->
<xsd:simpleType name="insertTypeType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="user"/>
    <xsd:enumeration value="system"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

Související odkazy

[Formát samostatného modulu protokolování souborů MFT](#)

[“Výchozí formát protokolu samostatného modulu protokolování souborů MFT” na stránce 214](#)

Výchozí definice formátu souboru protokolu pro samostatný modul protokolování souborů Managed File Transfer .

Knihovna SCSQFCMD

Knihovna SCSQFCMD poskytovaná produktem IBM MQ Managed File Transfer for z/OS obsahuje členy, kteří se chovají jako šablony pro úlohy, které lze použít k vytvoření konfigurace produktu Managed File Transfer, a k vytvoření a správě agenta nebo modulu protokolování.

Obsah knihovny je uveden v následující tabulce.

Člen	Popis
BFGCOPY	Úloha použitá k vytvoření kopie knihovny SCSQFCMD
BFGCUSTM	Úloha použitá k přizpůsobení kopie knihovny pro agenta nebo modul protokolování
BFGXCROB	fteObfuscate ukázková šablona.
BFGXLGCR	Šablona fteCreateLogger .
BFGXMNCR	fteCreateMonitor ukázková šablona.
BFGXMNDE	fteDeleteMonitor ukázková šablona.
BFGXPRAN	fteAnt Ukázková šablona
BFGXSTDE	fteDeleteScheduledTransfer Ukázková šablona
BFGXTMCR	fteCreateTemplate Ukázková šablona
BFGXTMDE	fteDeleteTemplate Ukázková šablona
BFGXTRCA	fteCancelTransfer Ukázková šablona
BFGXTRCR	fteCreateTransfer Ukázková šablona
BFGYAGST	Šablona pro spuštěnou proceduru úlohy ke spuštění agenta
BFGYLGST	Šablona pro spuštěnou proceduru úlohy pro spuštění modulu protokolování
BFGZAGCL	fteCleanAgent Ukázková šablona
BFGZAGCR	fteCreateAgent Ukázková šablona
BFGZAGDE	fteDeleteAgent Ukázková šablona
BFGZAGLG	fteSetAgentLogLevel Ukázková šablona
BFGZAGLI	fteListAgents Ukázková šablona
BFGZAGPI	ftePingAgent Ukázková šablona
BFGZAGSH	fteShowAgentDetails Ukázková šablona
BFGZAGSP	fteStopAgent Ukázková šablona
BFGZAGST	fteStartAgent Ukázková šablona
BFGZAGTC	fteSetAgentTraceLevel Ukázková šablona
BFGZCFCR	fteSetupCoordination Ukázková šablona
BFGZCFDF	fteChangeDefaultConfigurationOptions Ukázková šablona
BFGZCMCR	fteSetupCommands Ukázková šablona
BFGZCMD	Šablona pro skript REXX používaný ostatními členy v datové sadě
BFGZLGDE	fteDeleteLogger Ukázková šablona
BFGZLGSH	fteShowLoggerDetails Ukázková šablona

Člen	Popis
BFGZLGSP	fteStopLogger Ukázková šablona
BFGZLGST	fteStartLogger Ukázková šablona
BFGZLGTC	fteSetLoggerTraceLevel Ukázková šablona
BFGZMNL	fteListMonitors Ukázková šablona
BFGZPID	fteSetProductId Ukázková šablona
BFGZPROF	Šablona pro skript shellu používaný ostatními členy v datové sadě
BFGZPRSH	fteDisplayVersion Ukázková šablona
BFGZRAS	fteRas Ukázková šablona
BFGZSTLI	fteListScheduledTransfers Ukázková šablona
BFGZTMLI	fteListTemplates Ukázková šablona

Podrobnosti o použití knihovny SCSQFCMD ke generování nové knihovny pro vytvoření konfigurace Managed File Transfer a vytvoření a administraci agenta nebo modulu protokolování viz [Konfigurace Managed File Transfer for z/OS](#).

Související odkazy

“Použití proměnných prostředí ve vlastnostech MFT” na stránce 163

Je možné, aby se proměnné prostředí používaly ve vlastnostech Managed File Transfer, které představují umístění souborů nebo adresářů. To umožňuje, aby se umístění souborů nebo adresářů používaných při spouštění částí produktu lišila v závislosti na aktuálním prostředí (například uživatel spouštějící příkaz).

SYSTEM.FTE

Systém SYSTEM.FTE je téma koordinačního správce front, které produkt Managed File Transfer používá k protokolování přenosů a ukládání informací o agentech, monitorech, plánech a šablonách.

Struktura tématu

```
SYSTEM.FTE
  /Agents
    /agent_name
  /monitors
    /agent_name
  /Scheduler
    /agent_name
  /Templates
    /template_ID
  /Transfers
    /agent_name
    /transfer_ID
  /Log
    /agent_name
    /Monitors
    /schedule_ID
    /transfer_ID
```

SYSTEM.FTE/Agents/název_agenta

Toto téma obsahuje zachované publikování, které popisuje agenta ve vaší síti Managed File Transfer a jeho vlastnosti. Zpráva v tomto tématu je pravidelně aktualizována se stavem agenta. Další informace viz [Formát stavové zprávy agenta MFT](#).

SYSTEM.FTE/monitors/název_agenta

Toto téma obsahuje zachovaná publikování, která popisují monitory prostředků přidružené k agentovi *agent_name*. Kód XML zachovaného publikování odpovídá schématu *MonitorList.xsd*. Další informace viz [Formát zprávy seznamu monitorů MFT](#).

SYSTEM.FTE/Scheduler/název_agenta

Toto téma obsahuje zachované publikování, které popisuje všechny aktivní plány přidružené k agentovi *agent_name*. Kód XML zachovaného publikování odpovídá schématu `ScheduleList.xsd`. Další informace viz [Formát zprávy seznamu plánů MFT](#).

SYSTEM.FTE/Templates

Toto téma obsahuje zachovaná publikování, která popisují všechny šablony definované ve vaší Managed File Transfer topologii.

- Publikace, která je přidružena ke každé šabloně, je publikována v dílčím tématu s názvem `SYSTEM.FTE/Templates/template_ID`.

Příklad obsahu této zachované publikace viz [vzorová zpráva XML šablony MFT](#).

SYSTEM.FTE/Transfers/název_agenta

Toto téma obsahuje publikace, které popisují stav přenosů, které pocházejí od agenta *agent_name*. Publikace přidružené k jednotlivým přenosům jsou publikovány v dílčím tématu s názvem `SYSTEM.FTE/Transfers/agent_name/transfer_ID`. Tyto publikace jsou používány modulem plug-in IBM MQ Explorer k poskytování informací o průběhu jednotlivých přenosů. XML publikace odpovídá schématu `TransferStatus.xsd`. Další informace naleznete v tématu [Formát zprávy o stavu přenosu souborů](#).

SYSTEM.FTE/Log/název_agenta

Toto téma obsahuje publikace, které protokolují informace o přenosech, monitorech a plánech, které pocházejí od agenta *agent_name*. Tyto publikace mohou být protokolovány modulem pro protokolování databáze za účelem poskytnutí záznamů auditu událostí, ke kterým došlo ve vaší síti Managed File Transfer .

- Publikace, které jsou přidruženy k jednotlivým přenosům, jsou publikovány do dílčího tématu s názvem `SYSTEM.FTE/Log/agent_name/transfer_ID` a XML publikace odpovídá schématu `TransferLog.xsd`. Další informace naleznete v tématu [Formáty zpráv protokolu přenosu souborů](#).
- Publikace přidružené ke každému naplánovanému přenosu jsou publikovány v dílčím tématu s názvem `SYSTEM.FTE/Log/agent_name/schedule_ID` a XML publikování odpovídá schématu `ScheduleLog.xsd`. Další informace naleznete v tématu [Formáty zpráv protokolu naplánovaného přenosu souborů](#).
- Publikování přidružená ke každému monitoru jsou publikována v dílčím tématu s názvem `SYSTEM.FTE/Log/agent_name/Monitors/monitor_name/monitor_ID` a XML publikování odpovídá schématu `MonitorLog.xsd`. Další informace viz [Formát zprávy protokolu monitoru MFT](#).

MFT Nastavení fronty agenta

Příkazové skripty MQSC generované příkazem **fteCreateAgent** vytvoří fronty agenta s parametry nastavenými na následující hodnoty. Pokud nepoužijete skripty MQSC poskytnuté k vytvoření front, ale vytvoříte fronty ručně, ujistěte se, že jste nastavili následující parametry na dané hodnoty.

Fronty operací agenta

Fronty operací agenta mají následující názvy:

- `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`

Tabulka 114. Parametry fronty operací agenta	
Parametr	Hodnota (je-li použitelná)
DEFPRTY	0

<i>Tabulka 114. Parametry fronty operací agenta (pokračování)</i>	
Parametr	Hodnota (je-li použitelná)
DEFSOPT	SHARED
GET	POVOLENO
MAXDEPTH	5000
MAXMSGL	4194304
MSGDLVSQ	PRIORITY
PUT	POVOLENO
RETINTVL	999999999
SHARE	
Žádný spouštěč	
USAGE	NORMÁLNÍ
REPLACE	

Fronty oprávnění agenta

Fronty oprávnění agenta mají následující názvy:

- 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

<i>Tabulka 115. Parametry fronty oprávnění agenta</i>	
Parametr	Hodnota (je-li použitelná)
DEFPRTY	0
DEFSOPT	SHARED
GET	POVOLENO
MAXDEPTH	0
MAXMSGL	0
MSGDLVSQ	PRIORITY
PUT	POVOLENO
RETINTVL	999999999
SHARE	
Žádný spouštěč	
USAGE	NORMÁLNÍ
REPLACE	

Související odkazy

[fteCreateAgent \(vytvořit agenta MFT\)](#)

MFT systémové fronty a téma systému

Produkt Managed File Transfer má řadu systémových front a jedno systémové téma, které jsou pouze pro vnitřní použití.

Všechny fronty s názvem začínajícím na SYSTEM.FTE jsou vnitřní systémové fronty pro Managed File Transfer (MFT). Tyto fronty neodstraňujte, protože to brání správnému fungování produktu IBM MQ MFT . Tabulka 116 na stránce 225 zobrazuje, který typ zprávy je v každé frontě:

<i>Tabulka 116. Názvy front, typ a použití</i>		
Název fronty	Typ fronty	Použití
SYSTEM.FTE.AUTHAGT1.agent_name	Oprávnění	Fronta pro konfiguraci oprávnění pro odesílání a příjem požadavků na přenos.
SYSTEM.FTE.AUTHTRN1.agent_name	Oprávnění	Fronta pro konfiguraci oprávnění ke spuštění a zrušení spravovaných přenosů. Také pro spuštění spravovaných volání.
SYSTEM.FTE.AUTHMON1.agent_name	Oprávnění	Fronta pro konfiguraci oprávnění umožňující uživateli vytvořit nebo odstranit monitory prostředků, které byly vytvořeny stejným uživatelem.
SYSTEM.FTE.AUTHOPS1.agent_name	Oprávnění	Fronta pro konfiguraci oprávnění k odstranění monitorů prostředků a naplánovaných přenosů vytvořených jiným uživatelem.
SYSTEM.FTE.AUTHSCH1.agent_name	Oprávnění	Fronta pro konfiguraci oprávnění k vytvoření nebo odstranění naplánovaných přenosů, které byly vytvořeny stejným uživatelem.
SYSTEM.FTE.AUTHADM1.agent_name	Oprávnění	Fronta pro konfiguraci oprávnění k vypnutí agenta pomocí volby -m v příkazu fteStopAgent .
SYSTEM.FTE.COMMAND.agent_name	Operace	Fronta pro odesílání požadavků na příkazy agentovi.
SYSTEM.FTE.DATA.agent_name	Operace	Fronta používaná cílovým agentem pro uložení dat odeslaných zdrojovým agentem.
SYSTEM.FTE.REPLY.agent_name	Operace	Fronta pro příjem odpovědí od cílového agenta.
SYSTEM.FTE.STATE.agent_name	Operace	Fronta pro zadržení stavu požadavku na přenos.
SYSTEM.FTE.EVENT.agent_name	Operace	Fronta pro zadržení historie monitoru prostředků.
SYSTEM.FTE.HA.agent_name	Operace	Fronta používaná jako zámeček vysoce dostupnými instancemi agenta.

Pokud se agent účastní přenosů zpráv ze souboru do souboru nebo ze souboru do zprávy, může být nutné upravit definici fronty `SYSTEM.FTE.STATE.agent_name`, aby se tyto spravované přenosy mohly uskutečnit. Další informace naleznete v tématu [Pokyny pro nastavení atributů produktu MQ a vlastností MFT přidružených k velikosti zprávy](#).



Upozornění: Definice ostatních systémových front nesmíte měnit.

Také neupravujte ani neodstraňujte `SYSTEM.FTE` je také určeno pouze pro interní použití.

Dočasné fronty

Produkt Managed File Transfer vytváří dočasné fronty pro řadu účelů. Název každé fronty začíná řetězcem `WMQFTE`, ve výchozím nastavení. (Tečka je součástí výchozí předpony.) Chcete-li změnit tuto předponu, můžete použít vlastnost **`dynamicQueuePrefix`** v souboru `command.properties`, v souboru `coordination.properties` nebo v obou. Vlastnost v souboru `command.properties` se používá k nastavení předpony dočasných front, které jsou vytvořeny pro odpovědi na příkazy vyžadující odpověď od agenta. Vlastnost v souboru `coordination.properties` se používá k nastavení předpony dočasných front, které jsou vytvořeny pro jiné účely; například `WMQFTE.FTE.TIMECHECK.QUEUE`, kde `WMQFTE` je hodnota definovaná vlastností **`dynamicQueuePrefix`**.

Související odkazy

[Omezení oprávnění uživatele na akcích agenta MFT](#)


Konvence pojmenování objektů MFT

Pro objekty Managed File Transfer použijte následující konvence pojmenování:

- Názvy agentů a modulů protokolování:
 - Může mít délku maximálně 28 znaků a nerozlišují se velká a malá písmena.
 - Zadaná malými nebo smíšenými písmeny jsou převedena na velká písmena.
 - Musí být v souladu se standardními konvencemi pojmenování objektů IBM MQ.
- Tyto konvence jsou podrobně popsány takto: [Pravidla pro pojmenování IBM MQ objektů](#).
- Kromě konvencí pojmenování objektů IBM MQ :
 - Dopředné lomítko (/) nelze použít v názvech agentů nebo v názvech modulů protokolování.
 - Znak procenta (%) nelze použít v názvech agentů nebo v názvech modulů protokolování.
- Názvy vlastností v souborech vlastností rozlišují velikost písmen.
- Názvy správců front rozlišují velikost písmen.
- V názvech souborů se na některých platformách rozlišují malá a velká písmena.
- Názvy šablon monitoru prostředků a přenosu:
 - Nerozlišují se velká a malá písmena
 - Zadaná malými nebo smíšenými písmeny jsou převedena na velká písmena.
 - Nesmí obsahovat znaky hvězdička (*), procento (%) nebo otazník (?)
- Názvy souborových serverů protokolu musí:
 - Minimální délka je 2 znaky, ale maximální délka není omezena.
 - Nerozlišují se velká a malá písmena
 - Musí být v souladu se standardními konvencemi pojmenování objektů IBM MQ.

Tyto konvence jsou podrobně popsány takto: [Pravidla pro pojmenování IBM MQ objektů](#).

Soubory v integrovaném systému souborů IBM i (IFS)

 Názvy souborů v IFS nemohou obsahovat žádný z následujících znaků:

- Zpětné lomítko (\)

- Lomítko (/)
- Dvojtečka (:)
- Hvězdička (*)
- Otazník (?)
- Uvozovky (")
- Symbol menší než (<)
- Symbol větší než (>)
- Svislá čára (|)

Pokusíte-li se přenést soubory s názvy obsahujícími některý z těchto znaků do systému IBM i IFS, přenos těchto souborů se nezdaří.

Názvy datových sad

z/OS Datové sady mají omezení pojmenování, která ovlivňují maximální délku názvu a dostupné znaky, které můžete použít pro názvy datových sad. Názvy členů datové sady PDS mohou mít maximálně osm znaků a nemohou obsahovat znak tečky (.). Při přenosu do datové sady musíte explicitně zadat název, což znamená, že tato omezení pojmenování nezpůsobují problém. Při přenosu ze souborů do členů PDS však cesta k souboru nemusí být mapována na název člena PDS. Při přenosu do datové sady PDS se každý zdrojový soubor stane členem PDS a každý název členu je generován z názvu zdroje.

Názvy členů PDS jsou z/OS nekvalifikované názvy a jsou definovány následujícím regulárním výrazem:

```
[a-zA-Z#@][a-zA-Z0-9#@]{0-7}
```

Následující schéma se používá k převodu zdrojové datové sady nebo názvu zdrojového souboru na platný název člena PDS. Aspekty jsou použity v uvedeném pořadí:

1. Používají se pouze znaky v názvu za posledním dopředným lomítkem (/), posledním zpětným lomítkem (\) nebo posledním dvojtečkou (:). To znamená, že se použije pouze část názvu cesty k souboru.
2. V případě zdrojových souborů (nikoli datových sad nebo členů PDS) jsou znaky následující za posledním znakem tečky (.) a včetně těchto znaků ignorovány.
3. Pro libovolný název delší než osm znaků se použije pouze posledních osm znaků.
4. Tečkové znaky jsou nahrazeny znaky zavináče (@).
5. Neplatné znaky jsou nahrazeny znaky zavináč (@).
6. Pokud převod nevytvoří žádné znaky, název člena PDS je @.

Stavové zprávy agenta MFT

Agenti s vysokou dostupností publikují informace o stavu ve formátu XML.

Ukázkový kód XML zobrazující informace o třech rezervních instancích

```
<?xml version="1.0" encoding="UTF-8"?>
<AgentStandbyStatus version="6.00" xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="AgentStandbyStatus.xsd">
  <instance host="9.122.123.124" agentVersion="9.1.4.0" />
  <instance host="agenthost.ibm.com" agentVersion="9.1.4.0" />
  <instance host="10.11.12.14" agentVersion="9.1.4.0" />
</AgentStandby>
```

Publikování stavu agenta s vestavěným kódem XML stavu pohotovostního režimu.

Kód XML stavu pohotovostního režimu je zobrazen tučným písmem.

```

<?xml version="1.0" encoding="UTF-8"?>
<properties version="1.0">
  <entry key="SourceTransferStates"/>
  <entry key="queueManagerPort">1414</entry>
  <entry key="agentStandbyInstances">&lt;?xml version="1.0" encoding="UTF-8"?&gt;&lt;AgentStandbyStatus
version="6.00"
  xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="AgentStandbyStatus.xsd"&gt;&lt;Instances&gt;&lt;instance
host="9.122.123.124"
agentVersion="9.1.4.0" /&gt;&lt;/instance host="agenthost.ibm.com" agentVersion="9.1.4.0" /
&gt;&lt;/Instances&gt;&lt;/AgentStandbyStatus&gt;</entry>
  <entry key="agentType">STANDARD</entry>
  <entry key="agentDeclaredHostName">MFTHA1</entry>
  <entry key="agentDescription"/>
  <entry key="maxQueuedTransfers">1000</entry>
  <entry key="agentTimeZone">America/Los_Angeles</entry>
  <entry key="agentOsName">Windows Server 2012 R2</entry>
  <entry key="PublishTimeUTC">2019-05-22T06:02:50Z</entry>
  <entry key="queueManagerHost">localhost</entry>
  <entry key="AgentStartTimeUTC">2019-05-22T04:13:02Z</entry>
  <entry key="agentTraceLevel">&lt;?xml version="1.0" encoding="UTF-8"?&gt;&lt;
agentTraceStatus version="6.00" xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="AgentTraceStatus.xsd"&gt;&lt;trace
level="all"&gt;com.ibm.wmqfte&lt;/trace&gt;&lt;/agentTraceStatus&gt;</entry>
  <entry key="DestinationTransferStates"/>
  <entry key="queueManager">MFTHAQM</entry>
  <entry key="agentProductVersion">9.1.4.0</entry>
  <entry key="AgentStatusPublishRate">300</entry>
  <entry key="maxSourceTransfers">25</entry>
  <entry key="AgentStatus">STARTED</entry>
  <entry key="maxDestinationTransfers">25</entry>
  <entry key="agentName">SRC</entry>
  <entry key="CommandTimeUTC">2019-05-22T06:02:50Z</entry>
  <entry key="queueManagerChannel">MFT_HA_CHN</entry>
  <entry key="agentInterfaceVersion">6.00</entry>
  <entry key="agentVersion">p914-L191119</entry>
</properties>

```

Související odkazy

[fteCreateAgent](#)

[agent GET](#)

IBM MQ Internet Pass-Thru odkaz na konfiguraci

IBM MQ Internet Pass-Thru (MQIPT) používá konfigurační soubor nazvaný `mqipt.conf` k definování tras a k řízení akcí serveru MQIPT. V produktu IBM MQ 9.2 lze vlastnosti konfigurace pro příkaz `mqiptAdmin` zadat také v souboru vlastností.

Konfigurační soubor MQIPT

Konfigurační soubor MQIPT se skládá z několika sekcí. Existuje jedna sekce `[global]` a další sekce `[route]` pro každou trasu přes MQIPT, která byla definována.

Každá sekce obsahuje dvojici vlastností název/hodnota. Některé vlastnosti se mohou objevit pouze v sekci `[global]`, některé se mohou objevit pouze v sekcích `[route]` a některé se mohou objevit v sekcích `[route]` a `[global]`. Pokud se vlastnost objeví v sekcích `route` i `[global]`, hodnota vlastnosti v sekci `[route]` přepíše globální hodnotu, ale pouze pro danou trasu. Tímto způsobem lze sekci `[global]` použít k zavedení výchozích hodnot, které se mají použít pro ty vlastnosti, které nejsou nastaveny v jednotlivých `[route]` sekcích.

Sekce `[global]` začíná řádkem obsahujícím znaky `[global]` a končí, když začíná první sekce `[route]`. Sekce `[global]` musí předcházet všem sekcím `[route]` v souboru.

Každá sekce `[route]` začíná řádkem obsahujícím znaky `[route]` a končí, když začíná další sekce `[route]`, nebo když je dosažen konec konfiguračního souboru.

Jakýkoli nerozpoznaný název vlastnosti je ignorován. Pokud má vlastnost v sekci [route] rozpoznáný název, ale má neplatnou hodnotu (například MinConnectionThreads=x nebo HTTP=unsure), je tato trasa zakázána (to znamená, že nenaslouchá žádným příchozím připojením).



Upozornění: Maximální limit pro počet přenosových cest, které lze přidat do souboru `mqipt.conf`, je 100.

Neplatné hodnoty vlastností v sekci [global] mohou bránit spuštění produktu MQIPT nebo příkazového serveru. Pokud se příkazový server nespustí, produkt MQIPT nebude naslouchat administrativním příkazům odeslaným příkazem `mqiptAdmin` na ovlivněný příkazový port. Pokud jsou při aktualizaci souboru MQIPT přítomny vlastnosti s neplatnými hodnotami v sekci [global], zobrazí se varovná zpráva a efektivní hodnota vlastnosti zůstane beze změny. Tím zabráníte tomu, aby neplatné hodnoty vlastností způsobily vypnutí aktivní instance MQIPT při její aktualizaci.

Je-li vlastnost uvedena jako vlastnost s hodnotami `true` nebo `false`, lze v hodnotě vlastnosti použít libovolnou kombinaci velkých a malých písmen.

Hodnotu vlastnosti můžete změnit úpravou souboru `mqipt.conf`. Chcete-li použít jakékoli změny, aktualizujte soubor MQIPT pomocí příkazu `mqiptAdmin` s klíčovým slovem **-refresh**.

Chcete-li do konfiguračního souboru zahrnout komentáře, začněte řádek znakem "#".

Změny určitých vlastností způsobí restartování trasy pouze v případě, že jsou již povoleny jiné vlastnosti. Například jakékoli změny vlastností HTTP se projeví pouze v případě, že je povolena také vlastnost **HTTP**.

Po restartování přenosové cesty dojde k ukončení existujících připojení. Chcete-li toto chování potlačit, nastavte vlastnost **RouteRestart** na hodnotu `false`. Tím zabráníte restartování trasy, což umožní, aby existující připojení zůstala aktivní, dokud nebude znovu povolena vlastnost **RouteRestart**.

Informace o tom, jak nastavit některé jednoduché konfigurace, naleznete v tématu [Začínáme s produktem MQIPT](#). Ukázkovou konfiguraci naleznete v souboru `mqiptSample.conf` v instalačním adresáři MQIPT.

Soubor vlastností mqiptAdmin

Vlastnosti konfigurace pro příkaz `mqiptAdmin` lze zadat v samostatném souboru vlastností. Tyto vlastnosti konfigurace jsou potřebné, když se produkt `mqiptAdmin` připojí k příkazovému portu TLS produktu MQIPT.

Seznam vlastností, které lze zadat v souboru vlastností `mqiptAdmin`, viz "[mqiptAdmin vlastnosti](#)" na [stránce 258](#). V názvech vlastností se rozlišují malá a velká písmena. Všechny nerozpoznané vlastnosti jsou ignorovány.

Komentáře lze zahrnout do souboru vlastností tak, že na začátku řádku začneme znakem "#".

Souhrn vlastností MQIPT

Tato tabulka zobrazuje souhrn vlastností konfigurace MQIPT a obsahuje následující informace:

- Abecední seznam vlastností MQIPT s odkazy na další informace v sekci [route] nebo v sekci [global], pokud se sekce [route] nepoužije.
- Vlastnost, která musí být nastavena na hodnotu `true`, aby měla hodnota efekt.
- Zda vlastnost platí pro sekci [global], sekci [route] nebo obojí.
- Výchozí hodnoty, které se používají v případě, že vlastnost chybí v sekci [route] i v sekci [global]. Při zadávání hodnot `true` a `false` lze použít libovolnou kombinaci velkých a malých písmen.

Název vlastnosti	Vlastnost k nastavení true	Globální	Trasa	Výchozí
AccessPW		yes	no	null
AKTIVNÍ		yes	yes	true
ClientAccess		yes	yes	false



Název vlastnosti	Vlastnost k nastavení true	Globální	Trasa	Výchozí
CommandPort		yes	no	null
CommandPortListenerAddress		yes	no	null
ConnectionLog		yes	no	true
Místo určení		no	yes	null
DestinationPort		no	yes	1414
“EnableAdvanced” na stránce 236		yes	no	false
HTTP		yes	yes	false
HTTPProxy	HTTP	yes	yes	null
HTTPProxyPort	HTTP	yes	yes	8080
HTTPS	HTTP	yes	yes	false
HTTPServer	HTTP	yes	yes	null
HTTPServerPort	HTTP	yes	yes	null
IdleTimeout		yes	yes	0
IgnoreExpiredseznamy CRL		yes	yes	false
LDAP		yes	yes	false
LDAPIgnoreErrors	LDAP	yes	yes	false
LDAPCacheTimeout	LDAP	yes	yes	24
LDAPServer1	LDAP	yes	yes	null
LDAPServer1Port	LDAP	yes	yes	389
LDAPServer1Userid	LDAP	yes	yes	null
LDAPServer1Password	LDAP	yes	yes	null
LDAPServer1Timeout	LDAP	yes	yes	0
LDAPServer2	LDAP	yes	yes	null
LDAPServer2Port	LDAP	yes	yes	389
LDAPServer2Userid	LDAP	yes	yes	null
LDAPServer2Password	LDAP	yes	yes	null
LDAPServer2Timeout	LDAP	yes	yes	0
ListenerAddress		yes	yes	null
ListenerPort		no	yes	null
LocalAddress		yes	yes	null
LocalAdmin		yes	no	true
MaxConnectionPodprocesy		yes	yes	100
MaxLogFileSize		yes	no	50
MinConnectionPodprocesy		yes	yes	5
Název		no	yes	null

Název vlastnosti	Vlastnost k nastavení true	Globální	Trasa	Výchozí
OutgoingPort		no	yes	0
V 9.3.1 PasswordProtection		yes	yes	povinné
QMgrAccess		yes	yes	true
RemoteCommandRemoteCommand		yes	no	NONE
RemoteShutdown		yes	no	false
RouteRestart		yes	yes	true
SecurityExit		yes	yes	false
SecurityExit	SecurityExit	yes	yes	null
SecurityExit	SecurityExit	yes	yes	<i>mgipt_home</i> <i>\exits</i>
SecurityExitČasový limit	SecurityExit	yes	yes	30
SecurityManager (Poznámka 3)		yes	no	false
SecurityManager (Poznámka 3)		yes	no	null
SocksClient		yes	yes	false
SocksProxyHostitel	SocksClient	yes	yes	null
SocksProxyPort	SocksClient	yes	yes	1080
SocksServer		yes	yes	false
SSLClient		yes	yes	false
SSLClientCAKeyRing	Klient SSLClient	yes	yes	null
SSLClientCAKeyRingPW	Klient SSLClient	yes	yes	null
“SSLClientCAKeyRingUseCryptoHardware” na stránce 245	Klient SSLClient	yes	yes	false
SSLClientCipherSady	Klient SSLClient	yes	yes	null
SSLClientConnectČasový limit	Klient SSLClient	yes	yes	30
V 9.3.0 SSLClientCustomOutboundSNI	Klient SSLClient	yes	yes	null
SSLClientDN_C	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_CN	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_DC	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_DNQ	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_L	Klient SSLClient	yes	yes	* (Poznámka 1)


Název vlastnosti	Vlastnost k nastavení true	Globální	Trasa	Výchozí
SSLClientDN_O	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_OU	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_PC	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_ST	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_Street	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_T	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientDN_UID	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientExit		yes	yes	false
SSLClientKeyRing	Klient SSLClient	yes	yes	null
SSLClientKeyRingPW	Klient SSLClient	yes	yes	null
“SSLClientKeyRingUseCryptoHardware” na stránce 248	Klient SSLClient	yes	yes	false
“[MQ 9.3.0, červen 2022]SSLClientOutboundSNI” na stránce 248	Klient SSLClient	yes	yes	hostname
SSLClientProtocols	Klient SSLClient	yes	yes	V 9.3.0 TLSv1.2 TLSv1.3
SSLClientSiteDN_C	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_CN	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_DC	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_DNQ	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_L	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_O	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_OU	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_PC	Klient SSLClient	yes	yes	* (Poznámka 1)

Název vlastnosti	Vlastnost k nastavení true	Globální	Trasa	Výchozí
SSLClientSiteDN_ST	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_Street	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_T	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSiteDN_UID	Klient SSLClient	yes	yes	* (Poznámka 1)
SSLClientSitePopisek	Klient SSLClient	yes	yes	null
SSLCommandPort		yes	no	null
SSLCommandPortCipherSuites		yes	no	null
SSLCommandPortListenerAddress		yes	no	null
SSLCommandPortKeyRing		yes	no	null
SSLCommandPortKeyRingPW		yes	no	null
SSLCommandPortKeyRingUseCryptoHardware		yes	no	false
SSLCommandPortProtokoly		yes	no	V 9.3.0 TLSv1.2 TLSv1.3
SSLCommandPortSiteLabel		yes	no	null
SSLExitData	SSLServerExit	yes	yes	null
SSLExitName	SSLServerExit	yes	yes	null
SSLExitPath	SSLServerExit	yes	yes	<i>mqipt_home</i> <i>\ exits</i>
SSLExitTimeout	SSLServerExit	yes	yes	30
SSLProxyMode		yes	yes	false
SSLPlainConnections	buď SSLServer, nebo SSLProxyMode	yes	yes	false
SSLServer		yes	yes	false
SSLServerAskClientAuth	SSLServer	yes	yes	false
SSLServerCAKeyRing	SSLServer	yes	yes	null
SSLServerCAKeyRingPW	SSLServer	yes	yes	null
“SSLServerCAKeyRingUseCryptoHardware” na stránce 252	SSLServer	yes	yes	false
SSLServerCipher	SSLServer	yes	yes	null
SSLServerDN_C	SSLServer	yes	yes	* (Poznámka 1)

Název vlastnosti	Vlastnost k nastavení true	Globální	Trasa	Výchozí
SSLServerDN_CN	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_DC	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_DNQ	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_L	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_O	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_OU	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_PC	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_ST	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_Street	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_T	SSLServer	yes	yes	* (Poznámka 1)
SSLServerDN_UID	SSLServer	yes	yes	* (Poznámka 1)
SSLServerExit		yes	yes	false
SSLServerKeyRing	SSLServer	yes	yes	null
SSLServerKeyRingPW	SSLServer	yes	yes	null
“SSLServerKeyRingUseCryptoHardware” na stránce 255	SSLServer	yes	yes	false
SSLServerProtocols	SSLServer	yes	yes	V 9.3.0 TLSv1.2 TLSv1.3
SSLServerSiteDN_C	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_CN	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_DC	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_DNQ	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_L	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_O	SSLServer	yes	yes	* (Poznámka 1)

Název vlastnosti	Vlastnost k nastavení true	Globální	Trasa	Výchozí
SSLServerSiteDN_OU	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_PC	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_ST	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_Street	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_T	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteDN_UID	SSLServer	yes	yes	* (Poznámka 1)
SSLServerSiteOznačení	SSLServer	yes	yes	null
StoredCredentials		yes	yes	null
TCPKeepAlive		yes	yes	ne
Trasovat		yes	yes	0
 TraceFilePočet		yes	no	25
 TraceFileVelikost		yes	no	200
“[MQ 9.3.0, červen 2022][MQ 9.3.0, červen 2022] TraceUserData ” na stránce 258		yes	yes	64
UriName	HTTP	yes	yes	(Poznámka 2)

Notes:

1. Hvězdička (*) představuje zástupný znak.
2. Podrobnosti o výchozím nastavení viz [UriName](#) v části “MQIPT Vlastnosti trasy” na stránce 239 .
3.  Tato vlastnost je zamítnuta pro odebrání v budoucí verzi.

Související odkazy

“IBM MQ Internet Pass-Thru odkaz na konfiguraci” na stránce 228

IBM MQ Internet Pass-Thru (MQIPT) používá konfigurační soubor nazvaný `mqipt.conf` k definování tras a k řízení akcí serveru MQIPT . V produktu IBM MQ 9.2 lze vlastnosti konfigurace pro příkaz `mqiptAdmin` zadat také v souboru vlastností.

“MQIPT globálních vlastností” na stránce 235

Konfigurační soubor `mqipt.conf` může obsahovat řadu globálních vlastností.

“MQIPT Vlastnosti trasy” na stránce 239

Konfigurační soubor `mqipt.conf` může obsahovat vlastnosti pro jednotlivé trasy.

MQIPT globálních vlastností

Konfigurační soubor `mqipt.conf` může obsahovat řadu globálních vlastností.

Následující vlastnosti se mohou objevit pouze v `[global]` sekci `mqipt.conf`. Všechny [vlastnosti směrování](#) s výjimkou **ListenerPort**, **Destination**, **DestinationPort**, **Namea** **OutgoingPort** se

mohou také objevit v sekci [global] . Pokud se vlastnost objeví v sekcích route i [global] , hodnota vlastnosti v sekci [route] přepíše globální hodnotu, ale pouze pro danou trasu. Tímto způsobem lze sekci [global] použít k zavedení výchozích hodnot, které se mají použít pro ty vlastnosti, které nejsou nastaveny v jednotlivých [route] sekcích.

AccessPW

Heslo použité k ověření příkazů odeslaných na port příkazu MQIPT pomocí příkazu **mqiptAdmin** .

Hodnota může být buď heslo, které bylo zašifrováno pomocí příkazu **mqiptPW** , nebo heslo v prostém textu. Hesla v prostém textu mohou obsahovat pouze alfanumerické znaky. Důrazně se doporučuje šifrovat hesla, která jsou uložena v konfiguraci MQIPT . Další informace o šifrování hesel v konfiguraci produktu MQIPT naleznete v tématu [Šifrování uložených hesel](#).

Ověření se provádí pro administrativní příkazy přijaté portem příkazu, pokud jsou splněny obě následující podmínky:

- Vlastnost **AccessPW** je určena a nastavena na hodnotu, která není prázdná.
- Vlastnost **RemoteCommandAuthentication** je určena a nastavena na jinou hodnotu než none.

CommandPort

Číslo portu TCP/IP nezabezpečeného příkazového portu. Produkt MQIPT přijímá administrativní příkazy odeslané příkazem **mqiptAdmin** na tento příkazový port.

Připojení k nezabezpečenému příkazovému portu nejsou zabezpečena pomocí TLS. Data odeslaná na příkazový port, včetně přístupového hesla, mohou být přístupná jiným uživatelům sítě. Chcete-li nakonfigurovat příkazový port, který je zabezpečený pomocí TLS, nastavte místo toho vlastnost **SSLCommandPort** .

Není-li vlastnost **CommandPort** uvedena, produkt MQIPT nebude naslouchat administrativním příkazům na nezabezpečeném příkazovém portu. Chcete-li použít výchozí číslo portu 1881, které standardně používá příkaz **mqiptAdmin** , nastavte **CommandPort** na hodnotu 1881.

CommandPortListenerAddress

Adresa lokálního modulu listener, která má být použita nezabezpečeným portem příkazu. Nastavením adresy lokálního modulu listener můžete omezit příchozí připojení k nezabezpečenému příkazovému portu na připojení z konkrétního síťového rozhraní. Předvolba je naslouchat na všech síťových rozhraních.

ConnectionLog

Buď `true` , nebo `false`. Pokud je hodnota nastavena na `true`, produkt MQIPT protokoluje všechny pokusy o připojení (úspěšné nebo jiné) v podadresáři `logs` a události odpojení do souboru `mqiptYYYYMMDDHHmmSS.log` (kde `YYYYMMDDHHmmSS` jsou znaky představující aktuální datum a čas). Výchozí hodnota **ConnectionLog** je `true`. Když se tato vlastnost změní z `true` na `false`, MQIPT zavře existující protokol připojení a vytvoří nový. Nový protokol se použije, když je vlastnost resetována na hodnotu `true`.

EnableAdvanced

Nastavte tuto vlastnost na hodnotu `true` , chcete-li potvrdit, že rozšířené schopnosti, které vyžadují nárok IBM MQ Advanced, IBM MQ Appliance, IBM MQ Advanced for z/OS, nebo IBM MQ Advanced for z/OS VUE , mohou být použity produktem MQIPT. Máte-li odpovídající oprávnění, můžete použít rozšířené funkce v produktu MQIPT. Pokud jsou na trase povoleny rozšířené schopnosti, lokální správce front, který je připojen pomocí trasy MQIPT , musí mít také oprávnění IBM MQ Advanced, IBM MQ Appliance, IBM MQ Advanced for z/OS, nebo IBM MQ Advanced for z/OS VUE . Trasy, které používají rozšířené schopnosti, nelze spustit, pokud není tato vlastnost nastavena na hodnotu `true`. Když se tato vlastnost změní z `true` na `false`, trasy, které používají rozšířené schopnosti, jsou zastaveny.

LocalAdmin

Určuje, zda je povolena lokální administrace bez příkazového portu. Administrativní příkazy odeslané příkazem **mqiptAdmin** s použitím lokální administrace namísto portu příkazu nejsou přijaty, pokud je tato vlastnost nastavena na hodnotu `false`.

Platné hodnoty pro tuto vlastnost jsou `true` a `false`. Výchozí hodnota je `true`.

MaxLogFileSize

Maximální velikost (uvedená v kB) souboru protokolu připojení. Když se velikost souboru zvýší nad toto maximum, vytvoří se záložní kopie (mqipt001.log) a spustí se nový soubor. Uchovávají se pouze dva záložní soubory (mqipt001.log a mqipt002.log); pokaždé, když se hlavní soubor protokolu zaplní, jsou všechny dřívější zálohy vymazány. Výchozí hodnota **MaxLogFileSize** je 50; minimální povolená hodnota je 5.

Ověření RemoteCommand

Určuje, zda mají být ověřeny administrativní příkazy přijaté nezabezpečeným portem příkazu nebo portem příkazu TLS. Příkazy jsou ověřeny kontrolou, zda zadané heslo odpovídá heslu zadanému ve vlastnosti **AccessPW**. Hodnota může být jedna z následujících hodnot:

Není

Na příkazech vydaných na jednom z příkazových portů se neprovádí žádná autentizace. Uživatelé příkazu **mqiptAdmin** nemusí zadávat heslo. Toto je výchozí hodnota.

volitelné

Uživatelé příkazu **mqiptAdmin** nejsou povinni zadat heslo. Pokud je však zadáno heslo, musí být platné.

povinné

Uživatelé příkazu **mqiptAdmin** musí poskytnout platné heslo s každým příkazem vydaným na příkazové porty.

Chcete-li povolit ověřování pro příkazové porty, musí být zadána také vlastnost **AccessPW**.

RemoteShutMimo provoz

Uvádí, zda MQIPT lze vypnout příkazem stop odeslaným na nezabezpečený příkazový port nebo na příkazový port TLS příkazem **mqiptAdmin**. Tato vlastnost musí být nastavena na hodnotu **true**, aby příkazy zastavení přijaté jedním z příkazových portů mohly být zpracovány.

Platné hodnoty pro tuto vlastnost jsou **true** a **false**. Výchozí hodnota je **false**.

SecurityManager

Nastavte tuto vlastnost na hodnotu **true**, chcete-li povolit Java security manager pro tuto instanci produktu MQIPT. Musíte se ujistit, že jsou udělena správná oprávnění. Další informace viz [Java security manager](#). Výchozí hodnota této vlastnosti je **false**.

Tato vlastnost je zamítnuta pro odebrání v budoucí verzi.

Zásada SecurityManager

Úplný název souboru zásad Java security manager. Není-li tato vlastnost nastavena, použijí se pouze výchozí soubory systémových a uživatelských zásad. Pokud je Java security manager již povoleno, pak změny této vlastnosti nemají žádný účinek, dokud nebude Java security manager zakázáno a znovu povoleno.

Deprecated Tato vlastnost je zamítnuta pro odebrání v budoucí verzi.

SSLCommandPort

Číslo portu TCP/IP příkazového portu TLS. Produkt MQIPT přijímá administrativní příkazy odeslané příkazem **mqiptAdmin** na tento příkazový port. Tento port přijímá pouze připojení TLS. Tato vlastnost musí být zadána, aby bylo možné povolit příkazový port TLS.

SSLCommandPortCipherSuites

Název šifrovacích sad, které se mají povolit na příkazovém portu TLS. Více než jednu šifrovací sadu lze zadat oddělením hodnot čárkami. Lze uvést pouze šifrovací sady TLS 1.2 a TLS 1.3, které jsou standardně povoleny v prostředí Java runtime environment (JRE) dodávaném s produktem MQIPT. Není-li tato vlastnost určena, všechny šifrovací sady, které jsou povoleny v prostředí JRE, jsou povoleny na příkazovém portu TLS.

SSLCommandPortListenerAddress

Lokální adresa modulu listener, která má být použita portem příkazu TLS. Nastavením adresy lokálního modulu listener můžete omezit příchozí připojení k příkazovému portu TLS na připojení z konkrétního síťového rozhraní. Předvolba je naslouchat na všech síťových rozhraních.

SSLCommandPortKeyRing

Název souboru svazku klíčů PKCS#12, který obsahuje certifikát serveru příkazového portu TLS.

Na platformách Windows musíte jako oddělovač souborů použít dvojité zpětné lomítko (\\).

SSLCommandPortKeyRingPW

Šifrované heslo pro přístup k souboru svazku klíčů příkazového portu TLS nebo k úložišti klíčů PKCS #11 . Heslo musí být šifrováno pomocí příkazu mqiptPW a hodnota této vlastnosti musí být nastavena na řetězcový výstup pomocí mqiptPW.

SSLCommandPortKeyRingUseCryptoHardware

Určuje, zda se jako úložiště klíčů pro certifikát serveru příkazového portu TLS používá kryptografický hardware, který podporuje rozhraní PKCS #11 . Platné hodnoty pro tuto vlastnost jsou true a false. Je-li tato vlastnost nastavena na hodnotu true, nelze zadat také parametr **SSLCommandPortKeyRing** .

Použití šifrovacího hardwaru v produktu MQIPT je funkce IBM MQ Advanced . Vlastnost EnableAdvancedCapabilities musí být nastavena na hodnotu true , abyste potvrdili, že máte nárok IBM MQ Advanced .

SSLCommandPortProtokoly

Čárkami oddělený seznam protokolů, které se mají povolit na příkazovém portu TLS. Lze uvést jednu nebo více následujících hodnot.

Tabulka 117. Povolené hodnoty pro protokoly TLS příkazového portu	
Hodnota	Protokol
TLSv1.2	TLS 1.2
V 9.3.0 TLSv1.3	TLS 1.3

Pokud ve verzích starších než IBM MQ 9.2.5 tuto vlastnost neuvedete, jediný protokol, který je standardně povolen, je TLS 1.2. Pokud v produktu IBM MQ 9.2.5 neuvedete tuto vlastnost, jsou standardně povoleny protokoly TLS 1.2 a TLS 1.3 .

SSLCommandPortSiteLabel

Název jmenovky certifikátu serveru používaného příkazovým portem TLS. Není-li tato vlastnost uvedena, je vybrán jakýkoli certifikát v úložišti klíčů portu příkazu TLS, který je kompatibilní s šifrovací sadou.

Trasovat

Úroveň trasování pro globální podprocesy MQIPT , které nejsou přidruženy k trase, a pro trasy, které nemají nastavenou žádnou vlastnost **Trace** . Například hlavní řídicí podproces MQIPT a podprocesy příkazového serveru nejsou přidruženy k přenosové cestě a jsou trasovány pouze v případě, že je v sekci [global] povoleno trasování. Hodnota vlastnosti **Trace** v sekci [route] přepíše globální vlastnost **Trace** pro tuto trasu. Chcete-li získat informace o trasování podprocesů přidružených k přenosové cestě, prohlédněte si téma **Trace** v [route] sekci.

Hodnota této vlastnosti může být jedna z následujících:

0

Trasování není povoleno

Libovolné kladné celé číslo

Trasování je povoleno

Výchozí hodnota je 0.

V 9.3.2 Počet TraceFile

Počet trasovacích souborů v výměnné sadě souborů používaných produktem MQIPT k zápisu trasovacích dat.

Minimální povolená hodnota je 3. Výchozí hodnota je 25.

Změníte-li hodnotu této vlastnosti, aktuální trasovací soubor se zavře a otevře se další soubor v rotující sadě trasovacích souborů.

V 9.3.2 Velikost TraceFile

Maximální velikost trasovacích souborů vytvořených produktem MQIPT, uvedená v MB.

Minimální povolená hodnota je 1. Výchozí hodnota je 200.

Změníte-li hodnotu této vlastnosti, aktuální trasovací soubor se zavře a otevře se další soubor v rotující sadě trasovacích souborů.

MQIPT Vlastnosti trasy

Konfigurační soubor `mqipt.conf` může obsahovat vlastnosti pro jednotlivé trasy.

Sekce `[route]` konfiguračního souboru `mqipt.conf` může obsahovat následující vlastnosti:

Aktivní

Trasa přijímá příchozí připojení pouze v případě, že je hodnota **Active** nastavena na `true`. To znamená, že můžete dočasně vypnout přístup k místu určení nastavením této hodnoty na `false`, aniž byste museli odstranit sekci `[route]` z konfiguračního souboru. Změníte-li tuto vlastnost na `false`, trasa se zastaví při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

ClientAccess

Trasa umožňuje příchozí připojení kanálu klienta pouze v případě, že je hodnota **ClientAccess** nastavena na `true`. Všimněte si, že potenciálně můžete nakonfigurovat produkt MQIPT tak, aby přijímal pouze požadavky klienta, pouze požadavky správce front nebo oba typy požadavků. Tuto vlastnost použijte ve spojení s vlastností **QMGrAccess**. Změníte-li tuto vlastnost na hodnotu `false`, trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Místo určení

Název hostitele (nebo desítková adresa IP s tečkami) správce front nebo následné instance MQIPT, ke které se má tato trasa připojit. Každá sekce `[route]` musí obsahovat explicitní hodnotu **Destination**, ale několik sekcí `[route]` může odkazovat na stejné místo určení. Pokud změna této vlastnosti ovlivní trasu, je trasa zastavena a restartována při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena. Při použití vlastnosti **SocksProxyHost** musí vlastnost **Destination** používat formát adresy IPv4 s tečkami.

DestinationPort

Port na cílovém hostiteli, ke kterému se má tato přenosová cesta připojit. Každá sekce `[route]` musí obsahovat explicitní hodnotu **DestinationPort**, ale několik tras může odkazovat na stejnou kombinaci hodnot **Destination** a **DestinationPort**. Pokud změna této vlastnosti ovlivní trasu, je trasa zastavena a restartována při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

HTTP

Nastavte **HTTP** na hodnotu `true` pro trasy odpovědné za vytváření odchozích požadavků tunelového propojení HTTP. Vlastnost **Destination** pro trasu musí být název hostitele jiného MQIPT, když je HTTP nastaveno na hodnotu `true`. Pro trasy připojené ke správcům front IBM MQ nastavte hodnotu **HTTP** na `false`. Změníte-li tuto vlastnost, trasa se zastaví. Je-li volba HTTP nastavena na hodnotu `true`, musí být zadána také alespoň jedna z vlastností **HTTPProxy** nebo **HTTPServer**. Tuto vlastnost nelze použít ve spojení s vlastností **SocksClient**.

HTTPProxy

Název hostitele (nebo desítková adresa IP s tečkami) serveru proxy HTTP používaného všemi připojeními pro tuto trasu. Požadavek **CONNECT** je vydán na server proxy HTTP místo požadavku **POST**, který se obvykle používá, když není nakonfigurován žádný server proxy HTTP. Změníte-li tuto vlastnost (a vlastnost **HTTP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

HTTPProxyPort

Adresa portu, která se má použít na serveru proxy HTTP . Výchozí hodnota je 8080. Změníte-li tuto vlastnost (a vlastnost **HTTP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

HTTPServer-server

Název hostitele (nebo desítková adresa IP s tečkami) serveru HTTP používaného všemi připojeními pro tuto trasu. Obvykle se jedná o název hostitele jiného MQIPT.

Není-li parametr **HTTPProxy** uveden, produkt MQIPT se připojí k hostiteli uvedenému v souboru **HTTPServer** a vydá požadavky HTTP **POST** na hostitele uvedeného ve vlastnosti trasy **Destination** . Je-li zadán parametr **HTTPProxy** , produkt MQIPT se namísto toho připojí k hostiteli určenému v souboru **HTTPProxy** a vyžádá si, aby server proxy vytvořil tunel k hostiteli určenému v souboru **HTTPServer**.

Pokud je uvedeno **HTTPProxy** , výchozí hodnota je přenosová cesta **Destination**.

Změníte-li tuto vlastnost (a vlastnost **HTTP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

HTTPS

Nastavte **HTTPS** na hodnotu `true` , chcete-li provést požadavky HTTPS . Vlastnosti **HTTP** a **SSLClient** musí být také povoleny a svazek klíčů klienta nakonfigurovaný pomocí vlastnosti **SSLClientKeyRing** nebo **SSLClientKeyRingUseCryptoHardware** , jako pro operaci SSL/TLS. Změníte-li vlastnost **HTTPS** (a vlastnost **HTTP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

HTTPServerPort

Adresa portu, která se má použít na serveru HTTP . Výchozí hodnota je 8080, pokud není zadána hodnota **HTTPProxy** . V takovém případě je výchozí hodnota přenosová cesta **DestinationPort**.

Změníte-li tuto vlastnost (a vlastnost **HTTP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

IdleTimeout

Doba v minutách, po které je nečinné připojení zavřeno. Pověšimněte si, že kanály správce front pro správce front mají také vlastnost **DISCINT** . Pokud nastavíte parametr **IdleTimeout** , poznamenejte si **DISCINT**. Je-li parametr **IdleTimeout** nastaven na hodnotu 0, neexistuje žádný časový limit nečinnosti. Změny této vlastnosti se projeví pouze po restartování přenosové cesty.

IgnoreExpiredseznamů CRL

Nastavte **IgnoreExpiredCRLs** na hodnotu `true` , chcete-li ignorovat vypršelé seznam CRL. Výchozí hodnota je `false`. Všimněte si, že pokud nastavíte volbu **IgnoreExpiredCRLs** na hodnotu `true`, lze k vytvoření připojení SSL/TLS použít odvolaný certifikát.

LDAP

Nastavte **LDAP** na hodnotu `true` , chcete-li povolit použití serveru LDAP při použití připojení SSL/TLS. Produkt MQIPT použije server LDAP k načtení seznamů CRL a ARL. Vlastnost **SSLClient** nebo **SSLServer** musí být také nastavena na hodnotu `true` , aby se tato vlastnost projevila.

LDAPCacheTimeout

Doba vypršení platnosti dočasné mezipaměti, ve které je uložen seznam CRL načtený ze serveru LDAP, v hodinách. Po uplynutí této doby je celá mezipaměť CRL vyprázdněna. Například uvedení hodnoty 1 hodina znamená, že mezipaměť se vyprazdňuje jednou za hodinu. Výchozí hodnota je 24. Pokud zadáte hodnotu časového limitu 0, položky v mezipaměti nevyprší, dokud nebude trasa restartována. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

LDAPIgnoreErrors

Nastavte **LDAPIgnoreErrors** na hodnotu `true` , chcete-li ignorovat jakékoli chyby připojení nebo vypršení časového limitu při provádění hledání LDAP. Pokud produkt MQIPT nemůže provést úspěšné hledání, nepovolí dokončení připojení klienta, pokud není tato vlastnost povolena. Úspěšné hledání znamená, že byl načten seznam CRL nebo pro zadanou certifikační autoritu nejsou k dispozici žádné seznamy CRL. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Poznámka: Pokud tuto vlastnost povolíte, lze k vytvoření připojení SSL/TLS použít odvolaný certifikát.

LDAPServer1

Název hostitele nebo adresa IP hlavního serveru LDAP. Tato vlastnost musí být nastavena, pokud byl protokol LDAP nastaven na hodnotu `true`. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

LDAPServer1Port

Číslo naslouchajícího portu hlavního serveru LDAP. Výchozí hodnota je 389. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

LDAPServer1Userid

ID uživatele potřebné pro přístup k hlavnímu serveru LDAP. Tato vlastnost musí být nastavena, pokud je vyžadována autorizace pro přístup k hlavnímu serveru LDAP. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

LDAPServer1Password

Heslo potřebné pro přístup k hlavnímu serveru LDAP. Tato vlastnost musí být nastavena, pokud byla vlastnost **LDAPServer1Userid** nastavena na hodnotu `true`. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Hodnota může být buď heslo, které bylo zašifrováno pomocí příkazu `mqiPTPW`, nebo heslo v prostém textu. Hesla v prostém textu mohou obsahovat pouze alfanumerické znaky. Důrazně se doporučuje šifrovat hesla, která jsou uložena v konfiguraci MQIPT. Další informace o šifrování hesel v konfiguraci produktu MQIPT naleznete v tématu [Šifrování uložených hesel](#).

LDAPServer1Timeout

Doba v sekundách, po kterou produkt MQIPT čeká na odpověď od hlavního serveru LDAP. Výchozí hodnota je 0, což znamená, že připojení neuplyne časový limit. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

LDAPServer2

Název hostitele nebo adresa IP záložního serveru LDAP. Tato vlastnost je volitelná. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

LDAPServer2Port

Číslo naslouchajícího portu záložního serveru LDAP. Výchozí hodnota je 389. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

LDAPServer2Userid

ID uživatele potřebné pro přístup k záložnímu serveru LDAP. Tato vlastnost musí být nastavena, pokud je vyžadována autorizace pro přístup k záložnímu serveru LDAP. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

LDAPServer2Password

Heslo potřebné pro přístup k záložnímu serveru LDAP. Tato vlastnost musí být nastavena, pokud byla vlastnost **LDAPServer2** nastavena na hodnotu `true`. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Hodnota může být buď heslo, které bylo zašifrováno pomocí příkazu `mqiPTPW`, nebo heslo v prostém textu. Hesla v prostém textu mohou obsahovat pouze alfanumerické znaky. Důrazně se doporučuje šifrovat hesla, která jsou uložena v konfiguraci MQIPT. Další informace o šifrování hesel v konfiguraci produktu MQIPT naleznete v tématu [Šifrování uložených hesel](#).

LDAPServer2Timeout

Doba v sekundách, po kterou bude produkt MQIPT čekat na odezvu ze záložního serveru LDAP.

Výchozí hodnota je 0, což znamená, že připojení neuplyne časový limit. Pokud změníte tuto vlastnost (a vlastnost **LDAP** je nastavena na hodnotu **true**), trasa se zastaví a restartuje při zadání příkazu **refresh**. Všechna připojení k trase jsou zastavena.

ListenerAddress

Tuto vlastnost použijte, pokud má systém MQIPT více adres IP a musíte svázat port modulu listener přenosové cesty se specifickou adresou. To je užitečné pro omezení příchozích připojení na připojení z konkrétního síťového rozhraní. Hodnota této vlastnosti by měla být adresa IP patřící jednomu ze síťových rozhraní na systému, kde je spuštěn produkt MQIPT. Předvolba je přijmout připojení ze všech síťových rozhraní.

ListenerPort

Číslo portu, na kterém by měla trasa naslouchat příchozím požadavkům. Každá sekce `[route]` musí obsahovat explicitní **ListenerPort** hodnotu. Hodnoty **ListenerPort** nastavené v každé sekci musí být odlišné. Lze použít libovolné platné číslo portu, včetně portů 80 a 443, za předpokladu, že zvolené porty nejsou již používány žádným jiným modulem listener TCP/IP spuštěným na stejném hostiteli.

LocalAddress

Adresa IP pro svázání všech připojení pro tuto přenosovou cestu na tomto počítači. Zvolená adresa musí být adresou IP, která je přidružena k jednomu ze síťových rozhraní na počítači, na kterém je spuštěn produkt MQIPT. Změníte-li tuto vlastnost, trasa se zastaví a restartuje při zadání příkazu **refresh**. Všechna připojení k trase jsou zastavena.

MaxConnectionPodprocesy

Maximální počet podprocesů připojení, a tedy maximální počet souběžných připojení, která mohou být obsloužena touto přenosovou cestou. Je-li dosaženo tohoto limitu, hodnota **MaxConnectionThreads** také označuje počet připojení, která jsou zařazena do fronty, když jsou všechny podprocesy používány. Kromě tohoto počtu jsou následné požadavky na připojení odmítnuty.

Minimální povolená hodnota je větší z hodnot 1 a **MinConnectionThreads**.

Pokud se hodnota zvýší, nová hodnota se použije při zadání příkazu **refresh**. Všechna připojení používají novou hodnotu okamžitě. Trasa není zastavena.

Pokud se hodnota sníží, nová hodnota se projeví až po restartování přenosové cesty.

Podprocesy MinConnection

Počet podprocesů připojení přidělených pro obsluhu příchozích připojení na přenosové cestě při spuštění přenosové cesty. Počet přidělených podprocesů neklesne pod tuto hodnotu během doby, kdy je přenosová cesta aktivní.

Hodnota musí být v rozsahu 0 na hodnotu **MaxConnectionThreads**.

Změny této vlastnosti se projeví pouze po restartování přenosové cesty.

Název

Název, který pomáhá identifikovat trasu. Tato vlastnost je volitelná. Hodnota se zobrazí ve zprávách konzoly a v informacích o trasování. Změny této vlastnosti se projeví pouze po restartování přenosové cesty.

OutgoingPort

Počáteční číslo portu používané odchozími připojeními. Rozsah čísel portů se shoduje s hodnotou **MaxConnectionThread** pro tuto trasu. Výchozí hodnota 0 používá číslo portu definované systémem. Změníte-li tuto vlastnost, trasa se zastaví a restartuje při zadání příkazu **refresh**. Všechna připojení k této trase jsou zastavena. Při použití HTTP vyžaduje každé připojení kanálu dva odchozí porty. Další informace naleznete v tématu [Ovládací prvek čísla portu](#).

V 9.3.1 PasswordProtection

Uvádí, zda produkt MQIPT může přidat nebo odebrat ochranu pro pověření odeslaná ve strukturách MQCSP produktem IBM MQ clients, aby se zachovala kompatibilita mezi klientem a správcem front pro trasy MQIPT, které jsou konfigurovány pro přidání nebo odebrání šifrování TLS.

Pověření ve strukturách MQCSP lze buď chránit pomocí funkce ochrany hesla produktu IBM MQ MQCSP, nebo šifrovat pomocí šifrování TLS. Ochrana heslem protokolu MQCSP je užitečná pro účely testování a vývoje, protože je jednodušší než nastavení šifrování TLS, ale není tak bezpečná.

Další informace o ochraně pomocí hesla MQCSP naleznete v tématu [Ochrana pomocí hesla MQCSP](#).

Je-li směrování MQIPT konfigurováno pro přidání nebo odebrání šifrování TLS, může být nutné, aby produkt MQIPT chránil pověření ve struktuře MQCSP nebo aby odebral ochranu heslem MQCSP, aby bylo připojení úspěšné.

Hodnota vlastnosti může být jedna z následujících hodnot:

povinné

Produkt MQIPT zajišťuje, že pověření ve struktuře MQCSP jsou buď šifrována pomocí TLS, nebo chráněna pomocí ochrany heslem MQCSP.

Pokud jsou pověření ve struktuře MQCSP odesílána šifrovaná klientem pomocí šifrování TLS a přenosová cesta MQIPT odebere šifrování TLS, MQIPT chrání pověření pomocí ochrany pomocí hesla MQCSP před předáním pověření do místa určení přenosové cesty. K tomu dochází, když je přenosová cesta MQIPT nakonfigurována s `SSLServer=true` a `SSLClient=false` a vybraná CipherSuite nepoužívá šifru s hodnotou null.

Pokud jsou pověření ve struktuře MQCSP chráněna klientem s ochranou heslem MQCSP, produkt MQIPT ochranu neodebere, a to ani v případě, že připojení mezi produktem MQIPT a místem určení přenosové cesty používá šifrování TLS. Pokud připojení mezi produktem MQIPT a místem určení přenosové cesty používá šifrování TLS, může dojít k selhání připojení s kódem příčiny `MQRC_PASSWORD_PROTECTION_ERROR` (2594).

Toto je výchozí hodnota.

Kompatibilní

Produkt MQIPT používá nebo odebírá ochranu pomocí hesla MQCSP podle potřeby, aby se zajistilo úspěšné připojení.

Pokud jsou pověření ve struktuře MQCSP odesílána klientem šifrovaná pomocí šifrování TLS a přenosová cesta MQIPT odebere šifrování TLS, MQIPT chrání pověření pomocí ochrany heslem MQCSP před předáním hesla do místa určení přenosové cesty. K tomu dochází, když je přenosová cesta MQIPT nakonfigurována s `SSLServer=true` a `SSLClient=false` a vybraná CipherSuite nepoužívá šifru s hodnotou null.

Pokud jsou pověření ve struktuře MQCSP chráněna klientem s ochranou heslem MQCSP a MQIPT přenosová cesta přidává šifrování TLS, MQIPT odebere ochranu hesla MQCSP před předáním pověření do místa určení přenosové cesty. K tomu dochází, když je přenosová cesta MQIPT nakonfigurována s `SSLServer=false` a `SSLClient=true` a vybraná CipherSuite nepoužívá šifru s hodnotou null.

Tato možnost nabízí nejlepší kompatibilitu. Měl by však být používán pouze pro účely testování a vývoje v důvěryhodných sítích, protože nezajišťuje, aby bylo heslo v síti chráněno.

PASSTHRU

Pověření ve struktuře MQCSP jsou předána do cíle trasy produktem MQIPT bez přidání nebo odebrání ochrany pomocí hesla MQCSP. Je-li přenosová cesta MQIPT konfigurována tak, aby přidala nebo odebrala šifrování TLS, může dojít k selhání připojení klienta s kódem příčiny `MQRC_PASSWORD_PROTECTION_ERROR` (2594).

QMGrAccess

Chcete-li povolit příchozí připojení kanálu správce front (například odesílací kanály), nastavte hodnotu **QMGrAccess** na `true`. Změníte-li tuto vlastnost na `false`, trasa se zastaví při zadání příkazu `refresh`. Všechna připojení k této trase jsou zastavena.

RouteRestart

Nastavte **RouteRestart** na hodnotu `false`, chcete-li zastavit opětovné spuštění trasy, když byly změněny jiné vlastnosti trasy a byl vydán příkaz `refresh`. Výchozí hodnota této vlastnosti je `true`.

SecurityExit

Nastavte **SecurityExit** na hodnotu `true`, chcete-li povolit uživatelskou proceduru zabezpečení definovanou uživatelem. Výchozí hodnota této vlastnosti je `false`.

Název **SecurityExit**

Název třídy uživatelské procedury zabezpečení definované uživatelem. Tato vlastnost musí být nastavena, pokud byla vlastnost **SecurityExit** nastavena na hodnotu `true`. Změníte-li tuto vlastnost (a vlastnost **SecurityExit** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k této trase jsou zastavena.

Cesta **SecurityExit**

Úplný název cesty obsahující uživatelskou proceduru pro zabezpečení zprávy. Pokud tato vlastnost nebyla nastavena, bude standardně nastavena na podadresář `exits`. Tato vlastnost může také definovat název souboru JAR (Java archive), který obsahuje uživatelskou proceduru zabezpečení definovanou uživatelem. Změníte-li tuto vlastnost (a parametr **SecurityExit** je nastaven na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k této trase jsou zastavena.

Časový limit **SecurityExit**

Hodnota časového limitu (v sekundách) použitá produktem MQIPT k určení, jak dlouho se má čekat na odezvu při ověřování požadavku na připojení. Výchozí hodnota je 30. Změníte-li tuto vlastnost (a vlastnost **SecurityExit** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SocksClient

Nastavte **SocksClient** na hodnotu `true`, aby se trasa chovala jako klient SOCKS a definovala všechna připojení prostřednictvím serveru proxy SOCKS s vlastnostmi **SocksProxyHost** a **SocksProxyPort**. Změníte-li tuto vlastnost, trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena. Tuto vlastnost nelze použít s:

- **HTTP**
- **SocksServer**
- **SSLClient**
- **SSLProxyMode**

SocksProxyHostitel

Název hostitele (nebo desítková adresa IPv4 s tečkami) serveru proxy SOCKS, který používají všechna připojení pro tuto přenosovou cestu. Změníte-li tuto vlastnost (a vlastnost **SocksClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k této trase jsou zastavena. Při použití vlastnosti **SocksProxyHost** musí vlastnost **Destination** používat formát desetinných čísel oddělených tečkami.

Port **SocksProxy**

Číslo portu, které se má použít na serveru proxy SOCKS. Výchozí hodnota je 1080. Změníte-li tuto vlastnost (a vlastnost **SocksClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SocksServer

Nastavte **SocksServer** na hodnotu `true`, aby trasa fungovala jako server proxy SOCKS a přijímala připojení klienta SOCKS. Změníte-li tuto vlastnost, trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena. Tuto vlastnost nelze použít s následujícími vlastnostmi:

- **SocksClient**
- **SSLProxyMode**
- **SSLServer**

Klient **SSLClient**

Nastavte **SSLClient** na hodnotu `true`, aby se trasa chovala jako klient SSL/TLS a navazovala odchozí připojení SSL/TLS. Nastavení **SSLClient** na hodnotu `true` znamená, že cílem je buď jiná instance serveru MQIPT, která vystupuje jako server SSL/TLS, nebo server HTTP proxy/server.

Nastavíte-li parametr **SSLClient** na hodnotu `true`, musíte zadat svazek klíčů klienta SSL/TLS pomocí vlastnosti **SSLClientKeyRing** nebo **SSLClientCAKeyRing** nebo nakonfigurovat MQIPT tak, aby používal šifrovací hardware, nastavením vlastnosti **SSLClientKeyRingUseCryptoHardware** nebo **SSLClientCAKeyRingUseCryptoHardware**.

Změníte-li **SSLClient**, trasa se zastaví a restartuje se při zadání příkazu refresh. Všechna připojení k této trase jsou zastavena.

Tuto vlastnost nelze použít ve spojení s následující vlastností:

- **SSLProxyMode**

Svazek SSLClientCAKey

Úplný název souboru svazku klíčů obsahujícího certifikáty CA, který se používá k ověřování certifikátů ze serveru SSL/TLS. Na platformách Windows musíte jako oddělovač souborů použít dvojitě zpětné lomítko (\\). Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu refresh. Všechna připojení k trase jsou zastavena.

SSLClientCAKeyRingPW

Heslo pro otevření souboru svazku klíčů CA klienta SSL/TLS uvedeného ve vlastnosti **SSLClientCAKeyRing** nebo pro připojení k úložišti klíčů šifrovacího hardwaru, pokud je vlastnost **SSLClientCAKeyRingUseCryptoHardware** nastavena na hodnotu `true`.

Hodnota může být buď heslo, které bylo zašifrováno pomocí příkazu **mqiPTPW**, nebo úplný název souboru obsahujícího šifrované heslo. Zadáte-li název souboru na platformách Windows, musíte jako oddělovač souborů použít dvojitě zpětné lomítko (\\). Doporučuje se migrovat všechna hesla svazku klíčů, která jsou v současné době uložena v souboru, aby používala nejnovější a nejbezpečnější metodu ochrany, a to opětovným šifrováním hesel pomocí obslužného programu **mqiPTPW**. Další informace o šifrování hesel v konfiguraci produktu MQIPT naleznete v tématu [Šifrování uložených hesel](#).

Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu refresh. Všechna připojení k trase jsou zastavena.

SSLClientCAKeyRingUseCryptoHardware

Určuje, zda se kryptografický hardware, který podporuje rozhraní PKCS #11, používá jako úložiště klíčů pro certifikáty CA používané k ověřování certifikátů serveru ze serveru SSL/TLS, když produkt MQIPT vystupuje jako klient SSL/TLS. Je-li tato vlastnost nastavena na hodnotu `true`, **SSLClientCAKeyRing** nelze nastavit na stejnou trasu.

Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu refresh. Všechna připojení k trase jsou zastavena.

Použití šifrovacího hardwaru s produktem MQIPT je schopnost IBM MQ Advanced. Chcete-li použít tuto schopnost, lokální správce front, který je připojen pomocí přenosové cesty MQIPT, musí mít také nárok IBM MQ Advanced, IBM MQ Appliance, IBM MQ Advanced for z/OS, nebo IBM MQ Advanced for z/OS VUE. Trasa se nespustí, když je tato vlastnost nastavena na hodnotu `true`, pokud není globální vlastnost **EnableAdvancedCapabilities** nastavena na potvrzení, že lze použít schopnosti IBM MQ Advanced.

Sady SSLClientCipher

Název sady SSL/TLS CipherSuite, která má být použita na straně klienta SSL/TLS. Může se jednat o jednu nebo více podporovaných sad CipherSuites. Ponecháte-li tuto vlastnost prázdnou, použije se jakákoli CipherSuite pro povolené protokoly, které jsou kompatibilní s certifikátem klienta v svazku klíčů. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu refresh. Všechna připojení k této trase jsou zastavena.

Časový limit SSLClientConnect

Doba (v sekundách), po kterou klient SSL/TLS čeká na přijetí připojení SSL/TLS. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu refresh. Všechna připojení k trase jsou zastavena.

V 9.3.0 SSLClientCustomOutboundSNI

Uvádí hodnotu SNI (Server Name Indication) (SNI), když MQIPT zahájí připojení TLS k místu určení přenosové cesty, pokud je přenosová cesta nakonfigurována s **SSLClientOutboundSNI** nastavenou na `custom`. Pomocí této vlastnosti nastavíte SNI na specifickou hodnotu, kterou nelze automaticky nastavit pomocí MQIPT. Například, chcete-li nastavit SNI na název hostitele, ale místo určení přenosové cesty je nakonfigurováno s adresou IP.

Hodnota musí být platný název IDN (Internationalized Domain Name) vyhovující specifikaci RFC 3490 a nesmí končit koncovou tečkou. Trasa se nespustí, pokud je zadána neplatná hodnota.

Změníte-li hodnotu této vlastnosti a parametr **SSLClientOutboundSNI** je nastaven na hodnotu `custom`, trasa se zastaví a restartuje při zadání příkazu `refresh`.



Upozornění: Toto nastavení nesmíte použít při předávání připojení kanálu IBM MQ, který má v poli kanálu nakonfigurovaný popis certifikátu **CERTLABL**. Pokud postoupíte klienta takovým způsobem, bude odmítnut s návratovým kódem `MQRC_SSL_INITIALIZATION_ERROR` a s chybou `AMQ9673` vytištěnou v protokolech chyby vzdáleného správce front.

SSLClientDN_C

Pomocí této vlastnosti lze přijímat certifikáty přijaté ze serveru SSL/TLS, které se shodují s názvem této země. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, budou přijaty všechny názvy zemí. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_CN

Pomocí této vlastnosti lze přijímat certifikáty přijaté od serveru SSL/TLS, které odpovídají tomuto obecnému názvu. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, budou přijaty všechny obecné názvy. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_DC

Pomocí této vlastnosti lze přijímat certifikáty přijaté ze serveru SSL/TLS, které odpovídají této komponentě domény. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Můžete zadat více datových center tak, že je oddělíte čárkami. Každý DC představuje prvek v názvu domény, například název domény `example.ibm.com` je znázorněn jako příklad, `ibm`, `com` pomocí čárek pro oddělení více hodnot. Pokud tuto vlastnost nezádáte, budou přijaty všechny komponenty domény. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_DNQ

Pomocí této vlastnosti lze přijímat certifikáty přijaté ze serveru SSL/TLS, které odpovídají tomuto kvalifikátoru domény. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, budou přijaty všechny kvalifikátory domény. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_L

Pomocí této vlastnosti můžete přijímat certifikáty přijaté ze serveru SSL/TLS, které odpovídají tomuto umístění. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost neuvédete, implikujete "všechna umístění". Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_O

Pomocí této vlastnosti lze přijímat certifikáty přijaté ze serveru SSL/TLS, které odpovídají této organizaci. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost neuvédete, certifikáty budou přijaty od všech organizací. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_OU

Pomocí této vlastnosti můžete přijmout certifikáty přijaté ze serveru SSL/TLS, které se shodují s touto organizační jednotkou (OU). Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Můžete uvést více organizačních jednotek tak, že je oddělíte čárkami. (Shoda s literálovou čárkou s předponou se znakem zpětného lomítka (\).) Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným názvem organizační jednotky. Změníte-li tuto vlastnost (a parametr **SSLClient** je nastaven na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu k aktualizaci. Všechna připojení k této trase jsou zastavena.

SSLClientDN_PC

Pomocí této vlastnosti lze přijímat certifikáty přijaté ze serveru SSL/TLS, které odpovídají tomuto poštovnímu kódu. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, budou přijata všechna poštovní směrovací čísla. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_ST

Pomocí této vlastnosti lze přijímat certifikáty přijaté ze serveru SSL/TLS, které odpovídají tomuto stavu. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, budou certifikáty přijímány ze serverů ve všech stavech. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_Street

Pomocí této vlastnosti můžete přijmout certifikáty přijaté ze serveru SSL/TLS, které se shodují s tímto názvem ulice. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, budou přijaty všechny názvy ulic. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_T

Pomocí této vlastnosti lze přijímat certifikáty přijaté ze serveru SSL/TLS, které odpovídají tomuto názvu. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, budou přijaty všechny názvy. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientDN_UID

Pomocí této vlastnosti můžete přijímat certifikáty přijaté ze serveru SSL/TLS, které se shodují s tímto ID uživatele. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, budou přijata všechna ID uživatelů. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientExit

Pomocí této vlastnosti můžete povolit nebo zakázat použití uživatelské procedury, když se trasa chová jako klient SSL/TLS. To vám umožňuje definovat podrobnosti o ukončení v konfiguračním souboru, aniž by se skutečně používaly.

Svazek SSLClientKey

Úplný název souboru svazku klíčů obsahujícího certifikát klienta. Na platformách Windows musíte jako oddělovač souborů použít dvojité zpětné lomítko (\\). Změníte-li parametr **SSLClientKeyRing** (a parametr **SSLClient** je nastaven na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientKeyRingPW

Heslo pro otevření souboru svazku klíčů klienta SSL/TLS uvedeného ve vlastnosti **SSLClientKeyRing** nebo pro připojení k úložišti klíčů šifrovacího hardwaru, pokud je vlastnost **SSLClientKeyRingUseCryptoHardware** nastavena na hodnotu `true`.

Hodnota může být buď heslo, které bylo zašifrováno pomocí příkazu **mqiPTPW**, nebo úplný název souboru obsahujícího šifrované heslo. Zadáte-li název souboru na platformách Windows, musíte jako oddělovač souboru použít dvojitě zpětné lomítko (\\). Doporučuje se migrovat všechna hesla svazku klíčů, která jsou v současné době uložena v souboru, aby používala nejnovější a nejbezpečnější metodu ochrany, a to opětovným šifrováním hesel pomocí obslužného programu **mqiPTPW**. Další informace o šifrování hesel v konfiguraci produktu MQIPT naleznete v tématu [Šifrování uložených hesel](#).

Změníte-li parametr **SSLClientKeyRingPW** (a parametr **SSLClient** je nastaven na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientKeyRingUseCryptoHardware

Určuje, zda se kryptografický hardware, který podporuje rozhraní PKCS #11, používá jako úložiště klíčů obsahující certifikát klienta, když produkt MQIPT vystupuje jako klient SSL/TLS. Je-li tato vlastnost nastavena na hodnotu `true`, **SSLClientKeyRing** nelze nastavit na stejné trase.

Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Použití šifrovacího hardwaru s produktem MQIPT je schopnost IBM MQ Advanced. Chcete-li použít tuto schopnost, lokální správce front, který je připojen pomocí přenosové cesty MQIPT, musí mít také nárok IBM MQ Advanced, IBM MQ Appliance, IBM MQ Advanced for z/OS, nebo IBM MQ Advanced for z/OS VUE. Trasa se nespustí, když je tato vlastnost nastavena na hodnotu `true`, pokud není globální vlastnost **EnableAdvancedCapabilities** nastavena na potvrzení, že lze použít schopnosti IBM MQ Advanced.

V 9.3.0 SSLClientOutboundSNI

Uvádí hodnotu rozšíření [Indikace názvu serveru \(SNI\)](#), když produkt MQIPT zahájí připojení TLS k místu určení přenosové cesty. Rozhraní SNI je buď používáno správcem front IBM MQ k prezentaci správného certifikátu během navázání komunikace TLS, nebo ke směrování připojení k místu určení v závislosti na konfiguraci.

Tato vlastnost je použitelná pouze pro trasy, které jsou definovány pomocí `SSLClient=true`, a nelze ji zadat pro trasy definované pomocí `HTTP=true`. Změníte-li hodnotu této vlastnosti a parametr **SSLClient** je nastaven na hodnotu `true`, trasa se zastaví a restartuje při zadání příkazu `refresh`.



Upozornění: Je-li cílový kanál konfigurován s popisem certifikátu v poli **CERTLABL** objektu kanálu, musíte nastavit nastavení **CERTLABL** na hodnotu kanálu. Pokud je klient postoupen bez nastavení SNI kanálu, je odmítnut s návratovým kódem `MQRC_SSL_INITIALIZATION_ERROR` a zprávou `AMQ9673` vytištěnou v protokolech chyb vzdáleného správce front.

Hodnota vlastnosti může být jedna z následujících hodnot:

hostname

Hodnota SNI je nastavena na název hostitele místa určení přenosové cesty. Tuto volbu použijte, pokud se trasa připojuje k prostředku pro vyrovnávání zátěže nebo směrovači, který používá SNI ke směrování požadavků. Například produkt Red Hat® OpenShift® Container Platform Router používá SNI ke směrování požadavků do správce front IBM MQ.

Je-li cílem přenosové cesty správce front, požadavky na připojení obdrží během navázání komunikace TLS výchozí certifikát vzdáleného správce front, a proto nelze použít certifikáty pro jednotlivé kanály.

Pokud je místo určení přenosové cesty uvedeno pomocí adresy IP a nelze provést zpětné vyhledání DNS, SNI je prázdné.

Toto je výchozí hodnota.

kanál

Hodnota SNI je nastavena na název kanálu IBM MQ . Tuto volbu použijte, chcete-li povolit použití certifikátů pro jednotlivé kanály správcem cílové fronty, pokud připojení přijatá přenosovou cestou neobsahují název kanálu v rozhraní SNI z jednoho z následujících důvodů:

- Přenosová cesta je nakonfigurována tak, aby přijímala připojení, která nejsou zabezpečena pomocí TLS, buď pomocí `SSLServer=false` , nebo pomocí `SSLPlainConnections=true`.
- Aplikace, která se připojuje k přenosové cestě, nemůže nastavit SNI nebo je konfigurována pro nastavení SNI na jinou hodnotu než název kanálu IBM MQ .

PASSTHRU

Je-li přenosová cesta definována s `SSLServer=true`, SNI na odchozím připojení se nastaví na hodnotu SNI přijatého na příchozím připojení k přenosové cestě. Není-li přenosová cesta konfigurována tak, aby přijímala připojení TLS, je SNI nastaven na cílový název hostitele.

vlastní

Hodnota SNI je nastavena na hodnotu uvedenou ve vlastnosti **SSLClientCustomOutboundSNI** . Není-li vlastnost **SSLClientCustomOutboundSNI** uvedena, SNI se nastaví tak, jako by byla přenosová cesta nakonfigurována s `SSLClientOutboundSNI=hostname`.

Není

SNI není nastaveno.

SSLClientProtocols

Používá se k omezení sady povolených protokolů zabezpečeného soketu, které se používají k vytvoření odchozích připojení k místu určenému pro trasu, když je parametr **SSLClient** nastaven na hodnotu `true`.

Můžete zadat více hodnot tak, že je oddělíte čárkami. Pokud ve verzích starších než IBM MQ 9.2.5 tuto vlastnost neuvedete, jediný protokol, který je standardně povolen, je TLS 1.2. Pokud v produktu IBM MQ 9.2.5 neuvedete tuto vlastnost, jsou standardně povoleny protokoly TLS 1.2 a TLS 1.3 . Chcete-li povolit jiné protokoly než TLS 1.2 nebo TLS 1.3, musíte určit protokoly, které mají být povoleny v této vlastnosti, a také přidat podporu pro protokol v produktu Java runtime environment podle postupu v části [Povolení zamítnutých protokolů a CipherSuites](#). Můžete uvést jednu nebo více následujících hodnot.

Tabulka 118. Povolené hodnoty pro protokoly SSL/TLS

Hodnota	Protokol
SSLv3	SSL 3.0
TLSv1	TLS 1.0
TLSv1.1	TLS 1.1
TLSv1.2	TLS 1.2
V 9.3.0 TLSv1.3	TLS 1.3

Použijte položku uvedenou ve sloupci **Hodnota** ve vlastnosti trasy. Odpovídající položka ve sloupci **Protokol** je pouze pro informaci.

SSLClientSiteDN_C

Tato vlastnost slouží k zadání názvu země pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s libovolným názvem země. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_CN

Pomocí této vlastnosti lze určit obecný název pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s jakýmkoli běžným názvem. Změníte-li tuto vlastnost (a vlastnost

SSLClient je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_DC

Tato vlastnost slouží k zadání názvu komponenty domény pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Můžete zadat více datových center tak, že je oddělíte čárkami. Každý DC představuje prvek v názvu domény, například název domény `example.ibm.com` je znázorněn jako příklad, `ibm`, `com` pomocí čárek pro oddělení více hodnot. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným názvem komponenty domény. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_DNq

Pomocí této vlastnosti lze určit kvalifikátor domény pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným kvalifikátorem domény. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_L

Tato vlastnost slouží k zadání názvu umístění pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným názvem umístění. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_O

Tato vlastnost slouží k zadání názvu organizace pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným názvem organizace. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_OU

Tuto vlastnost použijte k uvedení názvu organizační jednotky (OU) pro výběr certifikátu, který se má odeslat na server SSL/TLS. Můžete uvést více organizačních jednotek tak, že je oddělíte čárkami. (Shoda s literálovou čárkou s předponou se znakem zpětného lomítka (\).) Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným názvem organizační jednotky. Změníte-li tuto vlastnost (a parametr **SSLClient** je nastaven na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu k aktualizaci. Všechna připojení k této trase jsou zastavena.

SSLClientSiteDN_PC

Pomocí této vlastnosti lze určit PSČ pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s jakýmkoli poštovním směrovacím číslem. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_ST

Tato vlastnost slouží k zadání názvu stavu pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným názvem stavu. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_Street

Tato vlastnost slouží k zadání názvu ulice pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným názvem ulice. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_T

Tato vlastnost slouží k zadání názvu pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost ne zadáte, certifikáty budou přijaty s libovolným titulkem. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLClientSiteDN_UID

Tato vlastnost slouží k zadání ID uživatele pro výběr certifikátu, který má být odeslán na server SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost ne zadáte, certifikáty budou přijaty s libovolným ID uživatele. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Popisek SSLClientSite

Tato vlastnost slouží k zadání názvu popisku pro výběr certifikátu, který má být odeslán na server SSL/TLS. Pokud tuto vlastnost ne zadáte, certifikáty budou přijaty s libovolným názvem popisku. Změníte-li tuto vlastnost (a vlastnost **SSLClient** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLExitData

Tato vlastnost slouží k zadání řetězce definovaného uživatelem, který má být předán uživatelské proceduře.

SSLExitName

Pomocí této vlastnosti definujete název třídy pro uživatelskou proceduru, která bude volána, když trasa vystupuje jako klient SSL/TLS nebo jako server SSL/TLS. Název musí obsahovat libovolný název balíku, například `com.ibm.mq.ippt.exit.TestExit`.

SSLExitPath

Pomocí této vlastnosti definujete umístění uživatelské procedury, která se má použít k načtení kopie uživatelské procedury. Název musí být úplný název, který se má použít k vyhledání souboru třídy, nebo název souboru `.jar`, který obsahuje soubor třídy; například `C:\mqipt\exits` nebo `C:\mqipt\exits\exits.jar`.

SSLExitTimeout

Pomocí této vlastnosti lze definovat, jak dlouho produkt MQIPT čeká na dokončení uživatelské procedury před ukončením požadavku na připojení. Hodnota `0` znamená, že MQIPT čeká neomezeně dlouho.

SSLPlainConnections

Pomocí této vlastnosti lze určit, zda je protokol SSL/TLS povinný pro připojení k portu modulu listener MQIPT na trase nakonfigurované tak, aby přijímala příchozí připojení SSL/TLS. Tuto vlastnost lze použít pro trasy, pro které je vlastnost **SSLServer** nebo **SSLProxyMode** nastavena na hodnotu `true`. Je-li tato vlastnost povolena, umožňuje nešifrovaná připojení připojit se k portu modulu listener trasy, což znamená, že MQIPT může postoupit všechna IBM MQ připojení k portu modulu listener správce front bez ohledu na to, zda je připojení šifrováno. Pokud tento parametr nenastavíte nebo jej nastavíte na hodnotu `false`, budou povolena pouze příchozí připojení SSL/TLS. Změníte-li tuto vlastnost, trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLProxyMode

Nastavte tuto vlastnost na hodnotu `true`, aby trasa přijímala pouze požadavky na připojení klienta SSL/TLS a tunelovala požadavek přímo do místa určení. Změníte-li tuto vlastnost, trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k této trase jsou zastavena. Tuto vlastnost nelze použít ve spojení s následujícími vlastnostmi:

- **SocksClient**
- **SocksServer**
- **SSLClient**
- **SSLServer**

SSLServer

Nastavte tuto vlastnost na hodnotu `true`, aby trasa fungovala jako server SSL/TLS a přijímala příchozí připojení SSL/TLS. Nastavení **SSLServer** na hodnotu `true` znamená, že volající je jiný klient MQIPT, který vystupuje jako klient SSL/TLS, nebo je klientem nebo správcem front IBM MQ s povoleným SSL/TLS.

Nastavíte-li parametr **SSLServer** na hodnotu `true`, musíte zadat svazek klíčů serveru SSL/TLS pomocí vlastnosti **SSLServerKeyRing** nebo nakonfigurovat produkt MQIPT tak, aby používal šifrovací hardware, nastavením vlastnosti **SSLServerKeyRingUseCryptoHardware**.

Změníte-li tuto vlastnost, trasa se zastaví a restartuje při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Tuto vlastnost nelze použít ve spojení s následujícími vlastnostmi:

- **SocksServer**
- **SSLProxyMode**

SSLServerCAKeyRing

Úplný název souboru svazku klíčů obsahujícího certifikáty CA, který se používá k ověřování certifikátů od klienta SSL/TLS. Na platformách Windows musíte jako oddělovač souborů použít dvojité zpětné lomítko (`\\`). Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k této trase jsou zastavena.

SSLServerCAKeyRingPW

Heslo pro otevření souboru svazku klíčů CA serveru SSL/TLS uvedeného ve vlastnosti **SSLServerCAKeyRing** nebo pro připojení k úložišti klíčů šifrovacího hardwaru, pokud je vlastnost **SSLServerCAKeyRingUseCryptoHardware** nastavena na hodnotu `true`.

Hodnota může být buď heslo, které bylo zašifrováno pomocí příkazu `mqiptPW`, nebo úplný název souboru obsahujícího šifrované heslo. Zadáte-li název souboru na platformách Windows, musíte jako oddělovač souborů použít dvojité zpětné lomítko (`\\`). Doporučuje se migrovat všechna hesla svazku klíčů, která jsou v současné době uložena v souboru, aby používala nejnovější a nejbezpečnější metodu ochrany, a to opětovným šifrováním hesel pomocí obslužného programu `mqiptPW`. Další informace o šifrování hesel v konfiguraci produktu MQIPT naleznete v tématu [Šifrování uložených hesel](#).

Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerCAKeyRingUseCryptoHardware

Určuje, zda se šifrovací hardware, který podporuje rozhraní PKCS #11, používá jako úložiště klíčů pro certifikáty CA používané k ověřování certifikátů od klienta SSL/TLS. Je-li tato vlastnost nastavena na hodnotu `true`, **SSLServerCAKeyRing** nelze nastavit na stejné trase.

Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Použití šifrovacího hardwaru s produktem MQIPT je schopnost IBM MQ Advanced. Chcete-li použít tuto schopnost, lokální správce front, který je připojen pomocí přenosové cesty MQIPT, musí mít také nárok IBM MQ Advanced, IBM MQ Appliance, IBM MQ Advanced for z/OS, nebo IBM MQ Advanced for z/OS VUE. Trasa se nespustí, když je tato vlastnost nastavena na hodnotu `true`, pokud není globální vlastnost **EnableAdvancedCapabilities** nastavena na potvrzení, že lze použít schopnosti IBM MQ Advanced.

SSLServerAskClientAuth

Tuto vlastnost použijte k vyžádání ověření klienta SSL/TLS serverem SSL/TLS. Klient SSL/TLS musí mít vlastní certifikát pro odeslání na server SSL/TLS. Certifikát je načten ze souboru klíčového řetězce. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k této trase jsou zastavena.

Sady SSLServerCipher

Název sady SSL/TLS CipherSuite , která má být použita na straně serveru SSL/TLS. Může se jednat o jednu nebo více podporovaných sad CipherSuites. Ponecháte-li toto pole prázdné, použije se jakákoli sada CipherSuite pro povolené protokoly, které jsou kompatibilní s certifikátem serveru v svazku klíčů. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k této trase jsou zastavena.

SSLServerDN_C

Pomocí této vlastnosti lze přijímat certifikáty přijaté od klienta SSL/TLS s tímto názvem země. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost ne zadáte, certifikáty budou přijaty s libovolným názvem společnosti. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_CN

Pomocí této vlastnosti lze přijímat certifikáty přijaté od klienta SSL/TLS s tímto běžným názvem. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost ne zadáte, certifikáty budou přijaty s jakýmkoli běžným názvem. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_DC

Pomocí této vlastnosti lze přijímat certifikáty přijaté od klienta SSL/TLS tohoto názvu komponenty domény. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Můžete zadat více datových center tak, že je oddělíte čárkami. Každý DC představuje prvek v názvu domény, například název domény `example.ibm.com` je znázorněn jako příklad `,ibm,com` pomocí čárek pro oddělení více hodnot. Pokud tuto vlastnost ne zadáte, certifikáty budou přijaty s libovolným názvem komponenty domény. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_DNQ

Pomocí této vlastnosti lze přijímat certifikáty přijaté od klienta SSL/TLS tohoto kvalifikátoru domény. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost ne zadáte, certifikáty budou přijaty s libovolným kvalifikátorem domény. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_L

Pomocí této vlastnosti můžete přijímat certifikáty přijaté od klienta SSL/TLS tohoto umístění. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost ne zadáte, certifikáty budou přijaty s jakýmkoli umístěním. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_O

Pomocí této vlastnosti lze přijímat certifikáty přijaté od klienta SSL/TLS této organizace. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost ne uvedete, certifikáty budou přijaty s jakoukoli organizací. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_OU

Tuto vlastnost použijte k přijetí certifikátů přijatých od klienta SSL/TLS této organizační jednotky (OU). Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Můžete uvést více organizačních jednotek tak, že je oddělíte čárkami. (Shoda s literálovou čárkou s předponou se znakem zpětného lomítka (\).) Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost ne zadáte, certifikáty budou přijaty s libovolným názvem organizační jednotky.

Změníte-li tuto vlastnost (a parametr **SSLServer** je nastaven na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu k aktualizaci. Všechna připojení k této trase jsou zastavena.

SSLServerDN_PC

Pomocí této vlastnosti lze přijímat certifikáty přijaté od klienta SSL/TLS tohoto poštovního směrovacího čísla. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s jakýmkoli poštovním směrovacím číslem. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_ST

Pomocí této vlastnosti lze přijímat certifikáty přijaté od klienta SSL/TLS tohoto stavu. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty v libovolném stavu. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_Street

Pomocí této vlastnosti můžete přijímat certifikáty přijaté od klienta SSL/TLS s tímto názvem ulice. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným názvem ulice. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_T

Pomocí této vlastnosti lze přijímat certifikáty přijaté od klienta SSL/TLS s tímto názvem. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným titulkem. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerDN_UID

Pomocí této vlastnosti můžete přijímat certifikáty přijaté od klienta SSL/TLS tohoto ID uživatele. Název může mít předponu nebo příponu hvězdičkou (*), aby se rozšířil jeho rozsah. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným ID uživatele. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerExit

Pomocí této vlastnosti můžete povolit nebo zakázat použití uživatelské procedury, pokud trasa funguje jako server SSL/TLS. To vám umožňuje definovat podrobnosti o ukončení v konfiguračním souboru, aniž by se skutečně používaly.

Svazek SSLServerKey

Úplný název souboru svazku klíčů obsahujícího certifikát serveru. Na platformách Windows musíte jako oddělovač souborů použít dvojitě zpětné lomítko (\\). Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerKeyRingPW

Heslo pro otevření souboru svazku klíčů serveru SSL/TLS uvedeného ve vlastnosti **SSLServerKeyRing** nebo pro připojení k úložišti klíčů šifrovacího hardwaru, pokud je vlastnost **SSLServerKeyRingUseCryptoHardware** nastavena na hodnotu `true`.

Hodnota může být buď heslo, které bylo zašifrováno pomocí příkazu **mqiPTW**, nebo úplný název souboru obsahujícího šifrované heslo. Zadáte-li název souboru na platformách Windows, musíte jako oddělovač souborů použít dvojitě zpětné lomítko (\\). Doporučuje se migrovat všechna hesla svazku klíčů, která jsou v současné době uložena v souboru, aby používala nejnovější a nejbezpečnější metodu ochrany, a to opětovným šifrováním hesel pomocí obslužného programu **mqiPTW**. Další informace o šifrování hesel v konfiguraci produktu MQIPT naleznete v tématu Šifrování uložených hesel.

Musíte uvést **SSLServerKeyRingPW** , pokud nastavíte **SSLServer** na `true`.

Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerKeyRingUseCryptoHardware

Určuje, zda se kryptografický hardware, který podporuje rozhraní PKCS #11 , používá jako úložiště klíčů pro certifikát serveru, když produkt MQIPT vystupuje jako server SSL/TLS. Je-li tato vlastnost nastavena na hodnotu `true`, **SSLServerKeyRing** nelze nastavit na stejně trase.

Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Použití šifrovacího hardwaru s produktem MQIPT je schopnost IBM MQ Advanced . Chcete-li použít tuto schopnost, lokální správce front, který je připojen pomocí přenosové cesty MQIPT , musí mít také nárok IBM MQ Advanced, IBM MQ Appliance, IBM MQ Advanced for z/OS, nebo IBM MQ Advanced for z/OS VUE . Trasa se nespustí, když je tato vlastnost nastavena na hodnotu `true` , pokud není globální vlastnost **EnableAdvancedCapabilities** nastavena na potvrzení, že lze použít schopnosti IBM MQ Advanced .

SSLServerProtocols

Používá se k omezení sady povolených protokolů zabezpečeného soketu, které se používají k přijetí příchozích připojení k portu modulu listener trasy pro trasu, když je parametr **SSLServer** nastaven na hodnotu `true`).

Můžete zadat více hodnot tak, že je oddělíte čárkami. Pokud ve verzích starších než IBM MQ 9.2.5 tuto vlastnost neuvedete, jediný protokol, který je standardně povolen, je TLS 1.2. Pokud v produktu IBM MQ 9.2.5 neuvedete tuto vlastnost, jsou standardně povoleny protokoly TLS 1.2 a TLS 1.3 . Chcete-li povolit jiné protokoly než TLS 1.2 nebo TLS 1.3, musíte určit protokoly, které mají být povoleny v této vlastnosti, a také přidat podporu pro protokol v produktu Java runtime environment podle postupu v části Povolení zamítnutých protokolů a CipherSuites. Můžete uvést jednu nebo více následujících hodnot.

Hodnota	Protokol
SSLv3	SSL 3.0
TLSv1	TLS 1.0
TLSv1.1	TLS 1.1
TLSv1.2	TLS 1.2
V 9.3.0 TLSv1.3	TLS 1.3

Použijte položku uvedenou ve sloupci **Hodnota** ve vlastnosti trasy. Odpovídající položka ve sloupci **Protokol** je pouze pro informaci.

SSLServerSiteDN_C

Tato vlastnost slouží k zadání názvu země pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s libovolným názvem země. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_CN

Pomocí této vlastnosti lze určit obecný název pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s jakýmkoli běžným názvem. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_DC

Tato vlastnost slouží k zadání názvu komponenty domény pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Můžete zadat více datových center tak, že je oddělíte čárkami. Každý DC představuje prvek v názvu domény, například název domény `example.ibm.com` je znázorněn jako příklad, `ibm`, `com` pomocí čárek pro oddělení více hodnot. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s libovolným názvem komponenty domény. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_DNQ

Pomocí této vlastnosti lze určit kvalifikátor domény pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s libovolným kvalifikátorem domény. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_L

Tato vlastnost slouží k zadání názvu umístění pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s libovolným názvem umístění. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_O

Tato vlastnost slouží k zadání názvu organizace pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s libovolným názvem organizace. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_OU

Tuto vlastnost použijte k uvedení názvu organizační jednotky (OU) pro výběr certifikátu, který se má odeslat klientovi SSL/TLS. Můžete uvést více organizačních jednotek tak, že je oddělíte čárkami. (Shoda s literálovou čárkou s předponou se znakem zpětného lomítka (\).) Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s libovolným názvem organizační jednotky. Změníte-li tuto vlastnost (a parametr **SSLServer** je nastaven na hodnotu `true`), trasa se zastaví a restartuje při zadání příkazu k aktualizaci. Všechna připojení k této trase jsou zastavena.

SSLServerSiteDN_PC

Pomocí této vlastnosti lze určit PSČ pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s jakýmkoli poštovním směrovacím číslem. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_ST

Tato vlastnost slouží k zadání názvu stavu pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s libovolným názvem stavu. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_Street

Tato vlastnost slouží k zadání názvu ulice pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezadáte, certifikáty budou přijaty s libovolným názvem ulice. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_T

Tato vlastnost slouží k zadání názvu pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným titulkem. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

SSLServerSiteDN_UID

Tato vlastnost slouží k zadání ID uživatele pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Při porovnávání certifikátů se nerozlišují malá a velká písmena. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným ID uživatele. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Popisek SSLServerSite

Tato vlastnost slouží k zadání názvu popisku pro výběr certifikátu, který má být odeslán klientovi SSL/TLS. Pokud tuto vlastnost nezádáte, certifikáty budou přijaty s libovolným názvem popisku. Změníte-li tuto vlastnost (a vlastnost **SSLServer** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`. Všechna připojení k trase jsou zastavena.

Formát StoredCredentials

Pomocí této vlastnosti lze určit, zda hodnoty vlastností hesla používají šifrovaný formát hesla podporovaný v produktu MQIPT from IBM MQ 9.1.5. Produkt MQIPT může téměř vždy zjistit, zda jsou hesla určena ve formátu šifrovaného hesla. Tuto vlastnost je třeba nastavit pouze v nepravděpodobném scénáři, že produkt MQIPT nemůže automaticky rozlišit mezi zašifrovaným heslem a heslem v prostém textu nebo názvem souboru.

Hodnota může být jedna z následujících hodnot:

Šifrovaný

Vlastnosti hesla obsahují šifrované heslo ve formátu, který je podporován v MQIPT z IBM MQ 9.1.5.

COMPAT

Vlastnosti hesla obsahují buď heslo v prostém textu, nebo pro hesla klíčového řetězce název souboru obsahujícího šifrované heslo.

TCPKeepAlive

Nastavte tuto vlastnost na hodnotu `true`, chcete-li povolit pravidelné odesílání paketů udržení aktivity TCP/IP, aby se zabránilo nečinnosti připojení na této trase. To snižuje pravděpodobnost, že připojení MQIPT budou přerušena bránou firewall nebo směrovačem. Odesílání paketů s udržovanou aktivitou TCP/IP je řízeno parametry ladění operačního systému. Další podrobnosti o tom, jak vyladit udržení aktivity, naleznete v dokumentaci k operačnímu systému. Pokud tento parametr nenastavíte nebo jej nastavíte na hodnotu `false`, pakety s udrženou aktivitou se neodešlou.

Trasovat

Úroveň trasování požadovaná pro tuto přenosovou cestu. Povolení trasování pro jednu trasu nepovoluje trasování pro žádné jiné trasy. Potřebujete-li trasovat více než jednu trasu, musíte přidat vlastnost **Trace** do sekce `[route]` každé trasované trasy.

Hodnota této vlastnosti může být jedna z následujících:

0

Trasování není povoleno

Libovolné kladné celé číslo

Trasování je povoleno

Výchozí hodnota je 0.

Pokud sekce `[route]` neobsahuje vlastnost **Trace**, použije se vlastnost **Trace** ze sekce `[global]`. Chcete-li získat informace o podprocesech trasování, které nejsou přidruženy k přenosové cestě, prohlédněte si téma **Trace** v `[global]` sekci. Pokud změna této vlastnosti ovlivní trasu, nová hodnota se použije při zadání příkazu `refresh`. Všechna připojení používají novou hodnotu okamžitě. Trasa není zastavena.

V 9.3.0

V 9.3.0

TraceUserData

Množství uživatelských dat v síťových přenosech přijatých a odeslaných touto přenosovou cestou, která jsou trasována, když je pro tuto přenosovou cestu povoleno trasování. Hodnota může být jedna z následujících hodnot:

0

Nejsou trasována žádná uživatelská data.

vše

Jsou trasována všechna uživatelská data.

numberOf

Je trasován uvedený počet bajtů dat, včetně záhlaví přenosového segmentu (TSH). Zadaná hodnota musí být větší než 15.

UriName

Tuto vlastnost lze použít ke změně názvu jednotného identifikátoru prostředku při použití serveru proxy HTTP, ačkoli výchozí hodnota bude pro většinu konfigurací postačující:

```
HTTP://destination:destination_port/mqipt
```

Změníte-li tuto vlastnost (a vlastnost **HTTP** je nastavena na hodnotu `true`), trasa se zastaví a restartuje se při zadání příkazu `refresh`.

mqiptAdmin vlastnosti

Příkaz **mqiptAdmin** čte vlastnosti konfigurace ze souboru vlastností, který je uveden při spuštění příkazu.

Následující vlastnosti lze zadat v souboru vlastností, který používá příkaz **mqiptAdmin**. V názvech vlastností se rozlišují malá a velká písmena.

PasswordProtectionKeyFile

Název souboru obsahujícího šifrovací klíč použitý k zašifrování hesla úložiště údajů o důvěryhodnosti, které je uvedeno ve vlastnosti **SSLClientCAKeyRingPW**. Není-li tato vlastnost uvedena, použije se k dešifrování hesla výchozí šifrovací klíč. Šifrovací klíč použitý k šifrování hesla úložiště údajů o důvěryhodnosti **mqiptAdmin** se může lišit od šifrovacího klíče použitého k šifrování hesel v konfiguračním souboru `mqipt.conf`.

Svazek SSLClientCAKey

Název souboru úložiště údajů o důvěryhodnosti PKCS#12, které má být použito pro připojení k příkazovému portu TLS produktu MQIPT. Úložiště údajů o důvěryhodnosti by mělo obsahovat certifikát CA certifikační autority, která podepsala certifikát serveru, pro jehož použití je konfigurován příkazový port TLS produktu MQIPT. Zpětné lomítko (\) v názvu souboru musí být uvozeno řídicími znaky a musí být zadáno jako dvojité zpětné lomítko (\\).

SSLClientCAKeyRingPW

Šifrované heslo pro přístup k úložišti údajů o důvěryhodnosti zadanému pomocí vlastnosti **SSLClientCAKeyRing**. Heslo musí být šifrováno pomocí příkazu **mqiptPW** a hodnota této vlastnosti musí být nastavena na řetězcový výstup **mqiptPW**.

Tyto informace byly vyvinuty pro produkty a služby poskytované v USA.

Společnost IBM nemusí nabízet produkty, služby nebo funkce uvedené v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou ve vaší oblasti aktuálně dostupné, získáte od místního zástupce společnosti IBM. Odkazy na produkty, programy nebo služby společnosti IBM v této publikaci nejsou míněny jako vyjádření nutnosti použití pouze uvedených produktů, programů či služeb společnosti IBM. Místo toho lze použít jakýkoli funkčně ekvivalentní produkt, program nebo službu, které neporušují žádná práva k duševnímu vlastnictví IBM. Ověření funkčnosti produktu, programu nebo služby pocházející od jiného výrobce je však povinností uživatele.

Společnost IBM může vlastnit patenty nebo nevyřízené žádosti o patenty zahrnující předměty popsané v tomto dokumentu. Vlastnictví tohoto dokumentu neposkytuje licenci k těmto patentům. Dotazy týkající se licencí můžete posílat písemně na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Odpovědi na dotazy týkající se licencí pro dvoubajtové znakové sady (DBCS) získáte od oddělení IBM Intellectual Property Department ve vaší zemi, nebo tyto dotazy můžete zasílat písemně na adresu:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Následující odstavec se netýká Spojeného království ani jiných zemí, ve kterých je takovéto vyjádření v rozporu s místními zákony: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE "TAK, JAK JE" BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Některé právní řády u určitých transakcí nepřipouštějí vyloučení záruk výslovně vyjádřených nebo vyplývajících z okolností, a proto se na vás toto omezení nemusí vztahovat.

Uvedené údaje mohou obsahovat technické nepřesnosti nebo typografické chyby. Údaje zde uvedené jsou pravidelně upravovány a tyto změny budou zahrnuty v nových vydáních této publikace. Společnost IBM může kdykoli bez upozornění provádět vylepšení nebo změny v produktech či programech popsanych 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
Kordinátor interoperability softwaru, oddělení 49XA
3605 Dálnice 52 N

Rochester, MN 55901
U.S.A.

Poskytnutí takových informací může být podmíněno dodržením určitých podmínek a požadavků zahrnujících v některých případech uhrazení stanoveného poplatku.

Licencovaný program popsáný v těchto informacích a veškerý licencovaný materiál, který je pro něj k dispozici, jsou poskytovány společností IBM na základě podmínek IBM Smlouvy se zákazníkem, IBM Mezinárodní licenční smlouvy pro programy nebo jiné ekvivalentní smlouvy mezi námi.

Jakékoli údaje o výkonnosti obsažené v této publikaci byly zjištěny v řízeném prostředí. Výsledky získané v jakémkoli jiném operačním prostředí se proto mohou výrazně lišit. Některá měření mohla být prováděna na vývojových verzích systémů a není zaručeno, že tato měření budou stejná i na běžně dostupných systémech. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky mohou být jiné. Čtenáři tohoto dokumentu by měli zjistit použitelné údaje pro své specifické prostředí.

Informace týkající se produktů jiných výrobců pocházejí od dodavatelů těchto produktů, z jejich veřejných oznámení nebo z jiných veřejně dostupných zdrojů. Společnost IBM tyto produkty netestovala a nemůže potvrdit správný výkon, kompatibilitu ani žádné jiné výroky týkající se produktů jiných výrobců než IBM. Otázky týkající se kompatibility produktů jiných výrobců by měly být směřovány dodavatelům těchto produktů.

Veškerá tvrzení týkající se budoucího směru vývoje nebo záměrů společnosti IBM se mohou bez upozornění změnit nebo mohou být zrušena a reprezentují pouze cíle a plány společnosti.

Tyto údaje obsahují příklady dat a sestav používaných v běžných obchodních operacích. Aby byla představa úplná, používají se v příkladech jména osob a názvy společností, značek a produktů. Všechna tato jména a názvy jsou fiktivní a jejich podobnost se jmény, názvy a adresami používanými ve skutečnosti je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči společnosti IBM jakýmkoli způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto příklady nebyly plně testovány za všech podmínek. Společnost IBM proto nemůže zaručit spolehlivost, upotřebitelnost nebo funkčnost těchto programů.

Při prohlížení těchto dokumentů v elektronické podobě se nemusí zobrazit všechny fotografie a barevné ilustrace.

Informace o programovacím rozhraní

Informace o programovacím rozhraní, jsou-li poskytnuty, jsou určeny k tomu, aby vám pomohly vytvořit aplikační software pro použití s tímto programem.

Tato příručka obsahuje informace o zamýšlených programovacích rozhraních, která zákazníkům umožňují psát programy za účelem získání služeb produktu WebSphere MQ.

Tyto informace však mohou obsahovat i diagnostické údaje a informace o úpravách a ladění. Informace o diagnostice, úpravách a vyladění jsou poskytovány jako podpora ladění softwarových aplikací.

Důležité: Tyto informace o diagnostice, úpravách a ladění nepoužívejte jako programovací rozhraní, protože se mohou měnit.

Ochranné známky

IBM, logo IBM, ibm.com, jsou ochranné známky společnosti IBM Corporation, registrované v mnoha jurisdikcích po celém světě. Aktuální seznam ochranných známek společnosti IBM je k dispozici na webu "Copyright and trademark information" www.ibm.com/legal/copytrade.shtml. Další názvy produktů a služeb mohou být ochrannými známkami společnosti IBM nebo jiných společností.

Microsoft a Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených státech a případně v dalších jiných zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse ve Spojených státech a případně v dalších jiných zemích.

Tento produkt zahrnuje software vyvinutý projektem Eclipse (<https://www.eclipse.org/>).

Java a všechny ochranné známky a loga založené na termínu Java jsou ochranné známky nebo registrované ochranné známky společnosti Oracle anebo příbuzných společností.



Číslo položky:

(1P) P/N: