9.3

Pianificazione per IBM MQ

Nota

Prima di utilizzare queste informazioni e il prodotto che supportano, leggere le informazioni in “Informazioni particolari” a pagina 211.

Questa edizione si applica alla versione 9 release 3 di IBM® MQ e a tutte le successive release e modifiche se non diversamente indicato nelle nuove edizioni.

Quando si inviano informazioni a IBM, si concede a IBM un diritto non esclusivo di utilizzare o distribuire le informazioni in qualsiasi modo ritenga appropriato senza incorrere in alcun obbligo verso l'utente.

© Copyright International Business Machines Corporation 2007, 2025.

Indice

Pianificazione.....5
tipi di release IBM MQ : considerazioni sulla pianificazione.....6
Considerazioni su IBM MQ e IBM MQ Appliance on premise per la conformità al GDPR.....9
Architetture basate su un singolo gestore code.....18
Architetture basate su più gestori code.....19
Pianificazione delle code e dei cluster distribuiti.....20
Pianificazione della rete di pubblicazione / sottoscrizione distribuita.....73
Pianificazione dei requisiti di storage e prestazioni su Multiplatforms.....112
Requisiti di spazio su disco su Multiplatforms.....113
Pianificazione del supporto del file system su Multiplatforms.....117
Pianificazione del supporto file system per MFT su Multiplatforms.....143
Scelta della registrazione circolare o lineare su Multiplatforms.....144
Memoria condivisa su AIX.....144
Risorse IPC IBM MQ e UNIX System V.....145
Priorità processo IBM MQ e UNIX.....145
Pianificazione dell'ambiente IBM MQ su z/OS.....146
Pianificazione per il gestore code.....146
Pianificazione dell'iniziatore di canali.....175
Pianificazione del gruppo di condivisione code (QSG).....179
Pianificazione del backup e del ripristino.....192
Pianificazione del tuo ambiente z/OS UNIX.....202
pianificazione per Advanced Message Security.....202
pianificazione per Managed File Transfer.....203
Pianificazione dell'uso di IBM MQ Console e REST API su z/OS.....208

Informazioni particolari.....211
Informazioni sull'interfaccia di programmazione.....212
Marchi.....212

Pianificazione di un'architettura IBM MQ

Quando si pianifica l'ambiente IBM MQ , considerare il supporto fornito da IBM MQ per le architetture di gestori code singoli e multipli e per gli stili di messaggistica point-to-point e di pubblicazione / sottoscrizione. Inoltre, pianificare i requisiti delle risorse e l'utilizzo delle funzioni di registrazione e backup.

Informazioni su questa attività

Prima di pianificare la propria architettura IBM MQ , acquisire familiarità con i concetti di IBM MQ di base. Vedere IBM MQ Panoramica tecnica.

Le architetture IBM MQ vanno da semplici architetture che utilizzano un singolo gestore code a reti più complesse di gestori code interconnessi. Più gestori code sono connessi insieme utilizzando tecniche di accodamento distribuito. Per ulteriori informazioni sulla pianificazione di singole architetture di gestori code e di più architetture di gestori code, consultare i seguenti argomenti:

- “Architetture basate su un singolo gestore code” a pagina 18
- “Architetture basate su più gestori code” a pagina 19
  - “Pianificazione delle code e dei cluster distribuiti” a pagina 20
  - “Pianificazione della rete di pubblicazione / sottoscrizione distribuita” a pagina 73

z/OS Su IBM MQ for z/OS è possibile utilizzare le code condivise e i gruppi di condivisione code per implementare il bilanciamento del carico di lavoro e le applicazioni IBM MQ per essere scalabili e altamente disponibili. Per informazioni sulle code condivise e sui gruppi di condivisione code, consultare Code condivise e gruppi di condivisione code.

IBM MQ fornisce due diversi modelli di release:

- La release Long Term Support (LTS) è la più adatta per i sistemi che richiedono una distribuzione a lungo termine e la massima stabilità.
- La release Continuous Delivery (CD) è destinata ai sistemi che devono sfruttare rapidamente gli ultimi miglioramenti funzionali per IBM MQ.

Entrambi i tipi di release sono installati nello stesso modo, ma vi sono considerazioni relative al supporto e alla migrazione che è necessario comprendere. Per ulteriori informazioni, consultare Tipi di release e controllo delle versioni diIBM MQ.

Per informazioni sulla pianificazione di più installazioni, sui requisiti di memoria e prestazioni e sull'utilizzo dei client, consultare gli altri argomenti secondari.

Concetti correlati

Versioni e tipi di release IBM MQ

“Pianificazione dell'ambiente IBM MQ su z/OS” a pagina 146
Quando si pianifica l'ambiente IBM MQ , è necessario considerare i requisiti delle risorse per i dataset, i set di pagine, Db2, le CF (Coupling Facility) e la necessità di funzioni di registrazione e backup. Utilizzare questo argomento per pianificare l'ambiente in cui viene eseguito IBM MQ .

Disponibilità, ripristino e riavvio

Attività correlate

Verifica dei requisiti

Verifica che i messaggi non vadano persi (registrazione)

© Copyright IBM Corp. 2007, 2025

tipi di release IBM MQ : considerazioni sulla pianificazione

I due tipi di release principali per IBM MQ sono: Long Term Support (LTS) e Continuous Delivery (CD). Per ogni piattaforma supportata, il tipo di rilascio scelto influenza l'ordine, l'installazione, la manutenzione e la migrazione.

Per informazioni dettagliate sui tipi di release, consultare IBM MQ tipi di release e controllo delle versioni.

Considerazioni per IBM MQ for Multiplatforms

Come ordinare

All'interno di Passport Advantage ci sono due eAssemblies separati per IBM MQ 9.3. Uno contiene le immagini di installazione per la release di IBM MQ 9.3.0 Long Term Support e l'altro contiene le immagini di installazione per la release di IBM MQ 9.3.x Continuous Delivery . Scaricare le immagini di installazione da eAssembly in base alla propria scelta di release.

Tutte le versioni IBM MQ e per IBM MQ 9.3 sia le release LTS che le release CD , appartengono allo stesso ID prodotto.

La titolarità ad utilizzare IBM MQ si estende all'intero prodotto (PID), in base ai vincoli dei componenti con licenza e delle metriche dei prezzi. Ciò significa che è possibile scegliere liberamente tra le immagini di installazione della release LTS e CD per IBM MQ 9.3.

Installazione

Dopo aver scaricato un'immagine di installazione da Passport Advantage, è necessario selezionare per l'installazione solo i componenti per cui è stata acquistata la titolarità. Consultare IBM MQ informazioni sulla licenza per ulteriori informazioni sui componenti installabili inclusi per ciascun componente addebitabile.

È possibile installare IBM MQ 9.3.0 LTS release e IBM MQ 9.3.x CD release sulla stessa immagine del sistema operativo. Se si esegue questa operazione, i componenti vengono visualizzati come installazioni separate, come supportato dal supporto multi - versione IBM MQ . Ciascuna versione dispone di set distinti di gestori code associati a tale versione.

Ogni nuova release di CD viene fornita come immagine di installazione. La nuova release CD può essere installata insieme a una release esistente oppure una release CD precedente può essere aggiornata dal programma di installazione alla nuova release.

Le release CD contengono miglioramenti funzionali e l'ultima serie di correzioni di difetti e aggiornamenti di sicurezza. Ogni release CD è cumulativa e sostituisce completamente tutte le release precedenti per quella versione di IBM MQ. Quindi, è possibile ignorare una release specifica di CD se non contiene alcuna funzione rilevante per la propria azienda.

Manutenzione

La release LTS è fornita dall'applicazione di fix pack, che forniscono correzioni di difettie aggiornamenti di sicurezza cumulativi (CSU), che forniscono patch di protezione. I fix pack e CSU vengono resi disponibili periodicamente e sono cumulativi.

Per CD, le CSU vengono prodotte solo per l'ultima release CD , che potrebbe essere su una versione successiva.

Occasionalmente, il team di supporto IBM potrebbe richiedere l'applicazione di una fix temporanea. Le fix temporanee sono note anche come fix di emergenza o di test e vengono utilizzate per applicare aggiornamenti urgenti che non possono attendere la successiva distribuzione della manutenzione.

Migrazione tra release LTS e release CD

Esistono dei vincoli e delle limitazioni, ma, generalmente, è possibile migrare un singolo gestore code dall'utilizzo del codice release LTS al codice release CD o dall'utilizzo del codice release CD al codice release LTS , purché la release di destinazione sia superiore a quella utilizzata prima della migrazione.

Sono possibili due approcci:

- Installare la nuova versione del codice in modo che venga aggiornata un'installazione esistente di IBM MQ . Tutti i gestori code associati all'installazione utilizzano la nuova release del codice quando vengono avviati.
- Installare la nuova release del codice come nuova installazione, quindi spostare le singole istanze del gestore code nella nuova installazione utilizzando il comando setmq .

Quando un gestore code avvia l'esecuzione di una release CD del codice, il livello di comando del gestore code viene aggiornato per indicare il nuovo livello di release. Ciò significa che tutte le nuove funzioni fornite nella release sono abilitate e che non è più possibile riavviare il gestore code utilizzando una release del codice con un numero VRM inferiore.

Considerazioni per IBM MQ for z/OS

Come ordinare

Quando si ordina IBM MQ for z/OS 9.3, su ShopZvengono offerte due funzioni separate. Le funzioni corrispondono alla release LTS e alla release CD . Entrambe le funzioni sono applicabili allo stesso ID prodotto (PID). Si tratta dell'ID prodotto concesso in licenza, quindi dove una funzione è concessa in licenza, vi è la possibilità di utilizzare la funzione alternativa, se richiesto. Quando si ordina, si seleziona la funzione corrispondente alla release LTS o CD .

Se si stanno selezionando prodotti da includere in un ServerPac, non è possibile scegliere sia la release LTS che la release CD nello stesso ordine ServerPac , in quanto i prodotti non possono essere installati da SMP/E nella stessa zona di destinazione.

Installazione

Le release LTS e CD sono fornite in serie separate di FMID. Tenere presente che questi FMID non possono essere installati nella stessa zona di destinazione SMP/E. Se sono necessarie entrambe le release LTS e CD :

- Installare la release LTS e CD in zone di destinazione separate.
- Mantenere le librerie di destinazione e di distribuzione separate per i due release.

Se il gestore code si trova in un gruppo di condivisione code, quando si esegue l'aggiornamento all'ultima versione del CD è necessario aggiornare tutti i gestori code del gruppo.

Il livello di comando di un gestore di code è il livello VRM a tre cifre. Un programma IBM MQ può chiamare `MQINQ`, passando il selettore `MQIA_COMMAND_LEVEL` , per ottenere il livello di comando del gestore di code a cui è collegato.

Poiché le release utilizzano FMID differenti, non è possibile aggiornare una release CD con la manutenzione per una release LTS o viceversa. Allo stesso modo, non esiste alcun modo per passare da una versione del codice del prodotto da una release LTS a una release CD o viceversa. Tuttavia, è possibile commutare un gestore code tra i modelli di release. Consultare Migrazione tra release LTS e release CD.

Nota:

Le release di IBM MQ 9.0.x e IBM MQ 9.1.x CD avevano FMID dipendenti da versione e release separati. Pertanto, il passaggio da 9.0.x CD a 9.1.x CD richiede almeno un'installazione SMP/E completa.

Da IBM MQ for z/OS 9.2.0, la release di CD usa una serie di FMID che rimangono gli stessi per tutte le release di IBM MQ for z/OS con un numero di versione 9. Poiché ogni nuova versione di IBM MQ è disponibile sia come release CD che come release LTS , è possibile aggiornare i release CD applicando le PTF a una singola installazione SMP/E anche quando si supera un limite di versione principale. Ad esempio, è possibile passare da IBM MQ for z/OS 9.2.0 CD, a IBM MQ for z/OS 9.2.2 CD, a IBM MQ for z/OS 9.2.4 CD, a IBM MQ for z/OS 9.3.0 CD, applicando le PTF.

È possibile distinguere tra una release LTS e CD con lo stesso livello VRM cercando il messaggio CSQY000I nel log del lavoro del gestore code.

Manutenzione

IBM MQ for z/OS utilizza le PTF per la manutenzione.

LTS Le PTF sono specifiche di una particolare serie di librerie corrispondenti a un livello di release specifico. Per le funzioni UNIX System Services (ovvero, JMS e WEB UI, Connector Pack e Managed File Transfer) le PTF z/OS sono allineate direttamente con i fix pack Multiplatforms e gli aggiornamenti di sicurezza cumulativi (CSU). Queste correzioni sono cumulative e sono rese disponibili contemporaneamente al fix pack Multiplatforms equivalente o CSU.

CD CD Le CSU di solito non vengono rese disponibili tra le release del CD, ma sono incluse nella release IBM MQ for z/OS CD successiva. Puoi anche contattare il supporto per richiedere un + + USERMOD.

Altre correzioni su IBM MQ for z/OS sono correzioni distinte su parti particolari. Queste correzioni risolvono problemi specifici, non sono cumulative e vengono rese disponibili man mano che vengono prodotte.

Migrazione tra release LTS e release CD

Esistono vincoli e limitazioni, ma generalmente è possibile migrare un singolo gestore code dall'utilizzo del codice release LTS al codice release CD o dall'utilizzo del codice release CD al codice release LTS a condizione che la release di destinazione sia superiore a quella in uso prima della migrazione.

Da IBM MQ for z/OS 9.2.0, è possibile migrare avanti e indietro tra le release CD e LTS con lo stesso VRM tutte le volte che è necessario e senza alcun impatto sulla capacità di migrare all'indietro. Ad esempio, un gestore code può essere avviato in IBM MQ for z/OS 9.3.0 LTS, quindi arrestato e avviato in IBM MQ for z/OS 9.3.0 CD, quindi arrestato e avviato in IBM MQ for z/OS 9.3.0 LTS.

IBM MQ for z/OS ha tradizionalmente fornito una funzionalità di fallback (migrazione all'indietro) in modo che dopo un periodo di esecuzione dopo una migrazione sia possibile eseguire il fallback alla release precedente. Questa funzione viene conservata per le release LTS e per quelle CD con un modificatore di `0` come 9.3.0 CD, ma non è possibile quando l'origine o la destinazione di una migrazione è una release CD con un numero di modificatore diverso da zero, ad esempio 9.2.5 o 9.3.1.

I seguenti sono scenari di migrazione validi e illustrano il funzionamento di questo principio:
V 9.3.0 V 9.3.0

Release di origine	Release di destinazione	Note
9.0.0 LTS	CD 9.3.0 LTS o 9.3.0	La migrazione all'indietro non è supportata poiché 9.0.0 LTS non è supportato standard.
LTS 9.1.0	CD 9.3.0 LTS o 9.3.0	Migrazione all'indietro supportata.
LTS 9.2.0	CD 9.3.0 LTS o 9.3.0	Migrazione all'indietro supportata.
CD 9.2.5	CD 9.3.0 LTS o 9.3.0	La migrazione all'indietro non è supportata poiché il release di origine è CD con un modificatore diverso da zero.
CD 9.3.0 LTS o 9.3.0	CD 9.3.1	Migrazione all'indietro non supportata poiché la release di destinazione è CD con un modificatore diverso da zero. `Write to operator with reply` CSQY041D viene emesso per confermare la migrazione.

Attività correlate

Applicazione e rimozione della manutenzione su z/OS

Informazioni correlate

Download di IBM MQ 9.3

Considerazioni su IBM MQ e IBM MQ Appliance on premise per la conformità al GDPR

Per i PID:

Distribuito

- IBM MQ/IBM MQ Advanced - 5724-H72
- IBM MQ for HPE NonStop - 5724-A39

z/OS

- IBM MQ for z/OS - 5655-MQ9
- IBM MQ for z/OS Value Unit Edition - 5655-VU9
- IBM MQ Advanced for z/OS - 5655-AV9
- IBM MQ Advanced for z/OS Value Unit Edition - 5655-AV1

IBM MQ Appliance

- IBM MQ Appliance M2003 - 5900 - ALJ
- IBM MQ Appliance M2002 - 5737-H47

Avviso:

Questo documento contiene informazioni che assistono l'utente nella preparazione per la conformità al GDPR. Fornisce informazioni sulle funzioni di IBM MQ configurate ed aspetti dell'utilizzo del prodotto da considerare per essere assistiti nell'organizzazione degli adempimenti del GDPR. Queste informazioni non sono un elenco esaustivo, a causa dei molti modi in cui i client possono scegliere e configurare le funzioni e della grande varietà di modi in cui il prodotto può essere utilizzato da solo e con applicazioni e sistemi di terze parti.

I clienti sono responsabili del rispetto delle normative di conformità, come European Union General Data Protection Regulation. I clienti sono gli unici responsabili di ottenere consigli legali competenti per identificare e interpretare leggi e norme pertinenti che possono influire sul business ed eventuali azioni da intraprendere per conformarsi a tali normative.

I prodotti, servizi e altre funzionalità qui descritti non sono adatti per tutte le situazioni dei clienti e potrebbero avere una disponibilità limitata. IBM non fornisce consulenza legale, contabile o di revisione contabile né dichiara o garantisce che i suoi servizi o prodotti garantiranno la conformità dei clienti a qualsiasi legge o regolamento.

Sommario

1. GDPR
2. Configurazione del prodotto per il GDPR
3. Ciclo di vita dei dati
4. Raccolta dei dati
5. Archiviazione dei dati
6. Accesso ai dati
7. Elaborazione dei dati

8. Eliminazione dei dati
9. Monitoraggio dei dati
10. Capacità di limitare l'utilizzo dei dati personali
11. Gestione file

GDPR

Il Regolamento generale sulla protezione dei dati (GDPR) è stato adottato dall'Unione Europea ("UE") e si applica dal 25 maggio 2018.

Perché è importante il GDPR?

Il GDPR istituisce un quadro normativo più solido per la protezione dei dati, per il trattamento dei dati personali degli individui. Il GDPR apporta:

- Diritti nuovi e potenziati per gli individui
- Definizione ampliata dei dati personali
- Nuovi obblighi per i processori
- Potenziale per importanti sanzioni pecuniarie in caso di inosservanza
- Notifica di violazione di dati obbligatoria

Ulteriori informazioni su GDPR:

- Portale di informazioni sul GDPR dell'Unione Europea
- Sito webibm.com/GDPR

Configurazione del prodotto - Considerazioni per la conformità al GDPR

Le seguenti sezioni espongono le considerazioni per configurare IBM MQ per aiutare l'organizzazione ad utilizzare il GDPR.

Ciclo di vita dei dati

IBM MQ è un prodotto middleware transazionale orientato ai messaggi che consente alle applicazioni di scambiare in modo asincrono i dati forniti dalle applicazioni. IBM MQ supporta una gamma di API di messaggistica, protocolli e bridge allo scopo di collegare le applicazioni. Come tale, IBM MQ può essere utilizzato per scambiare molte forme di dati, alcuni dei quali potrebbero essere potenzialmente soggetti al GDPR. Esistono diversi prodotti di terze parti con cui IBM MQ potrebbe scambiare dati. Alcuni di questi sono di proprietà di IBM, ma molti altri sono forniti da altri fornitori di tecnologie. Il sito Web Software Product Compatibility Reports fornisce elenchi del software associato. Per considerazioni relative alla conformità al GDPR di un prodotto di terze parti, è necessario consultare la relativa documentazione. Gli amministratori IBM MQ controllano il modo in cui IBM MQ interagisce con i dati che vi passano attraverso, mediante la definizione di code, argomenti e sottoscrizioni.

Quali tipi di flusso di dati attraverso IBM MQ?

Poiché IBM MQ fornisce un servizio di messaggistica asincrona per i dati dell'applicazione, non vi è alcuna risposta definitiva a questa domanda perché i casi di utilizzo variano in base alla distribuzione dell'applicazione. I dati dei messaggi dell'applicazione vengono resi persistenti nei file della coda (serie di pagine o Coupling Facility su z/OS), nei log e negli archivi e il messaggio stesso può contenere dati regolati dal GDPR. I dati dei messaggi forniti dall'applicazione possono essere inclusi anche nei file raccolti per la determinazione dei problemi, ad esempio i log degli errori, i file di traccia e gli FFST. Sull'applicazione z/OS , i dati dei messaggi forniti possono essere inclusi anche nello spazio di indirizzo o nei dump della CF (Coupling Facility).

Di seguito sono riportati alcuni esempi tipici di dati personali che possono essere scambiati utilizzando IBM MQ:

- I dipendenti del cliente (ad esempio; IBM MQ potrebbe essere utilizzato per collegare il libro paga del cliente o i sistemi HR)
- I dati personali dei clienti del cliente (ad esempio; IBM MQ potrebbe essere utilizzato da un cliente per lo scambio di dati tra le applicazioni relative ai propri clienti, ad esempio l'acquisizione di lead di vendita e la memorizzazione di dati all'interno del proprio sistema CRM).
- I dati personali sensibili dei clienti del cliente (ad esempio; IBM MQ potrebbe essere utilizzato all'interno di contesti industriali che richiedono lo scambio di dati personali, come i record sanitari HL7-based quando si integrano le applicazioni cliniche).

Oltre ai dati dei messaggi forniti dall'applicazione, IBM MQ elabora i seguenti tipi di dati:

- Credenziali di autenticazione (come nome utente e password, chiavi API, ecc.)
- Informazioni personali tecnicamente identificabili (come ID dispositivo, identificativi basati sull'utilizzo, indirizzo IP, ecc.) - quando è collegato a un individuo)

Dati personali utilizzati per il contatto online con IBM

I clienti IBM MQ possono inoltrare commenti / feedback/richieste online per contattare IBM su IBM MQ argomenti in vari modi, principalmente:

- Area dei commenti pubblici sulle pagine nell'area IBM MQ su IBM Developer
- Area commenti pubblici sulle pagine di Informazioni sul prodotto IBM MQ in IBM Documentation
- Commenti pubblici in IBM Support Forums
- Commenti pubblici in IBM Integration Ideas

Generalmente, vengono utilizzati solo il nome del cliente e l'indirizzo email, per abilitare le risposte personali per l'oggetto del contatto e l'uso dei dati personali è conforme alla IBM Online Privacy Statement.

Raccolta dati

IBM MQ può essere utilizzato per raccogliere dati personali. Nel valutare il tuo utilizzo di IBM MQ e le tue esigenze di soddisfare le richieste del GDPR, dovresti considerare i tipi di dati personali che, nelle tue circostanze, stanno passando attraverso IBM MQ. È possibile considerare aspetti quali:

- In che modo i dati arrivano ai gestori code? (In quali protocolli? I dati sono crittografate? I dati sono firmati?)
- Come vengono inviati i dati dai gestori code? (In quali protocolli? I dati sono crittografate? I dati sono firmati?)
- Come vengono memorizzati i dati mentre passano attraverso un gestore code? (Qualsiasi applicazione di messaggistica ha il potenziale per scrivere i dati del messaggio su un supporto con stato, anche se un messaggio è non persistente. Si è consapevoli del modo in cui le funzioni di messaggistica potrebbero potenzialmente esporre aspetti dei dati dei messaggi dell'applicazione che passano attraverso il prodotto?)
- In che modo le credenziali vengono raccolte e archiviate dove necessario da IBM MQ per accedere alle applicazioni di terze parti?

IBM MQ potrebbe dover comunicare con altri sistemi e servizi che richiedono l'autenticazione, ad esempio LDAP. Dove necessario, i dati di autenticazione (ID utente, password) vengono configurati e memorizzati da IBM MQ per il loro utilizzo in tali comunicazioni. Laddove possibile, è necessario evitare di utilizzare le credenziali personali per l'autenticazione IBM MQ . Considerare la protezione della memoria utilizzata per i dati di autenticazione. (Consultare Data Storage di seguito.)

Archiviazione dati

Quando i dati del messaggio viaggiano attraverso i gestori code, IBM MQ persisterà (forse più copie di) tali dati direttamente su un supporto con stato. Gli utenti IBM MQ potrebbero considerare di proteggere i dati dei messaggi mentre sono inattivi.

I seguenti elementi evidenziano le aree in cui IBM MQ persiste i dati forniti dall'applicazione, che gli utenti possono considerare quando assicurano la conformità con il GDPR.

- Code messaggi applicazione:

  IBM MQ fornisce code di messaggi per consentire lo scambio di dati asincrono tra le applicazioni. I messaggi persistenti e non persistenti memorizzati su una coda vengono scritti su un supporto con stato.

- Code agent trasferimento file

  IBM MQ Managed File Transfer utilizza code di messaggi per coordinare il trasferimento affidabile dei dati dei file, i file che contengono dati personali e i record dei trasferimenti vengono memorizzati su queste code.

- Code di trasmissione

  Per trasferire i messaggi in modo affidabile tra gestori code, i messaggi vengono memorizzati temporaneamente nelle code di trasmissione.

- Code di messaggi non recapitabili:

  Esistono alcune circostanze in cui i messaggi non possono essere inseriti in una coda di destinazione e vengono memorizzati in una coda di messaggi non recapitabili, se tale coda è configurata sul gestore code.

- Code di backout:

  Le interfacce di messaggistica JMS e XMS forniscono una funzione che consente ai messaggi non elaborabili di essere spostati in una coda di backout dopo che si sono verificati diversi backout per consentire l'elaborazione di altri messaggi validi.

- Coda errori AMS:

  IBM MQ Advanced Message Security sposterà i messaggi non conformi a una politica di sicurezza nel SISTEMA SYSTEM.PROTECTION.ERROR.QUEUE è simile alla coda dei messaggi non instradabili.

- Pubblicazioni conservate:

  IBM MQ fornisce una funzione di pubblicazione conservata per consentire alle applicazioni di sottoscrizione di richiamare una pubblicazione precedente.

- Consegna rinviata:

  IBM MQ supporta la funzione di ritardo di consegna JMS 2.0 e Jakarta Messaging 3.0 che consente ai messaggi di essere consegnati a destinazione in un momento futuro. I messaggi che non sono stati ancora recapitati vengono memorizzati nel SISTEMA SYSTEM.DDELAY.LOCAL.QUEUE .

Ulteriori informazioni:

- Registrazione: verifica della perdita di messaggi
- Impostazioni coda agent MFT
- Utilizzo della coda di messaggi non recapitabili
- Gestione di messaggi non elaborabili nelle classi IBM MQ for JMS
- Gestione degli errori AMS
- Pubblicazioni conservate
- JMS 2.0 ritardo di consegna

I seguenti elementi evidenziano le aree in cui IBM MQ può conservare indirettamente i dati forniti dall'applicazione che gli utenti possono anche voler considerare quando assicurano la conformità con il GDPR.

- Messaggistica di instradamento traccia:

  IBM MQ fornisce funzioni di instradamento traccia, che registrano l'instradamento di un messaggio tra le applicazioni. I messaggi di evento generati possono includere informazioni personali tecnicamente identificabili come indirizzi IP.

- Traccia attività applicazione:

  IBM MQ fornisce la traccia dell'attività dell'applicazione, che registra le attività API di messaggistica di applicazioni e canali, la traccia dell'attività dell'applicazione può registrare il contenuto dei dati dei messaggi forniti dall'applicazione ai messaggi di eventi.
- Traccia servizio:

  IBM MQ fornisce funzioni di traccia del servizio, che registrano i percorsi del codice interno attraverso i quali vengono trasmessi i dati del messaggio. Come parte di queste funzioni, IBM MQ può registrare il contenuto dei dati dei messaggi forniti dall'applicazione nei file di traccia memorizzati sul disco.
- Eventi gestore code:

  IBM MQ può generare messaggi di evento che possono includere dati personali, come eventi di configurazione, comandi e autorizzazioni.

Ulteriori informazioni:

- Messaggistica di indirizzamento traccia
- Utilizzo della traccia
- Monitoraggio eventi
- Eventi di gestori code

Per proteggere l'accesso alle copie dei dati del messaggio forniti dall'applicazione, considerare le azioni riportate di seguito:

- Limitare l'accesso utente privilegiato ai dati IBM MQ nel sistema di file, ad esempio limitando l'appartenenza dell'utente al gruppo 'mqm' sulle piattaforme UNIX and Linux® .
- Limitare l'accesso dell'applicazione ai dati IBM MQ tramite code dedicate e controllo accessi. Se necessario, evitare la condivisione non necessaria delle risorse, come le code tra le applicazioni e fornire un controllo di accesso granulare alle risorse di argomenti e code.
- Limitare l'accesso alle copie replicate dei dati IBM MQ in configurazioni HA (High Availability) o DR (Disaster Recovery) e proteggere le connessioni utilizzate per la replica.
- Utilizzare IBM MQ Advanced Message Security per fornire la firma end-to-end e / o la codifica dei dati del messaggio.
- Utilizzare la crittografia a livello di file o di volume per proteggere le directory o i file system che potrebbero contenere dati, traccia o log IBM MQ .
- Una volta caricata la traccia del servizio in IBM, è possibile eliminare i file di traccia del servizio e i dati FFST se si è preoccupati del contenuto potenzialmente contenente dati personali.

Ulteriori informazioni:

- Utenti privilegiati
- Pianificazione del supporto file system su Multiplatforms
- Considerazioni sull'archiviazione per IBM MQ Operator - Crittografia
- Codifica del filesystem su IBM MQ Appliance

Un amministratore IBM MQ può configurare un gestore code con credenziali (nome utente e password, chiavi API, ecc.) per 3rd come LDAP, Salesforce, ecc. Questi dati vengono generalmente memorizzati nella directory dei dati del gestore code protetta tramite le autorizzazioni del filesystem.

Quando viene creato un gestore code IBM MQ , la directory dei dati viene impostata con il controllo accessi basato sul gruppo in modo che IBM MQ possa leggere i file di configurazione e utilizzare le credenziali per connettersi a tali sistemi. Gli amministratori IBM MQ sono considerati utenti privilegiati e sono membri di questo gruppo, quindi hanno accesso in lettura ai file. Alcuni file sono offuscati ma non sono crittografati. Per questo motivo, per proteggere completamente l'accesso alle credenziali, è necessario considerare le seguenti azioni:

- Limitare l'accesso utente privilegiato ai dati IBM MQ , ad esempio limitando l'appartenenza del gruppo 'mqm' sulle piattaforme UNIX and Linux .

- Utilizzare la codifica a livello di file o volume per proteggere il contenuto della directory dei dati del gestore code.
- Crittografare i backup della directory di configurazione di produzione e memorizzarli con i controlli di accesso appropriati.
- Considerare la possibilità di fornire tracce di controllo per errori di autenticazione, controllo degli accessi e modifiche di configurazione con eventi di sicurezza, comandi e configurazione.

Ulteriori informazioni:

- Protezione di IBM MQ

Accesso ai dati

È possibile accedere ai dati del gestore code IBM MQ tramite le seguenti interfacce del prodotto, alcune delle quali sono progettate per l'accesso tramite una connessione remota e altre per l'accesso mediante una connessione locale.

- IBM MQ Console [Solo remoto]
- API REST di gestione IBM MQ [Solo remota)
- IBM MQ Messaggistica REST API [solo remota]
- MQI [Locale e remoto]
- JMS [locale e remoto]
- XMS [Locale e Remoto]
- IBM MQ Telemetria (MQTT) [Solo remoto]
- IBM MQ Light (AMQP) [Solo remoto]
- Bridge IBM MQ IMS [Solo locale]
- Bridge IBM MQ CICS [Solo locale]
- IBM MQ MFT Protocol bridges [Solo remoto]
- IBM MQ Connect:Direct bridge [Solo remoto]
- IBM MQ Bridge per Salesforce [Solo remoto]
- IBM MQ Bridge to Blockchain [Solo remoto]
- IBM MQ MQAI [Locale e remoto]
- Comandi PCF IBM MQ [locale e remoto]
- Comandi IBM MQ MQSC [Locale e remoto]
- IBM MQ Explorer [Locale e Remoto]
- Uscite utente IBM MQ [solo locali]
- IBM MQ Internet Pass-Thru [Solo remoto]
- Metriche Red Hat® OpenShift® Monitoring (Prometheus) (le metriche sono dati numerici sulle statistiche del gestore code)
- Deprecated Removed Integrazione di IBM Cloud Pak for Integration Operations Dashboard, che inoltra dati di traccia di alto livello a un'origine centrale (soloCP4I). Si noti che questa funzione è obsoleta in IBM MQ Operator 2.3.0e rimossa in IBM MQ Operator 2.4.0.
- IBM MQ Appliance Console seriale [Solo locale]
- IBM MQ Appliance SSH [Solo remoto]
- API REST IBM MQ Appliance [Solo remota]
- IBM MQ Appliance Web UI [Solo remota]
- V 9.3.3 IBM MQ Kafka Connectors (Kafka Connect) [Locale e Remoto]

Le interfacce sono progettate per consentire agli utenti di apportare modifiche a un gestore code IBM MQ e ai messaggi memorizzati su di esso. Le operazioni di amministrazione e di messaggistica sono protette in modo che vi siano tre fasi coinvolte quando viene effettuata una richiesta;

- Autenticazione
- Associazione ruolo
- Autorizzazione

Autenticazione:

Se il messaggio o l'operazione di gestione è stata richiesta da una connessione locale, l'origine di questa connessione è un processo in esecuzione sullo stesso sistema. L'utente che esegue il processo deve aver superato tutte le fasi di autenticazione fornite dal sistema operativo. Il nome utente del proprietario del processo da cui è stata effettuata la connessione viene dichiarato come identità. Ad esempio, questo potrebbe essere il nome dell'utente che esegue la shell da cui è stata avviata un'applicazione. Le possibili forme di autenticazione per le connessioni locali sono:

1. Nome utente asserito (SO locale)
2. Nome utente e password facoltativi (OS, LDAP o repository 3rd parti personalizzati)
3. Solo JWT (Security Token) IBM MQ e solo da IBM MQ 9.3.4

Se l'azione di gestione è stata richiesta da una connessione remota, le comunicazioni con IBM MQ vengono effettuate tramite un'interfaccia di rete. Le seguenti forme di identità possono essere presentate per l'autenticazione tramite connessioni di rete;

1. Nome utente asserito (dal sistema operativo remoto)
2. Nome utente e password (SO, LDAP o repository 3rd parti personalizzati)
3. Indirizzo di rete di origine (come l'indirizzo IP)
4. X.509 Certificato digitale (autenticazione SSL/TLS reciproca)
5. Token di sicurezza (come LTPA2 o token JWT)
6. Altra sicurezza personalizzata (funzionalità fornita dalle uscite di 3rd parti)
7. Chiavi SSH

L'integrazione di IBM MQcon IBM Cloud Pak for Integration aggiunge un nuovo tipo di autenticazione per il IBM MQ Console: Single Sign - On con il Cloud Pak. (soloCP4I)

Associazione ruoli:

Nella fase di associazione dei ruoli, le credenziali fornite nella fase di autenticazione possono essere associate a un identificativo utente alternativo. A condizione che l'identificativo utente associato sia autorizzato a procedere (ad esempio, gli utenti amministrativi possono essere bloccati dalle regole di autenticazione del canale), l'ID utente associato viene portato avanti nella fase finale quando si autorizzano le attività rispetto alle risorse IBM MQ .

Autorizzazione:

IBM MQ consente a utenti differenti di disporre di autorizzazioni differenti per le diverse risorse di messaggistica, come code, argomenti e altri oggetti gestore code.

Registrazione attività:

Alcuni utenti di IBM MQ potrebbero dover creare un record di controllo dell'accesso alle risorse MQ . Esempi di log di controllo desiderati potrebbero includere modifiche alla configurazione che contengono informazioni sulla modifica oltre a chi l'ha richiesto.

Le seguenti fonti di informazioni sono disponibili per implementare questo requisito:

1. Un gestore code IBM MQ può essere configurato per produrre eventi di comando quando un comando di gestione è stato eseguito correttamente.
2. Un gestore code IBM MQ può essere configurato per produrre eventi di configurazione quando una risorsa del gestore code viene creata, modificata o eliminata.

3. Un gestore code IBM MQ può essere configurato per produrre un evento di autorizzazione quando un controllo di autorizzazione non riesce per una risorsa.
4. Messaggi di errore che indicano che i controlli di autorizzazione non riusciti vengono scritti nei log degli errori del gestore code.
5. La console IBM MQ scriverà i messaggi di controllo nei relativi log quando l'autenticazione, i controlli di autorizzazione hanno esito negativo o quando i gestori code vengono creati, avviati, arrestati o eliminati.
6. IBM MQ Appliance scriverà i messaggi di controllo nei propri log per registrare i login utente e le modifiche di sistema.

Quando si considera questo tipo di soluzioni, gli utenti di IBM MQ potrebbero voler considerare i seguenti punti:

- I messaggi di eventi non sono persistenti, quindi quando un gestore code viene riavviato le informazioni vengono perse. I monitor di eventi devono essere configurati per consumare costantemente i messaggi disponibili e trasferire il contenuto ai supporti persistenti.
- Gli utenti con privilegi IBM MQ dispongono di privilegi sufficienti per disabilitare gli eventi, cancellare i log o eliminare i gestori code.

Per ulteriori informazioni sulla sicurezza dell'accesso ai dati IBM MQ e sulla fornitura di una traccia di controllo, fare riferimento ai seguenti argomenti:

- IBM MQ meccanismi di sicurezza
- Eventi di configurazione
- Eventi di comandi
- Utilizzo dei log degli errori

Elaborazione dati

Codifica mediante un'infrastruttura di chiavi pubbliche:

È possibile proteggere le connessioni di rete a IBM MQ specificando che le connessioni utilizzano TLS, che può anche fornire l'autenticazione reciproca del lato iniziale della connessione.

L'utilizzo delle funzioni di sicurezza PKI fornite dai meccanismi di trasporto è il primo passo per proteggere l'elaborazione dei dati con IBM MQ. Tuttavia, senza abilitare ulteriori funzioni di sicurezza, il comportamento di un'applicazione di consumo è quello di elaborare tutti i messaggi consegnati ad essa senza convalidare l'origine del messaggio o se è stato modificato durante il transito.

Gli utenti di IBM MQ che dispongono della licenza per utilizzare le funzionalità Advanced Message Security (AMS) possono controllare il modo in cui le applicazioni elaborano i dati personali contenuti nei messaggi, mediante la definizione e configurazione delle politiche di sicurezza. Le politiche di sicurezza consentono di applicare la firma digitale e / o la codifica ai dati dei messaggi tra le applicazioni.

È possibile utilizzare le politiche di sicurezza per richiedere e convalidare una firma digitale quando si utilizzano messaggi per garantire che i messaggi siano autentici. La crittografia AMS fornisce un metodo con cui i dati del messaggio vengono convertiti da un formato leggibile a una versione codificata che può essere decodificata solo da un'altra applicazione se è il destinatario previsto o il messaggio e ha accesso alla chiave di decrittografia corretta.

Per ulteriori informazioni sull'utilizzo di SSL e dei certificati per proteggere le connessioni di rete, fare riferimento ai seguenti argomenti nella documentazione del prodotto IBM MQ :

- Configurazione della sicurezza TLS per IBM MQ
- Panoramica AMS

Eliminazione dei dati

IBM MQ fornisce comandi e azioni dell'interfaccia utente per eliminare i dati forniti al prodotto. Ciò significa che gli utenti di IBM MQ possono eliminare i dati relativi a particolari individui, se necessario.

- Aree di comportamento IBM MQ da considerare per la conformità con l'eliminazione dei dati del client GDPR
  - Eliminare i dati del messaggio memorizzati su una coda dell'applicazione:
    - Rimozione di singoli messaggi utilizzando l'API di messaggistica o gli strumenti o utilizzando la scadenza del messaggio.
    - Specificando che i messaggi sono non persistenti, conservati su una coda in cui la classe di messaggi non persistenti è normale e riavviando il gestore code.
    - Cancellare amministrativamente la coda.
    - Eliminazione della coda.
  - Eliminare i dati di pubblicazione conservati memorizzati su un argomento da:
    - Specificare che i messaggi sono non persistenti e riavviare il gestore code.
    - Sostituzione dei dati conservati con nuovi dati o utilizzando la scadenza del messaggio.
    - Cancellare amministrativamente la stringa di argomenti.
  - Eliminare i dati memorizzati su un gestore code eliminando l'intero gestore code e tutte le copie replicate per l'alta disponibilità o il ripristino di emergenza.
  - Eliminare i dati memorizzati dai comandi di traccia del servizio eliminando i file nella directory di traccia.
  - Eliminare i dati FFST memorizzati eliminando i file nella directory degli errori.
  - Eliminare lo spazio di indirizzi e i dump della CF (Coupling Facility) (su z/OS).
  - Eliminare l'archivio, il backup o altre copie di tali dati.
- Aree di comportamento IBM MQ da considerare per la conformità con l'eliminazione dei dati dell'account GDPR
  - È possibile eliminare i dati di account e le preferenze memorizzate da IBM MQ per la connessione ai gestori code e ai servizi di 3rd eliminando (incluse le copie di archivio, di backup o in altro modo replicate):
    - Oggetti delle informazioni di autenticazione del gestore code che memorizzano credenziali.
    - Record di autorizzazione del gestore code che fanno riferimento agli identificatori utente.
    - Regole di autenticazione del canale del gestore code che associano o bloccano indirizzi IP specifici, DN certificato o identificatori utente.
    - File di credenziali utilizzati da IBM MQ Managed File Transfer Agent, Logger e MQ Explorer MFT Plugin per l'autenticazione con il gestore code e i file server.
    - I certificati digitali X.509 che rappresentano o contengono informazioni su un individuo dai keystore che possono essere utilizzati dalle connessioni SSL/TLS o IBM MQ Advanced Message Security (AMS).
    - Singoli account utente da IBM MQ Appliance, incluso il riferimento a tali account nei file di log del sistema.
    - Metadati dello spazio di lavoro IBM MQ Explorer e impostazioni Eclipse .
    - IBM MQ Explorer come specificato in Preferenze password.
    - IBM MQ Console e file di configurazione del server mqweb.
    - File di configurazione dei dati di connessione Salesforce .
    - File di configurazione dei dati di connessione Blockchain .
    - File di configurazione e keystore IBM MQ Internet Pass-Thru .

Ulteriori informazioni:

- Configurazione di IBM MQ Bridge to Salesforce
- Configurazione di IBM MQ per l'utilizzo con blockchain
- MFT e IBM MQ autenticazione della connessione

- Mappare le credenziali per un file server utilizzando il file ProtocolBridgeCredentials.xml
- Configurazione di utenti e ruoli IBM MQ Console

Monitoraggio dei dati

IBM MQ fornisce una serie di funzioni di controllo che gli utenti possono utilizzare per comprendere meglio le prestazioni delle applicazioni e dei gestori code.

IBM MQ fornisce inoltre una serie di funzioni che consentono di gestire i log degli errori del gestore code.

Ulteriori informazioni:

- Monitoraggio della rete IBM MQ
- Servizi di messaggi diagnostici
- Servizio QMErrorLog
- Monitoraggio quando si utilizza l'operatore IBM MQ
- IBM MQ Appliance monitoraggio e reporting

Capacità di limitare l'uso dei dati personali

Utilizzando le funzioni riepiloga in questo documento, IBM MQ consente all'utente finale di limitare l'utilizzo dei propri dati personali.

Le code di messaggi IBM MQ non devono essere utilizzate come archivio dati permanente allo stesso modo di un database, il che è particolarmente vero quando si gestiscono i dati dell'applicazione soggetti al GDPR.

A differenza di un database in cui i dati possono essere trovati attraverso una query di ricerca, può essere difficile trovare i dati del messaggio a meno che non si conosca la coda, il messaggio e gli identificatori di correlazione di un messaggio.

I messaggi contenenti i dati di un individuo possono essere prontamente identificati e localizzati, è possibile utilizzare le funzioni di messaggistica IBM MQ standard per accedere o modificare i dati del messaggio.

Gestione file

1. IBM MQ Managed File Transfer non esegue la scansione del malware sui file trasferiti. I file vengono trasferiti così come sono e viene eseguito un controllo di integrità per garantire che i dati file non vengano modificati durante il trasferimento. I checksum di origine e di destinazione vengono pubblicati come parte della pubblicazione dello stato di trasferimento. Si consiglia agli utenti finali di implementare la scansione del malware come appropriato per il loro ambiente prima che MFT trasferisca il file e dopo che MFT distribuisca un file a un endpoint remoto.
2. IBM MQ Managed File Transfer non esegue azioni in base al tipo MIME o all'estensione file. MFT legge i file e trasferisce i byte esattamente come letti dal file di input.

Architetture basate su un singolo gestore code

Le architetture IBM MQ più semplici implicano la configurazione e l'utilizzo di un singolo gestore code.

Prima di pianificare la propria architettura IBM MQ , acquisire familiarità con i concetti di IBM MQ di base. Vedere IBM MQ Panoramica tecnica.

Nelle seguenti sezioni sono descritte diverse possibili architetture che utilizzano un singolo gestore code:

- “Singolo gestore code con applicazioni locali che accedono a un servizio” a pagina 19
- “Singolo gestore code con applicazioni remote che accedono a un servizio come client” a pagina 19
- “Singolo gestore code con una configurazione di pubblicazione / sottoscrizione” a pagina 19

Singolo gestore code con applicazioni locali che accedono a un servizio

La prima architettura basata su un singolo gestore code è quella in cui le applicazioni che accedono a un servizio sono in esecuzione sullo stesso sistema delle applicazioni che forniscono il servizio. Un gestore code IBM MQ fornisce l'intercomunicazione asincrona tra le applicazioni che richiedono il servizio e quelle che forniscono il servizio. Ciò significa che la comunicazione tra le applicazioni può continuare anche se una delle applicazioni è offline per un lungo periodo di tempo.

Singolo gestore code con applicazioni remote che accedono a un servizio come client

La seconda architettura basata su un singolo gestore code ha le applicazioni in esecuzione in remoto dalle applicazioni che forniscono il servizio. Le applicazioni remote sono in esecuzione su sistemi differenti per i servizi. Le applicazioni si connettono come client al singolo gestore code. Questo significa che l'accesso a un servizio può essere fornito a più sistemi tramite un singolo gestore code.

Una limitazione di questa architettura è che una connessione di rete deve essere disponibile per il funzionamento di un'applicazione. L'interazione tra l'applicazione e il gestore code sulla connessione di rete è sincrona.

Singolo gestore code con una configurazione di pubblicazione / sottoscrizione

Un'architettura alternativa che utilizza un singolo gestore code è quella di utilizzare una configurazione di pubblicazione / sottoscrizione. Nella messaggistica di pubblicazione / sottoscrizione, è possibile disaccoppiare il provider di informazioni dai consumatori di tali informazioni. Ciò differisce dagli stili di messaggistica punto a punto nelle architetture precedentemente descritte, in cui le applicazioni devono conoscere le informazioni sull'applicazione di destinazione, ad esempio il nome della coda su cui inserire i messaggi. Utilizzando la pubblicazione / sottoscrizione IBM MQ , l'applicazione di invio pubblica un messaggio con un argomento specificato in base all'oggetto delle informazioni. IBM MQ gestisce la distribuzione del messaggio alle applicazioni che hanno registrato un interesse in tale soggetto tramite una sottoscrizione. Inoltre, le applicazioni riceventi non hanno bisogno di conoscere l'origine dei messaggi per riceverli. Per ulteriori informazioni, consultare Messaggistica di pubblicazione / sottoscrizione e Esempio di una singola configurazione di pubblicazione / sottoscrizione del gestore code.

Concetti correlati

Introduzione a IBM MQ

Attività correlate

“Pianificazione di un'architettura IBM MQ” a pagina 5
Quando si pianifica l'ambiente IBM MQ , considerare il supporto fornito da IBM MQ per le architetture di gestori code singoli e multipli e per gli stili di messaggistica point-to-point e di pubblicazione / sottoscrizione. Inoltre, pianificare i requisiti delle risorse e l'utilizzo delle funzioni di registrazione e backup.

Creazione e gestione di gestori code su più piattaforme

Architetture basate su più gestori code

È possibile utilizzare le tecniche di accodamento dei messaggi distribuiti per creare un'architettura IBM MQ che implica la configurazione e l'utilizzo di più gestori code.

Prima di pianificare la propria architettura IBM MQ , acquisire familiarità con i concetti di IBM MQ di base. Vedere IBM MQ Panoramica tecnica.

Un'architettura IBM MQ può essere modificata, senza alcuna modifica alle applicazioni che forniscono servizi, aggiungendo ulteriori gestori code.

Le applicazioni possono essere ospitate sulla stessa macchina di un gestore code e quindi ottenere una comunicazione asincrona con un servizio ospitato su un altro gestore code su un altro sistema. In alternativa, le applicazioni che accedono a un servizio possono connettersi come client a un gestore code che fornisce l'accesso asincrono al servizio su un altro gestore code.

Gli instradamenti che connettono gestori code differenti e le relative code vengono definiti utilizzando tecniche di accodamento distribuito. I gestori code nell'architettura sono connessi utilizzando i canali. I canali vengono utilizzati per spostare automaticamente i messaggi da un gestore code a un altro in una direzione a seconda della configurazione dei gestori code.

Per una panoramica di alto livello della pianificazione di una rete IBM MQ , consultare “Progettazione di reti di gestori code distribuiti” a pagina 21.

Per informazioni su come pianificare i canali per la tua architettura IBM MQ , vedi Tecniche di accodamento distribuito IBM MQ.

La gestione delle code distribuite consente di creare e monitorare la comunicazione tra gestori code. Per ulteriori informazioni sulla gestione delle code distribuite, consultare Introduzione alla gestione delle code distribuite.

Attività correlate

“Pianificazione di un'architettura IBM MQ” a pagina 5
Quando si pianifica l'ambiente IBM MQ , considerare il supporto fornito da IBM MQ per le architetture di gestori code singoli e multipli e per gli stili di messaggistica point-to-point e di pubblicazione / sottoscrizione. Inoltre, pianificare i requisiti delle risorse e l'utilizzo delle funzioni di registrazione e backup.

Creazione e gestione di gestori code su più piattaforme

Pianificazione delle code e dei cluster distribuiti

È possibile connettere manualmente le code che si trovano sui gestori code distribuiti oppure è possibile creare un cluster di gestori code e consentire al prodotto di connettere i gestori code. Per scegliere una topologia adatta per la rete di messaggistica distribuita, è necessario considerare i requisiti per il controllo manuale, la dimensione della rete, la frequenza di modifica, la disponibilità e la scalabilità.

Prima di iniziare

Questa attività presuppone che l'utente comprenda quali sono le reti di messaggistica distribuite e come funzionano. Per una panoramica tecnica, consultare Accodamento distribuito e cluster.

Informazioni su questa attività

Per creare una rete di messaggistica distribuita, è possibile configurare manualmente i canali per connettere le code ospitate su diversi gestori code oppure è possibile creare un cluster di gestori code. Il clustering consente ai gestori code di comunicare tra loro senza la necessità di impostare definizioni di canali supplementari o definizioni di code remote, semplificandone la configurazione e la gestione.

Per scegliere una topologia adatta per la propria rete di pubblicazione / sottoscrizione distribuita, è necessario considerare le seguenti domande generali:

- Di quale controllo manuale hai bisogno per le connessioni nella tua rete?
- Quanto sarà grande la tua rete?
- Quanto sarà dinamico?
- Quali sono i requisiti di disponibilità e scalabilità?

Procedura

- Considerare quanto controllo manuale è necessario sulle connessioni nella rete.

  Se sono necessarie solo poche connessioni o se le singole connessioni devono essere definite in modo molto preciso, è necessario creare la rete manualmente.

  Se sono necessari più gestori code che sono logicamente correlati e che devono condividere dati e applicazioni, è consigliabile raggrupparli insieme in un cluster di gestori code.
- Stimare la dimensione della rete.

a) Stimare quanti gestori code sono necessari. Tenere presente che le code possono essere ospitate su più di un gestore code.

b) Se si sta considerando l'utilizzo di un cluster, aggiungere due ulteriori gestori code che fungano da repository completi.

Per reti più grandi, la configurazione manuale e la manutenzione delle connessioni possono richiedere molto tempo e si consiglia di utilizzare un cluster.

- Considerare la dinamica dell'attività di rete.

  Pianificare le code occupate da ospitare sui gestori code con prestazioni.

  Se si prevede che le code vengano create ed eliminate di frequente, considerare l'uso di un cluster.
- Considera i tuoi requisiti di disponibilità e scalabilità.

  a) Decidere se è necessario garantire l'alta disponibilità dei gestori code. In tal caso, stimare il numero di gestori code a cui si applica questo requisito.

  b) Considerare se alcuni dei gestori code sono meno capaci di altri.

  c) Considerare se i collegamenti di comunicazione ad alcuni dei gestori code sono più fragili rispetto ad altri.

  d) Considerare la possibilità di ospitare code su più gestori code.

  Le reti e i cluster configurati manualmente possono essere entrambi configurati per essere altamente disponibili e scalabili. Se si utilizza un cluster, è necessario definire due ulteriori gestori code come repository completi. Disporre di due repository completi garantisce che il cluster continui a funzionare se uno dei repository completi diventa non disponibile. Assicurarsi che i gestori code del repository completo siano solidi, performanti e abbiano una buona connettività di rete. Non pianificare l'utilizzo dei gestori code del repository completo per qualsiasi altro lavoro.
- In base a questi calcoli, utilizzare i link forniti per decidere se configurare manualmente le connessioni tra i gestori code o utilizzare un cluster.

Operazioni successive

È ora possibile configurare la rete di messaggistica distribuita.

Attività correlate

Configurazione dell'accodamento distribuito

Configurazione di un cluster di gestore code

Progettazione di reti di gestori code distribuiti

IBM MQ invia e riceve i dati tra le applicazioni e sulle reti utilizzando gestori code e canali. La pianificazione della rete implica la definizione dei requisiti per creare un framework per la connessione di questi sistemi su una rete.

I canali possono essere creati tra il sistema e qualsiasi altro sistema con cui è necessario disporre di comunicazioni. È possibile creare canali multi - hop per connettersi a sistemi in cui non si dispone di connessioni dirette. Le connessioni del canale dei messaggi descritte negli scenari vengono mostrati come diagramma di rete in Figura 1 a pagina 22.

Se è necessario creare canali tra sistemi su reti fisiche differenti o canali che comunicano attraverso un firewall, l'utilizzo di IBM MQ Internet Pass-Thru potrebbe semplificare la configurazione. Per ulteriori informazioni, consultare IBM MQ Internet Pass-Thru.

Nomi di canali e code di trasmissione

È possibile assegnare qualsiasi nome alle code di trasmissione. Ma per evitare confusione, è possibile assegnare loro gli stessi nomi dei nomi dei gestori code di destinazione o dei nomi degli alias dei gestori code, a seconda dei casi. Ciò associa la coda di trasmissione all'instradamento che utilizzano, fornendo una chiara panoramica degli instradamenti paralleli creati tramite gestori code intermedi (con più passaggi).

Non è così chiaro per i nomi dei canali. I nomi dei canali in Figura 1 a pagina 22 per QM2, ad esempio, devono essere diversi per i canali in entrata e in uscita. Tutti i nomi canale possono ancora contenere i propri nomi di coda di trasmissione, ma devono essere qualificati per renderli univoci.

Ad esempio, in QM2, esiste un canale QM3 proveniente da QM1e un canale QM3 che passa a QM3. Per rendere univoci i nomi, il primo potrebbe essere denominato QM3_from_QM1e il secondo potrebbe essere denominato QM3_from_QM2. In questo modo, i nomi dei canali mostrano il nome della coda di trasmissione nella prima parte del nome. La direzione e il nome del gestore code adiacente vengono mostrati nella seconda parte del nome.

Una tabella di nomi di canali suggeriti per Figura 1 a pagina 22 viene fornita in Tabella 1 a pagina 22.

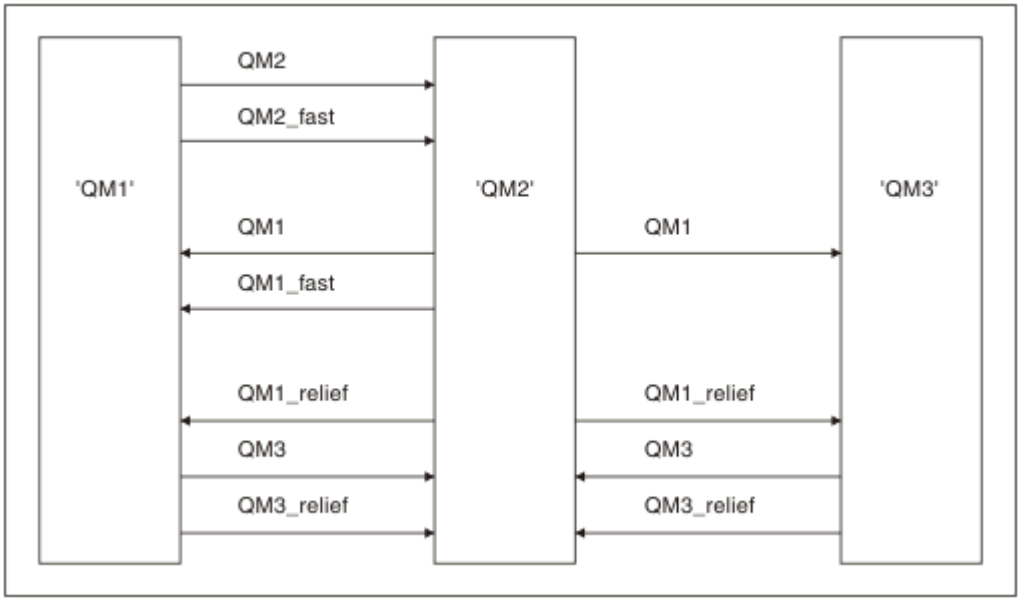


Figura 1. Diagramma di rete che mostra tutti i canali

Tabella 1. Esempio di nomi di canali

Nome instradamento	**Gestori code che ospitano il canale**	**Nome coda di trasmissione**	**Nome canale suggerito**
QM1	QM1 & QM2	QM1 (in QM2)	QM1.from.QM2
QM1	QM2 & QM3	QM1 (in QM3)	QM1.from.QM3
QM1_fast	QM1 & QM2	QM1_fast (in QM2)	QM1_fast.from.QM2
QM1_relief	QM1 & QM2	QM1_relief (alle QM2)	QM1_relief.from.QM2
QM1_relief	QM2 & QM3	QM1_relief (in QM3)	QM1_relief.from.QM3
QM2	QM1 & QM2	QM2 (in QM1)	QM2.from.QM1
QM2_fast	QM1 & QM2	QM2_fast (all'indirizzo QM1)	QM2_fast.from.QM1
QM3	QM1 & QM2	QM3 (in QM1)	QM3.from.QM1
QM3	QM2 & QM3	QM3 (in QM2)	QM3.from.QM2
QM3_relief	QM1 & QM2	QM3_relief (in QM1)	QM3_relief.from.QM1
QM3_relief	QM2 & QM3	QM3_relief (in QM2)	QM3_relief.from.QM2

Nota:

1. z/OS Su IBM MQ for z/OS, i nomi dei gestori code sono limitati a quattro caratteri.
2. Denominare in modo univoco tutti i canali nella rete. Come mostrato nella sezione Tabella 1 a pagina 22, includere i nomi dei gestori code di origine e di destinazione nel nome del canale è un buon modo per farlo.

Pianificatore di rete

La creazione di una rete presuppone l'esistenza di un'altra funzione di livello superiore di *pianificatore di rete* i cui piani sono implementati dagli altri membri del team.

Per le applicazioni ampiamente utilizzate, è più economico pensare in termini di siti di accesso locale per la concentrazione del traffico dei messaggi, utilizzando i collegamenti a banda larga tra i siti di accesso locale, come mostrato in Figura 2 a pagina 24.

In questo esempio ci sono due sistemi principali e un certo numero di sistemi satellitari. La configurazione effettiva dipende da considerazioni di business. Ci sono due gestori code concentratori situati in centri convenienti. Ogni concentratore QM dispone di canali di messaggi per i gestori code locali:

- QM - concentrator 1 dispone di canali di messaggi per ciascuno dei tre gestori code locali, QM1, QM2e QM3. Le applicazioni che utilizzano questi gestori code possono comunicare tra loro tramite i concentratori QM.
- QM - concentrator 2 dispone di canali di messaggi per ognuno dei tre gestori code locali, QM4, QM5e QM6. Le applicazioni che utilizzano questi gestori code possono comunicare tra loro tramite i concentratori QM.
- I concentratori QM hanno canali di messaggi tra loro, consentendo così a qualsiasi applicazione in un gestore code di scambiare messaggi con qualsiasi altra applicazione in un altro gestore code.

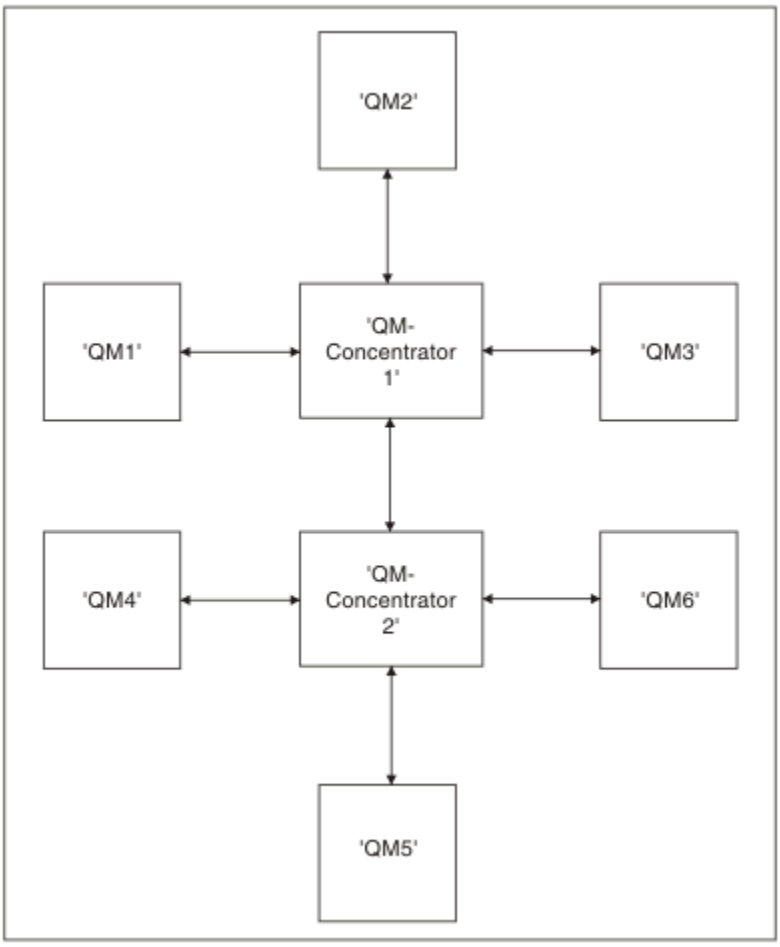


Figura 2. Diagramma di rete che mostra i concentratori QM

Progettazione di cluster

I cluster forniscono un meccanismo per l'interconnessione dei gestori code in modo da semplificare sia la configurazione iniziale che la gestione in corso. I cluster devono essere attentamente progettati per garantire che funzionino correttamente e che raggiungano i livelli richiesti di disponibilità e reattività.

Prima di iniziare

Per un'introduzione ai concetti di clustering, consultare i seguenti argomenti:

- Accodamento distribuito e cluster
- “Confronto tra cluster e accodamento distribuito” a pagina 31
- Componenti di un cluster

Quando si progetta il cluster del gestore code, è necessario prendere alcune decisioni. È necessario prima decidere quali gestori code nel cluster devono contenere i repository completi delle informazioni cluster. Qualsiasi gestore code creato può essere utilizzato in un cluster. È possibile scegliere un qualsiasi numero di gestori code per questo scopo, ma il numero ideale è due. Per informazioni sulla selezione dei gestori code per contenere i repository completi, consultare “Come scegliere i gestori code del cluster per conservare i repository completi” a pagina 33.

Per ulteriori informazioni sulla progettazione del cluster, consultare i seguenti argomenti:

- “Cluster di esempio” a pagina 40
- “Organizzazione di un cluster” a pagina 35
- “Convenzioni di denominazione cluster” a pagina 35

- z/OS “Cluster e gruppi di condivisione code” a pagina 36
- “Cluster sovrapposti” a pagina 37

Operazioni successive

Consultare i seguenti argomenti per ulteriori informazioni sulla configurazione e l'utilizzo dei cluster:

- Come stabilire la comunicazione in un cluster
- Configurazione di un cluster di gestori code
- Instradamento dei messaggi verso e dai cluster
- Utilizzo dei cluster per la gestione del workload

Per ulteriori informazioni che ti aiutano a configurare il tuo cluster, vedi“Suggerimenti per il clustering” a pagina 38.

Pianificazione della modalità di utilizzo di più code di trasmissione cluster

È possibile definire esplicitamente le code di trasmissione o fare in modo che il sistema crei le code di trasmissione. Se si definiscono le code di trasmissione, si ha un maggiore controllo sulle definizioni delle code. z/OS Su z/OS, si ha anche un maggiore controllo sulla serie di pagine in cui sono contenuti i messaggi.

Definizione delle code di trasmissione

Esistono due metodi per definire le code di trasmissione:

- Automaticamente, utilizzando l'attributo DEFCLXQ del gestore code, come segue:

  ```
  ALTER QMGR DEFCLXQ(SCTQ | CHANNEL)
  ```

  DEFCLXQ (SCTQ) indica che la coda di trasmissione predefinita per tutti i canali mittente del cluster è SYSTEM.CLUSTER.TRANSMIT.QUEUE. Questo è il valore predefinito.

  DEFCLXQ (CHANNEL) indica che per impostazione predefinita ogni canale mittente del cluster utilizza una coda di trasmissione separata denominata SYSTEM.CLUSTER.TRANSMIT.*nome canale*. Ogni coda di trasmissione viene definita automaticamente dal gestore code. Per ulteriori informazioni, consultare “Code di trasmissione cluster definite automaticamente” a pagina 26.
- Manualmente, definendo una coda di trasmissione con un valore specificato per l'attributo CLCHNAME. L'attributo CLCHNAME indica quali canali mittente del cluster devono utilizzare la coda di trasmissione.

  z/OS Se si sta definendo manualmente una coda di trasmissione su z/OS, consultare “Pianificazione di code di trasmissione cluster definite manualmente” a pagina 28 per ulteriori informazioni.

Di quale sicurezza ho bisogno?

Per avviare uno switch, automaticamente o manualmente, è necessaria l'autorità per avviare un canale.

Per definire la coda utilizzata come coda di trasmissione, è necessaria l'autorizzazione IBM MQ standard per definire la coda.

Quando è il momento adatto per implementare la modifica?

Quando si modifica la coda di trasmissione utilizzata dai canali mittente del cluster, è necessario assegnare un tempo in cui effettuare l'aggiornamento, considerando i seguenti punti:

- Il tempo richiesto per un canale per commutare la coda di trasmissione dipende dal numero totale di messaggi sulla vecchia coda di trasmissione, dal numero di messaggi da spostare e dalla dimensione dei messaggi.

- Le applicazioni possono continuare a inserire i messaggi nella coda di trasmissione mentre si verifica la modifica. Ciò potrebbe portare ad un aumento del tempo di transizione.
- È possibile modificare il parametro CLCHNAME di qualsiasi coda di trasmissione o DEFCLXQ in qualsiasi momento, preferibilmente quando il carico di lavoro è basso.

  Si noti che nulla accade immediatamente.
- Le modifiche si verificano solo quando un canale viene avviato o riavviato. Quando un canale viene avviato, controlla la configurazione corrente e, se necessario, passa a una nuova coda di trasmissione.
- Esistono diverse modifiche che potrebbero modificare l'associazione di un canale mittente del cluster con una coda di trasmissione:
  - Modifica del valore dell'attributo CLCHNAME di una coda di trasmissione, rendendo CLCHNAME meno specifico o vuoto.
  - Modifica del valore dell'attributo CLCHNAME di una coda di trasmissione, rendendo CLCHNAME più specifico.
  - Eliminazione di una coda con CLCHNAME specificato.
  - Modifica dell'attributo del gestore code DEFCLXQ.

Quanto tempo ci vorrà per l'interruttore?

Durante il periodo di transizione, tutti i messaggi per il canale vengono spostati da una coda di trasmissione ad un'altra. Il tempo richiesto per un canale per commutare la coda di trasmissione dipende dal numero totale di messaggi sulla vecchia coda di trasmissione e dal numero di messaggi che devono essere spostati.

Per le code contenenti alcune migliaia di messaggi, lo spostamento dei messaggi dovrebbe richiedere meno di un secondo. Il tempo effettivo dipende dal numero e dalla dimensione dei messaggi. Il gestore code deve essere in grado di spostare i messaggi a molti megabyte al secondo.

Le applicazioni possono continuare a inserire i messaggi nella coda di trasmissione mentre si verifica la modifica. Ciò potrebbe portare ad un aumento del tempo di transizione.

Ogni canale mittente del cluster interessato deve essere riavviato per rendere effettiva la modifica. Pertanto, si consiglia di modificare la configurazione della coda di trasmissione quando il gestore code non è occupato e pochi messaggi sono memorizzati nelle code di trasmissione del cluster.

runswchl , comando z/OS o comando SWITCH CHANNEL (*) STATUS in CSQUTIL su z/OS, può essere utilizzato per interrogare lo stato dei canali mittenti del cluster e quali modifiche in sospeso sono in sospeso per la configurazione della coda di trasmissione.

Come implementare il cambiamento

Consultare Implementazione del sistema utilizzando più code di trasmissione cluster per dettagli su come apportare la modifica a più code di trasmissione cluster, automaticamente o manualmente.

Annullamento della modifica

z/OS

Consultare Annullamento di una modifica ad una coda di trasmissione su z/OS per i dettagli su come eseguire il backout delle modifiche in caso di problemi.

Code di trasmissione cluster definite automaticamente
È possibile che il sistema generi le code di trasmissione per conto dell'utente.

Prima di iniziare

z/OS Per impostare manualmente le code di trasmissione cluster su z/OS, consultare “Pianificazione di code di trasmissione cluster definite manualmente” a pagina 28.

Informazioni su questa attività

Se un canale non dispone di una coda di trasmissione del cluster definita manualmente associata e si specifica DEFCLXQ (CHANNEL), quando il canale avvia il gestore code definisce automaticamente una coda dinamica permanente per il canale mittente del cluster. Modello coda SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE viene utilizzato per definire automaticamente la coda di trasmissione del cluster dinamico permanente con il nome SYSTEM.CLUSTER.TRANSMIT.`ChannelName`.

Importante: z/OS

Se il gestore code viene migrato a IBM MQ 8.0, il gestore code non dispone di SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE.

Definire prima questa coda, in modo che il comando ALTER QGMR DEFCLXQ (CHANNEL) abbia effetto.

Il seguente JCL è un esempio di codice che è possibile utilizzare per definire la coda modello:

```
//CLUSMODL JOB MSGCLASS=H,NOTIFY=&SYSUID
/*JOBPARM SYSAFF=(MVCC)
//MQCMD EXEC PGM=CSQUTIL,REGION=4096K,PARM='CDLK'
//STEPLIB DD DISP=SHR,DSN=SCEN.MQ.V000.COM.BASE.SCSQAUTH
// DD DISP=SHR,DSN=SCEN.MQ.V000.COM.BASE.SCSQANLE
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND DDNAME(CMDINP)
/*
//CMDINP DD *
DEFINE QMODEL( 'SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE' ) +
QSGDISP( QMGR ) +

* COMMON QUEUE ATTRIBUTES
DESCR( 'SYSTEM CLUSTERING TRANSMISSION MODEL QUEUE' ) +
PUT( ENABLED ) +
DEFPRTY( 5 ) +
DEFPSIST( YES ) +

* MODEL QUEUE ATTRIBUTES
DEFTYPE( PERMDYN ) +

* LOCAL QUEUE ATTRIBUTES
GET( ENABLED ) +
SHARE +
DEFSOPT( EXCL ) +
MSGDLVSQ( PRIORITY ) +
RETINTVL( 999999999 ) +
MAXDEPTH( 999999999 ) +
MAXMSGL( 4194304 ) +
NOHARDENBO +
BOTHRESH( 0 ) +
BOQNAME( ' ' ) +
STGCLASS( 'REMOTE' ) +
USAGE( XMITQ ) +
INDXTYPE( CORRELID ) +
CFSTRUCT( ' ' ) +
MONQ( OFF ) ACCTQ( OFF ) +

* EVENT CONTROL ATTRIBUTES
QDPMAXEV( ENABLED ) +
QDPHIEV( DISABLED ) +
QDEPTHHI( 80 ) +
QDPLOEV( DISABLED ) +
QDEPTHLO( 40 ) +
QSVCIEV( NONE ) +
QSVCINT( 999999999 ) +

* TRIGGER ATTRIBUTES
TRIGGER +
TRIGTYPE( FIRST ) +
TRIGMPRI( 0 ) +
TRIGDPTH( 1 ) +
TRIGDATA( ' ' ) +
PROCESS( ' ' ) +
INITQ( ' ' )
/*
```

Procedura

1. Utilizzare l'attributo del gestore code *DEFCLXQ* .

   Per ulteriori informazioni su questo attributo, consultare ALTER QMGR.

   Ci sono due opzioni:

   Ctcs
   Questa opzione è quella predefinita e indica che si utilizza il singolo SYSTEM.CLUSTER.TRANSMIT.QUEUE.

CHANNEL
Indica che si utilizzano più code di trasmissione cluster.

2. Per passare alla nuova associazione:
   - Arrestare e riavviare il canale.
   - Il canale utilizza la nuova definizione della coda di trasmissione.
   - I messaggi vengono trasferiti da un processo di commutazione di transizione dalla vecchia coda alla nuova coda di trasmissione.

   Tenere presente che tutti i messaggi dell'applicazione vengono inseriti nella vecchia definizione.

   Quando il numero di messaggi nella vecchia coda raggiunge lo zero, i nuovi messaggi vengono inseriti direttamente nella nuova coda di trasmissione.
3. Per controllare quando termina il processo di commutazione:
   a) Uno switch della coda di trasmissione avviato da un canale viene eseguito in background e l'amministratore può monitorare il log dei lavori del gestore code per determinare quando è stato completato.
   b) Monitorare i messaggi nella registrazione lavoro per visualizzare l'avanzamento dello switch.
   c) Per assicurarsi che solo i canali desiderati stiano utilizzando questa coda di trasmissione, immettere il comando DIS CLUSQMGR (*) dove, ad esempio, la proprietà della coda di trasmissione che definisce la coda di trasmissione è `APPQMGR.CLUSTER1.XMITQ`.
   d) z/OS
   Utilizzare il comando SWITCH CHANNEL (*) STATUS in CSQUTIL.

   Questa opzione indica quali modifiche in sospeso sono in sospeso e quanti messaggi devono essere spostati tra le code di trasmissione.

Risultati

Sono state impostate le code o la coda di trasmissione del cluster.

Attività correlate

“Pianificazione di code di trasmissione cluster definite manualmente” a pagina 28
Su IBM MQ for z/OS, se si definiscono le code di trasmissione, si ha un maggiore controllo sulle definizioni e sulla serie di pagine in cui vengono conservati i messaggi.

Riferimenti correlati

Gestore code ALTER
VISUALIZZA CLUSQMGR

z/OS *Pianificazione di code di trasmissione cluster definite manualmente*

Su IBM MQ for z/OS, se si definiscono le code di trasmissione, si ha un maggiore controllo sulle definizioni e sulla serie di pagine in cui vengono conservati i messaggi.

Prima di iniziare

Per impostare automaticamente le code di trasmissione cluster, consultare “Code di trasmissione cluster definite automaticamente” a pagina 26.

Informazioni su questa attività

L'amministratore definisce manualmente una coda di trasmissione e utilizza l'attributo della coda CLCHNAME per definire quale canale mittente del cluster, o canali, utilizzerà questa coda come coda di trasmissione.

Tenere presente che CLCHNAME può includere un carattere jolly all'inizio o alla fine, per consentire l'utilizzo di una singola coda per più canali.

Procedura

1. Ad esempio, immettere quanto segue:

```
DEFINE QLOCAL(APPQMGR.CLUSTER1.XMITQ)
CLCHNAME(CLUSTER1.TO.APPQMGR)
USAGE(XMITQ) STGCLASS(STG1)
INDXTYPE( CORRELID ) SHARE

DEFINE STGCLASS(STG1) PSID(3)
DEFINE PSID(3) BUFFERPOOL(4)
```

   Suggerimento: È necessario pianificare la serie di pagine (e il pool di buffer) da utilizzare per le code di trasmissione. È possibile disporre di serie di pagine differenti per code differenti e fornire l'isolamento tra di esse, in modo che il riempimento di una serie di pagine non influisca sulle code di trasmissione in altre serie di pagine.

   Consultare Gestione delle code di trasmissione del cluster e dei canali mittenti del cluster per informazioni su come ciascun canale seleziona la coda appropriata.

   Quando il canale viene avviato, passa la sua associazione alla nuova coda di trasmissione. Per assicurarsi che nessun messaggio venga perso, il gestore code trasferisce automaticamente i messaggi dalla vecchia coda di trasmissione del cluster alla nuova coda di trasmissione in ordine.

2. Utilizzare la funzione CSQUTIL SWITCH per passare alla nuova associazione.

   Per ulteriori informazioni, consultare Commutare la coda di trasmissione associata ai canali mittente del cluster (SWITCH) .

   a) Arrestare il canale, o i canali, la cui coda di trasmissione deve essere modificata, in modo che si trovino nello stato ARRESTATO.

      Ad esempio:

```
STOP CHANNEL(CLUSTER1.TO.APPQMGR)
```

   b) Modificare l'attributo CLCHNAME(XXXX) nella coda di trasmissione.

   c) Utilizzare la funzione SWITCH per commutare i messaggi o monitorare ciò che sta accadendo.

      Utilizzare il comando

```
SWITCH CHANNEL(*) MOVEMSGS(YES)
```

      per spostare i messaggi senza avviare il canale.

   d) Avviare il canale, o i canali, e verificare se il canale sta utilizzando le code corrette.

      Ad esempio:

```
DIS CHS(CLUSTER1.TO.APPQMGR)
DIS CHS(*) where(XMITQ eq APPQMGR.CLUSTER1.XMITQ)
```

   Suggerimento: Il seguente processo utilizza la funzione CSQUTIL SWITCH. Per ulteriori informazioni, consultare Commutazione della coda di trasmissione associata ai canali mittente del cluster (SWITCH).

   Non è necessario utilizzare questa funzione, ma l'utilizzo di questa funzione fornisce più opzioni:

   - L'utilizzo di SWITCH CHANNEL (*) STATUS fornisce un metodo semplice per identificare lo stato di commutazione dei canali mittente del cluster. Consente all'amministratore di visualizzare quali canali sono attualmente in fase di commutazione e i canali con uno switch in sospeso che diventano effettivi al successivo avvio di tali canali.

     Senza questa funzione, l'amministratore deve utilizzare più comandi DISPLAY, quindi elaborare l'output risultante per verificare queste informazioni. L'amministratore può anche confermare che una modifica della configurazione ha il risultato richiesto.
   - Se CSQUTIL viene utilizzato per avviare lo switch, CSQUTIL continua a monitorare l'avanzamento di questa operazione e termina solo quando lo switch è stato completato.

Ciò può rendere molto più semplice l'esecuzione di queste operazioni in batch. Inoltre, se CSQUTIL viene eseguito per commutare più canali, CSQUTIL esegue queste azioni in modo sequenziale; ciò può avere un impatto minore per l'azienda rispetto a più switch in esecuzione in parallelo.

Risultati

È stata impostata la coda di trasmissione del cluster, o le code, su z/OS.

Controllo accessi e code di trasmissione di più cluster

Scegliere tra tre modalità di controllo quando un'applicazione inserisce i messaggi nelle code cluster remote. Le modalità sono la verifica in remoto rispetto alla coda del cluster, la verifica in locale rispetto a `SYSTEM.CLUSTER.TRANSMIT.QUEUE`o la verifica rispetto ai profili locali per la coda del cluster o il gestore code del cluster.

IBM MQ consente di verificare localmente, o localmente e in remoto, che un utente disponga dell'autorizzazione per inserire un messaggio in una coda remota. Un'applicazione tipica IBM MQ utilizza solo il controllo locale e si basa sul gestore code remoto che considera attendibili i controlli di accesso effettuati sul gestore code locale. Se non viene utilizzato il controllo remoto, il messaggio viene inserito nella coda di destinazione con l'autorizzazione del processo del canale dei messaggi remoto. Per utilizzare il controllo remoto, è necessario impostare l'autorizzazione di inserimento del canale di ricezione sulla sicurezza del contesto.

I controlli locali vengono eseguiti rispetto alla coda aperta dall'applicazione. Nell'accodamento distribuito, l'applicazione di solito apre una definizione di coda remota e vengono effettuati controlli di accesso rispetto alla definizione di coda remota. Se il messaggio viene inserito con un'intestazione di instradamento completa, i controlli vengono eseguiti sulla coda di trasmissione. Se un'applicazione apre una coda cluster che non è sul gestore code locale, non vi è alcun oggetto locale da controllare. I controlli del controllo accessi vengono effettuati rispetto alla coda di trasmissione del cluster, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Anche con più code di trasmissione del cluster, i controlli del controllo dell'accesso locale per le code del cluster remoto vengono eseguiti su `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

La scelta del controllo locale o remoto è una scelta tra due estremi. La verifica in remoto è dettagliata. Ogni utente deve disporre di un profilo di controllo accessi su ogni gestore code nel cluster per poter essere inserito in qualsiasi coda cluster. La verifica locale è generica. Ogni utente necessita di un solo profilo di controllo accessi per la coda di trasmissione del cluster sul gestore code a cui è connesso. Con tale profilo, possono inserire un messaggio in qualsiasi coda del cluster su qualsiasi gestore code in qualsiasi cluster.

Gli amministratori hanno un altro modo per impostare il controllo accessi per code cluster. È possibile creare un profilo di sicurezza per una coda del cluster su qualsiasi gestore code nel cluster utilizzando il comando **setmqaut** . Il profilo ha effetto se si apre localmente una coda di cluster remota, specificando solo il nome della coda. È inoltre possibile impostare un profilo per un gestore code remoto. In questo caso, il gestore code può controllare il profilo di un utente che apre una coda cluster fornendo un nome completo.

I nuovi profili funzionano solo se si modifica l'impostazione della stanza Queue Manager **ClusterQueueAccessControl** in `RQMName`. Il valore predefinito è `Xmitq`. Prima di modificare questa impostazione, assicuratevi di aver creato i profili per tutte le applicazioni esistenti che accedono alle code remote del cluster. Se si modifica l'impostazione della stanza in `RQMName` senza creare i profili, è probabile che le applicazioni falliscano.

Suggerimento: Il controllo dell'accesso alla coda del cluster non è valido per l'accodamento remoto. I controlli di accesso vengono ancora eseguiti rispetto alle definizioni locali. Le modifiche indicano che è possibile seguire lo stesso approccio per configurare il controllo accessi sulle code cluster e sugli argomenti cluster. z/OS Le modifiche allineano inoltre l'approccio di controllo dell'accesso per le code cluster più strettamente con z/OS. I comandi per impostare il controllo accessi su z/OS sono diversi, ma entrambi controllano l'accesso rispetto a un profilo piuttosto che all'oggetto stesso.

Concetti correlati

“Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 48
È possibile isolare i flussi di messaggi tra gestori code in un cluster. È possibile inserire i messaggi trasportati da canali mittenti del cluster differenti in code di trasmissione cluster differenti. È possibile utilizzare l'approccio in un singolo cluster o con cluster sovrapposti. L'argomento fornisce esempi e alcune procedure ottimali per guidare l'utente nella scelta di un approccio da utilizzare.

Attività correlate

Impostazione `ClusterQueueAccessControl`

Confronto tra cluster e accodamento distribuito

Confrontare i componenti che devono essere definiti per connettere i gestori code utilizzando l'accodamento distribuito e il cluster.

Se non si utilizzano i cluster, i gestori code sono indipendenti e comunicano utilizzando l'accodamento distribuito. Se un gestore code deve inviare messaggi a un altro gestore code, è necessario definire:

- Una coda di trasmissione
- Un canale per il gestore code remoto

Figura 3 a pagina 31 mostra i componenti richiesti per l'accodamento distribuito.

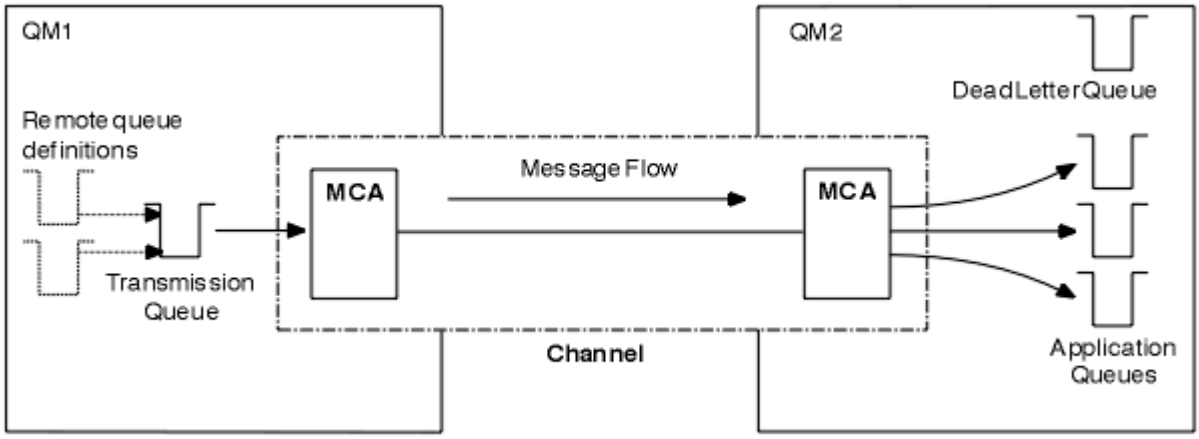


Figura 3. accodamento distribuito

Se si raggruppano i gestori code in un cluster, le code su qualsiasi gestore code sono disponibili per qualsiasi altro gestore code nel cluster. Qualsiasi gestore code può inviare un messaggio a qualsiasi altro gestore code nello stesso cluster senza definizioni esplicite. Non vengono fornite definizioni di canale, definizioni di coda remota o code di trasmissione per ciascuna destinazione. Ogni gestore code in un cluster ha una singola coda di trasmissione da cui può trasmettere messaggi a qualsiasi altro gestore code nel cluster. Ogni gestore code in un cluster deve definire solo:

- Un canale ricevente del cluster su cui ricevere i messaggi
- Un canale mittente del cluster con cui si introduce e impara a conoscere il cluster

Definizioni per impostare un cluster rispetto all'accodamento distribuito

Consultare Figura 4 a pagina 32, che mostra quattro gestori code ciascuno con due code. Considerare quante definizioni sono necessarie per connettere questi gestori code utilizzando l'accodamento distribuito. Confrontare quante definizioni sono necessarie per impostare la stessa rete di un cluster.

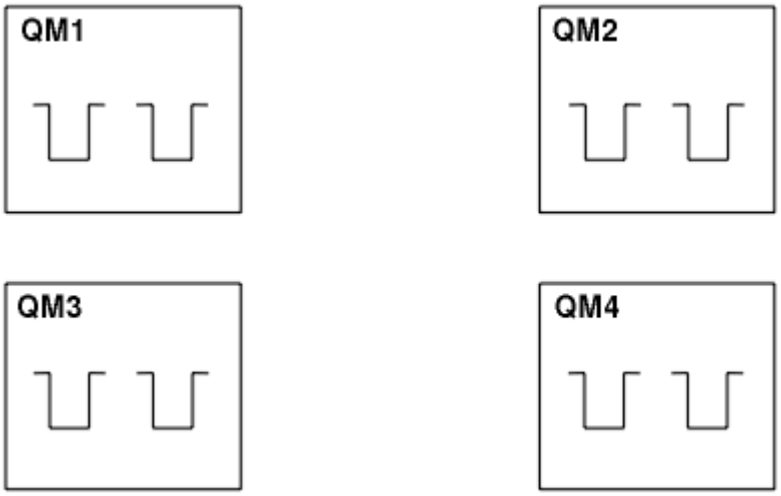


Figura 4. Una rete di quattro gestori code

Definizioni per impostare una rete utilizzando l'accodamento distribuito

Per impostare la rete mostrata in Figura 3 a pagina 31 utilizzando l'accodamento distribuito, è possibile disporre delle seguenti definizioni:

Tabella 2. Definizioni per l'accodamento distribuito

Descrizione	Numero per gestore code	Numero totale
Una definizione di canale mittente per un canale su cui inviare messaggi a ogni altro gestore code	3	12
Una definizione di canale ricevente per un canale su cui ricevere i messaggi da ogni altro gestore code	3	12
Una definizione della coda di trasmissione per una coda di trasmissione per ogni altro gestore code	3	12
Una definizione di coda locale per ciascuna coda locale	2	8
Una definizione di coda remota per ciascuna coda remota in cui questo gestore code desidera inserire i messaggi	6	24

È possibile ridurre questo numero di definizioni utilizzando definizioni generiche di canale ricevente. Il numero massimo di definizioni può essere pari a 17 su ciascun gestore code, che è un totale di 68 per questa rete.

Definizioni per configurare una rete utilizzando i cluster

Per configurare la rete mostrata in Figura 3 a pagina 31 utilizzando cluster sono necessarie le seguenti definizioni:

Tabella 3. Definizioni per il clustering

Descrizione	Numero per gestore code	Numero totale
Una definizione di canale mittente del cluster per un canale su cui inviare i messaggi a un gestore code del repository	1	4
Una definizione di canale ricevente del cluster per un canale su cui ricevere messaggi da altri gestori code nel cluster	1	4

Tabella 3. Definizioni per il clustering (Continua)		
Descrizione	**Numero per gestore code**	**Numero totale**
Una definizione di coda locale per ciascuna coda locale	2	8

Per impostare questo cluster di gestori code (con due repository completi), sono necessarie quattro definizioni su ciascun gestore code, per un totale di sedici definizioni. È inoltre necessario modificare le definizioni dei gestori code per due gestori code, per renderli gestori code con repository completo per il cluster.

Sono richieste solo una definizione di canale CLUSSDR e una CLUSRCVR . Una volta definito il cluster, è possibile aggiungere o rimuovere i gestori code (diversi dai gestori code del repository) senza alcuna interruzione per gli altri gestori code.

L'utilizzo di un cluster riduce il numero di definizioni richieste per configurare una rete contenente molti gestori code.

Con meno definizioni da fare c'è meno rischio di errore:

- I nomi degli oggetti corrispondono sempre, ad esempio il nome del canale in una coppia mittente - destinatario.
- Il nome della coda di trasmissione specificato in una definizione di canale corrisponde sempre alla definizione della coda di trasmissione corretta o al nome della coda di trasmissione specificato in una definizione di coda remota.
- Una definizione QREMOTE punta sempre alla coda corretta sul gestore code remoto.

Una volta impostato un cluster, è possibile spostare le code del cluster da un gestore code a un altro all'interno del cluster senza dover eseguire alcuna attività di gestione del sistema su un altro gestore code. Non è possibile dimenticare di eliminare o modificare le definizioni di canale, coda remota o coda di trasmissione. È possibile aggiungere nuovi gestori code a un cluster senza alcuna interruzione della rete esistente.

Come scegliere i gestori code del cluster per conservare i repository completi

In ogni cluster è necessario scegliere almeno uno e preferibilmente due gestori code per contenere repository completi. Due archivi completi sono sufficienti per tutte le circostanze, tranne le più eccezionali. Se possibile, scegliere i gestori code ospitati su piattaforme robuste e connesse in modo permanente, che non hanno interruzioni coincidenti e che si trovano in una posizione centrale geograficamente. Considerare inoltre la possibilità di dedicare i sistemi come host di repository completi e di non utilizzare tali sistemi per altre attività.

I *repository completi* sono gestori code che mantengono un quadro completo dello stato del cluster. Per condividere queste informazioni, ogni repository completo è connesso dai canali CLUSSDR (e dalle corrispondenti definizioni CLUSRCVR) a ogni altro repository completo nel cluster. È necessario definire manualmente questi canali.

Figura 5. Due repository completi collegati.

Ogni altro gestore code nel cluster conserva un'immagine di ciò che al momento conosce sullo stato del cluster in un *repository parziale*. Questi gestori code pubblicano informazioni su se stessi e richiedono informazioni su altri gestori code, utilizzando due repository completi disponibili. Se un repository completo scelto non è disponibile, ne viene utilizzato un altro. Quando il repository completo scelto diventa di nuovo disponibile, raccoglie le informazioni nuove e modificate più recenti dagli altri in modo che mantengano il passo. Se tutti i repository completi vengono disattivi, gli altri gestori code utilizzano le

informazioni di cui dispongono nei repository parziali. Tuttavia, sono limitati all'utilizzo delle informazioni di cui dispongono; non è possibile elaborare nuove informazioni e richieste di aggiornamenti. Quando i repository completi si riconnettono alla rete, i messaggi vengono scambiati per aggiornare tutti i repository (completi e parziali).

Quando si pianifica l'assegnazione di repository completi, includere le seguenti considerazioni:

- I gestori code selezionati per contenere repository completi devono essere affidabili e gestiti. Scegliere i gestori code ospitati su una piattaforma solida e connessa in modo permanente.
- Considera le interruzioni pianificate per i sistemi che ospitano i tuoi repository completi e assicurati che non abbiano interruzioni coincidenti.
- Considerare le prestazioni di rete: scegliere i gestori code che si trovano in una posizione centrale geograficamente o che condividono lo stesso sistema di altri gestori code nel cluster.
- Considerare se un gestore code è un membro di più di un cluster. Può essere amministrativamente conveniente utilizzare lo stesso gestore code per ospitare i repository completi per diversi cluster, purché questo vantaggio sia bilanciato rispetto a quanto si prevede che il gestore code sia occupato.
- Considerare la possibilità di dedicare alcuni sistemi per contenere solo repository completi e non utilizzare questi sistemi per altre attività. Ciò garantisce che questi sistemi richiedano solo la gestione per la configurazione del gestore code e non vengano rimossi dal servizio per la manutenzione di altre applicazioni aziendali. Inoltre, garantisce che l'attività di gestione del repository non sia in competizione con le applicazioni per le risorse di sistema. Ciò può essere particolarmente utile nei cluster di grandi dimensioni (ad esempio, i cluster di più di un migliaio di gestori code), in cui i repository completi hanno un carico di lavoro molto più elevato nel mantenere lo stato del cluster.

Avere più di due repository completi è possibile, ma raramente consigliato. Sebbene le definizioni degli oggetti (ossia, code, argomenti e canali) fluiscano in tutti i repository completi disponibili, le richieste fluiscono solo da un repository parziale a un massimo di due repository completi. Ciò significa che, quando vengono definiti più di due repository completi e due repository completi diventano non disponibili, alcuni repository parziali potrebbero non ricevere gli aggiornamenti previsti. Consultare ClusterMQ : perché solo due repository completi?

Una situazione in cui potrebbe essere utile definire più di due repository completi è quando si migrano i repository completi esistenti su un nuovo hardware o su nuovi gestori code. In questo caso, è necessario introdurre i repository completi di sostituzione e confermare che siano diventati completamente popolati, prima di rimuovere i repository completi precedenti. Ogni volta che si aggiunge un repository completo, è necessario connetterlo direttamente a ogni altro repository completo con i canali CLUSSDR .

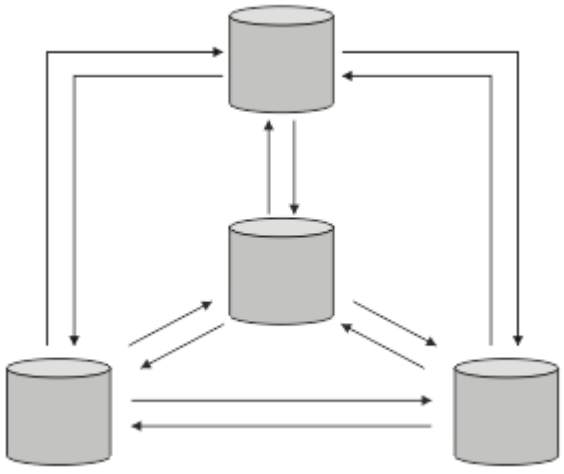


Figura 6. Più di due repository completi connessi

Informazioni correlate

Cluster MQ : perché solo due repository completi?
Quanto può essere grande un cluster MQ ?

Organizzazione di un cluster

Selezionare quali gestori code collegare e a quale repository completo. Considerare l'effetto delle prestazioni, la versione del gestore code e se sono desiderabili più canali CLUSSDR .

Dopo aver selezionato i gestori code per conservare i repository completi, è necessario decidere quali gestori code collegare a quale repository completo. La definizione del Canale CLUSSDR collega un gestore code a un repository completo da cui rileva gli altri repository completi nel cluster. Da quel momento in poi, il gestore code invia messaggi a due repository completi. Tenta sempre di utilizzare prima quello per cui ha una definizione di canale CLUSSDR . È possibile scegliere di collegare un gestore code a un repository completo. Nella scelta, considerare la topologia della propria configurazione e la posizione fisica o geografica dei gestori code.

Poiché tutte le informazioni sul cluster vengono inviate a due repository completi, potrebbero verificarsi situazioni in cui si desidera creare una seconda definizione di canale CLUSSDR . È possibile definire un secondo canale CLUSSDR in un cluster con molti repository completi distribuiti su una vasta area. È quindi possibile controllare a quali due repository completi vengono inviate le informazioni.

Convenzioni di denominazione cluster

Considerare la denominazione dei gestori code nello stesso cluster utilizzando una convenzione di denominazione che identifica il cluster a cui appartiene il gestore code. Utilizzare una convenzione di denominazione simile per i nomi canale ed estenderla per descrivere le caratteristiche del canale.

Procedure ottimali per la denominazione di cluster MQ

Sebbene i nomi cluster possano avere una lunghezza massima di 48 caratteri, i nomi cluster relativamente brevi sono utili quando si applicano le convenzioni di denominazione ad altri oggetti. Consultare “Procedure ottimali per la scelta dei nomi dei canali cluster” a pagina 35.

Quando si sceglie un nome cluster, di solito è utile rappresentare lo 'scopo' del cluster (che è probabile sia di lunga durata) piuttosto che il 'contenuto'. Ad esempio 'B2BPROD' o 'ACTTEST' invece di 'QM1_QM2_QM3_CLUS'.

Procedure ottimali nella scelta dei nomi dei gestori code del cluster

Se si sta creando un nuovo cluster e i relativi membri da zero, considerare una convenzione di denominazione per i gestori code che rifletta l'utilizzo del cluster. Ogni gestore code deve avere un nome differente. Tuttavia, è possibile fornire ai gestori code in un cluster una serie di nomi simili, per facilitare l'identificazione e la memorizzazione dei raggruppamenti logici (ad esempio, 'ACTTQM1, ACTTQM2).

I nomi dei gestori code relativamente brevi (ad esempio, meno di 8 caratteri) aiutano se si sceglie di utilizzare la convenzione descritta nella sezione successiva, o qualcosa di simile, per i nomi dei canali.

Procedure ottimali per la scelta dei nomi dei canali cluster

Poiché i gestori code e i cluster possono avere nomi fino a 48 caratteri e un nome canale è limitato a 20 caratteri, prestare attenzione quando si denominano gli oggetti per evitare di dover modificare la convenzione di denominazione a metà di un progetto (vedere la sezione precedente).

Quando si definiscono i canali, tenere presente che i canali mittenti del cluster creati automaticamente su qualsiasi gestore code del cluster prendono il loro nome dal canale ricevente del cluster corrispondente configurato sul gestore code ricevente nel cluster e devono pertanto essere univoci e avere senso *sui gestori code remoti nel cluster.*

Un approccio comune consiste nell'utilizzare il nome gestore code preceduto dal nome cluster. Ad esempio, se il nome del cluster è CLUSTER1 e i gestori code sono QM1, QM2, i canali riceventi del cluster sono CLUSTER1.QM1, CLUSTER1.QM2.

È possibile estendere questa convenzione se i canali hanno priorità differenti o utilizzano protocolli differenti. Ad esempio:

- CLUSTER1.QM1.S1

- CLUSTER1.QM1.N3
- CLUSTER1.QM1.T4

In questo esempio, S1 potrebbe essere il primo canale SNA, N3 potrebbe essere il canale NetBIOS con una priorità di rete di tre e T4 potrebbe essere un IP TCP utilizzando una rete IPV4 .

Denominazione delle definizioni di canale condiviso

Una singola definizione di canale può essere condivisa tra più cluster, nel qual caso le convenzioni di denominazione qui suggerite richiedono modifiche. Tuttavia, come descritto in Gestione delle definizioni di canale , di solito è preferibile definire canali discreti per ciascun cluster in ogni caso.

Convenzioni di denominazione dei canali meno recenti

Al di fuori degli ambienti cluster, è stato storicamente comune utilizzare una convenzione di denominazione 'FROMQM.TO.TARGETQM', quindi è possibile che i cluster esistenti abbiano utilizzato qualcosa di simile (come CLUSTER.TO.TARGET). Ciò non è consigliato come parte di un nuovo schema di denominazione del cluster in quanto riduce ulteriormente i caratteri disponibili per trasmettere informazioni 'utili' all'interno del nome del canale.

z/OS **Nomi canale su IBM MQ for z/OS**

È possibile definire le risorse generiche VTAM o i nomi generici DDNS (*Dynamic Domain Name Server*). È possibile definire i nomi di connessione utilizzando nomi generici. Tuttavia, quando si crea una definizione ricevente del cluster, non utilizzare un nome di connessione generico.

Il problema con l'utilizzo di nomi di connessione generici per le definizioni di ricevente del cluster è il seguente: se si definisce un CLUSRCVR con un CONNAME generico, non è possibile garantire che i canali CLUSSDR puntino ai gestori code desiderati. Il CLUSSDR iniziale potrebbe finire per puntare a qualsiasi gestore code nel gruppo di condivisione code, non necessariamente uno che ospita un repository completo. Se un canale inizia a tentare nuovamente una connessione, potrebbe riconnettersi a un gestore code differente con lo stesso nome generico, interrompendo il flusso di messaggi.

z/OS ***Cluster e gruppi di condivisione code***

Le code condivise possono essere code cluster e i gestori code in un gruppo di condivisione code possono essere anche gestori code cluster.

Su IBM MQ for z/OS è possibile raggruppare i gestori code in gruppi di condivisione code. Un gestore code in un gruppo di condivisione code può definire una coda locale che deve essere condivisa da un massimo di 32 gestori code.

Le code condivise possono anche essere code cluster. Inoltre, i gestori code in un gruppo di condivisione code possono trovarsi anche in uno o più cluster.

È possibile definire le risorse generiche VTAM o i nomi generici DDNS (*Dynamic Domain Name Server*). È possibile definire i nomi di connessione utilizzando nomi generici. Tuttavia, quando si crea una definizione ricevente del cluster, non utilizzare un nome di connessione generico.

Il problema con l'utilizzo di nomi di connessione generici per le definizioni di ricevente del cluster è il seguente: se si definisce un CLUSRCVR con un CONNAME generico, non è possibile garantire che i canali CLUSSDR puntino ai gestori code desiderati. Il CLUSSDR iniziale potrebbe finire per puntare a qualsiasi gestore code nel gruppo di condivisione code, non necessariamente uno che ospita un repository completo. Se un canale inizia a tentare nuovamente una connessione, potrebbe riconnettersi a un gestore code differente con lo stesso nome generico, interrompendo il flusso di messaggi.

Un canale CLUSRCVR che utilizza la porta del listener del gruppo non può essere avviato perché, in questo caso, non sarebbe possibile indicare a quale gestore code si connette ogni volta CLUSRCVR . Le code del sistema cluster su cui vengono conservate le informazioni sul cluster non vengono condivise. Ogni gestore code ha il proprio.

I canali cluster vengono utilizzati non solo per trasferire i messaggi dell'applicazione ma anche per i messaggi di sistema interni relativi all'impostazione del cluster. Ogni gestore code nel cluster deve

ricevere questi messaggi di sistema interni per partecipare correttamente al clustering, quindi necessita del proprio canale CLUSRCVR univoco su cui riceverli.

Un CLUSRCVR condiviso potrebbe essere avviato su qualsiasi gestore code nel gruppo di condivisione code (QSG) e quindi portare a una fornitura incoerente dei messaggi di sistema interni ai gestori code QSG, il che significa che nessuno può partecipare correttamente al cluster. Per garantire che non sia possibile utilizzare canali CLUSRCVR condivisi, qualsiasi tentativo non riesce con il messaggio CSQX502E .

Cluster sovrapposti

I cluster sovrapposti forniscono ulteriori funzioni di gestione. Utilizzare gli elenchi nomi per ridurre il numero di comandi necessari per gestire i cluster che si sovrappongono.

È possibile creare cluster che si sovrappongono. Ci sono una serie di motivi per cui è possibile definire i cluster che si sovrappongono; ad esempio:

- Per consentire alle diverse organizzazioni di avere la propria amministrazione.
- Per consentire la gestione separata delle applicazioni indipendenti.
- Per creare classi di servizio.

In Figura 7 a pagina 38, il gestore code STF2 è membro di entrambi i cluster. Quando un gestore code è membro di più di un cluster, è possibile sfruttare gli elenchi dei nomi per ridurre il numero di definizioni necessarie. Gli elenchi nomi contengono un elenco di nomi, ad esempio, nomi cluster. È possibile creare un elenco nomi che denomina i cluster. Specificare l'elenco nomi nel comando ALTER QMGR per STF2 per renderlo un gestore code del repository completo per entrambi i cluster.

Se hai più di un cluster nella tua rete, devi fornire loro nomi diversi. Se due cluster con lo stesso nome vengono uniti, non è possibile separarli di nuovo. È anche una buona idea dare ai cluster e ai canali nomi diversi. Sono più facilmente distinguibili quando si guarda l'output dei comandi DISPLAY . I nomi dei gestori code devono essere univoci all'interno di un cluster per poter funzionare correttamente.

Definizione di classi di servizio

Immagina un'università che abbia un gestore code per ogni membro del personale e ogni studente. I messaggi tra membri del personale devono viaggiare su canali con una priorità elevata e una larghezza di banda elevata. I messaggi tra gli studenti devono viaggiare su canali più economici e lenti. È possibile impostare questa rete utilizzando tecniche di accodamento distribuite tradizionali. IBM MQ seleziona quali canali utilizzare esaminando il nome della coda di destinazione e il nome del gestore code.

Per distinguere chiaramente tra il personale e gli studenti, è possibile raggruppare i relativi gestori code in due cluster, come mostrato in Figura 7 a pagina 38. IBM MQ sposta i messaggi nella coda delle riunioni nel cluster del personale solo sui canali definiti in quel cluster. I messaggi per la coda di gossip nel cluster di studenti passano attraverso i canali definiti in tale cluster e ricevono la classe di servizio appropriata.

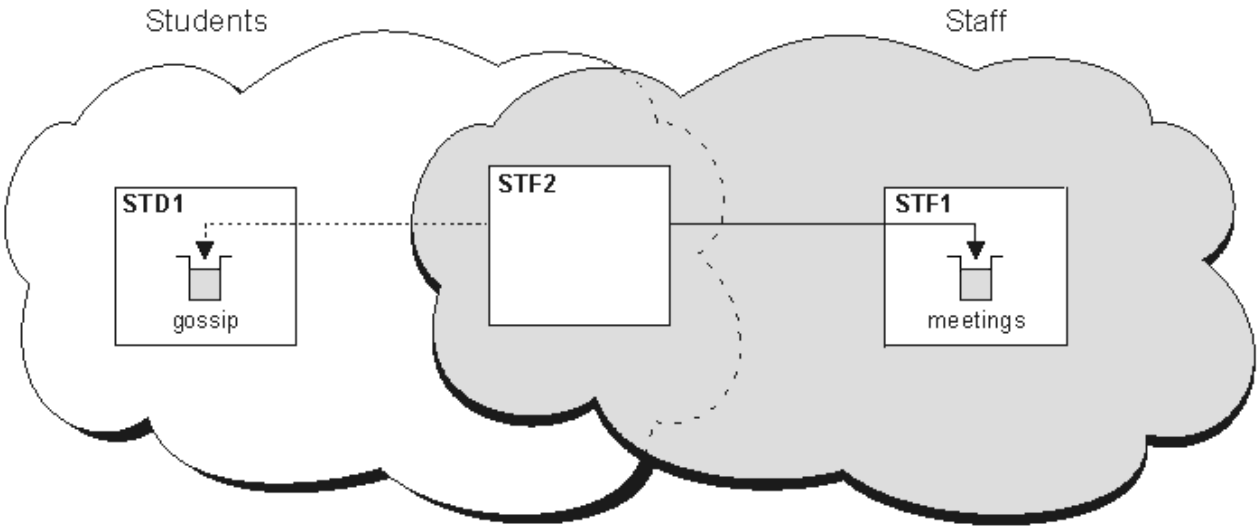


Figura 7. Classi di servizio

Suggerimenti per il clustering

Potrebbe essere necessario apportare alcune modifiche ai propri sistemi o applicazioni prima di utilizzare il clustering. Ci sono sia somiglianze che differenze dal comportamento dell'accodamento distribuito.

- È necessario aggiungere definizioni di configurazione manuali ai gestori code all'esterno di un cluster per consentire loro di accedere alle code cluster.
- Se si uniscono due cluster con lo stesso nome, non è possibile separarli di nuovo. Pertanto, è consigliabile assegnare a tutti i cluster un nome univoco.
- Se un messaggio arriva a un gestore code ma non vi è alcuna coda per riceverlo, il messaggio viene inserito nella coda di messaggi non recapitabili. Se non è presente una coda di messaggi non recapitabili, il canale ha esito negativo e riprova. L'utilizzo della coda di messaggi non recapitabili è uguale a quello della coda distribuita.
- L'integrità dei messaggi persistenti viene mantenuta. I messaggi non vengono duplicati o persi come risultato dell'utilizzo dei cluster.
- L'utilizzo di cluster riduce la gestione del sistema. I cluster semplificano la connessione di reti più grandi con molti più gestori code di quanti ne sarebbero in grado di considerare l'utilizzo dell'accodamento distribuito. Esiste il rischio che si consumino risorse di rete eccessive se si tenta di abilitare la comunicazione tra ogni gestore code in un cluster.
- Se si utilizza IBM MQ Explorer, che presenta i gestori code in una struttura ad albero, la vista per i cluster di grandi dimensioni potrebbe essere complessa.
- Multi Lo scopo degli elenchi di distribuzione è utilizzare un singolo comando MQPUT per inviare lo stesso messaggio a più destinazioni. Gli elenchi di distribuzione sono supportati su IBM MQ for Multiplatforms. È possibile utilizzare elenchi di distribuzione con cluster di gestori code. In un cluster, tutti i messaggi vengono espansi all'ora MQPUT . Il vantaggio, in termini di traffico di rete, non è così grande come in un ambiente non cluster. Il vantaggio delle liste di distribuzione è che i numerosi canali e code di trasmissione non devono essere definiti manualmente.
- Se stai per utilizzare i cluster per bilanciare il tuo carico di lavoro, esamina le tue applicazioni. Verificare se i messaggi devono essere elaborati da un particolare gestore code o in una particolare sequenza. Si dice che tali applicazioni abbiano affinità di messaggi. Potrebbe essere necessario modificare le applicazioni prima di poterle utilizzare in cluster complessi.
- È possibile scegliere di utilizzare l'opzione MQOO_BIND_ON_OPEN su un MQOPEN per forzare l'invio di messaggi a una destinazione specifica. Se il gestore code di destinazione non è disponibile, i messaggi non vengono consegnati finché il gestore code non diventa nuovamente disponibile. I messaggi non vengono instradati a un altro gestore code a causa del rischio di duplicazione.

- Se un gestore code deve ospitare un repository del cluster, è necessario conoscerne il nome host o l'indirizzo IP. È necessario specificare queste informazioni nel parametro CONNAME quando si crea la definizione CLUSSDR su altri gestori code che si uniscono al cluster. Se si utilizza DHCP, l'indirizzo IP è soggetto a modifica in quanto DHCP può assegnare un nuovo indirizzo IP ogni volta che si riavvia un sistema. Pertanto, non è necessario specificare l'indirizzo IP nelle definizioni CLUSSDR . Anche se tutte le definizioni CLUSSDR specificano il nome host piuttosto che l'indirizzo IP, le definizioni non sarebbero comunque affidabili. DHCP non aggiorna necessariamente la voce della directory DNS per l'host con il nuovo indirizzo. Se è necessario denominare i gestori code come repository completi sui sistemi che utilizzano DHCP, installare il software che garantisce l'aggiornamento della directory DNS.
- Non utilizzare nomi generici, ad esempio risorse generiche VTAM o nomi generici DDNS (Dynamic Domain Name Server) come nomi di connessione per i propri canali. In tal caso, i canali potrebbero connettersi a un gestore code diverso da quello previsto.
- È possibile ottenere un messaggio solo da una coda cluster locale, ma è possibile inserire un messaggio in qualsiasi coda in un cluster. Se si apre una coda per utilizzare il comando MQGET , il gestore code apre la coda locale.
- Non è necessario modificare alcuna delle applicazioni se si imposta un cluster IBM MQ semplice. L'applicazione può denominare la coda di destinazione sulla chiamata MQOPEN e non è necessario conoscere l'ubicazione del gestore code. Se si configura un cluster per la gestione del carico di lavoro, è necessario esaminare le applicazioni e modificarle in base alle esigenze.
- È possibile visualizzare i dati di monitoraggio e di stato correnti per un canale o una coda utilizzando i comandi DISPLAY CHSTATUS e DISPLAY QSTATUS **runmqsc** . Le informazioni di controllo possono essere utilizzate per misurare le prestazioni e l'integrità del sistema. Il monitoraggio è controllato dagli attributi gestore code, coda e canale. Il monitoraggio dei canali mittenti del cluster definiti automaticamente è possibile con l'attributo del gestore code MONACLS .

Concetti correlati

Cluster

“Confronto tra cluster e accodamento distribuito” a pagina 31
Confrontare i componenti che devono essere definiti per connettere i gestori code utilizzando l'accodamento distribuito e il cluster.

Componenti di un cluster

Attività correlate

Configurazione di un cluster di gestore code

Configurazione di un nuovo cluster

Per quanto tempo i repository dei gestori code conservano le informazioni?

I repository del gestore code conservano le informazioni per 30 giorni. Un processo automatico aggiorna in modo efficiente le informazioni utilizzate.

Quando un gestore code invia alcune informazioni su se stesso, i gestori code del repository completo e parziale memorizzano le informazioni per 30 giorni. Le informazioni vengono inviate, ad esempio, quando un gestore code annuncia la creazione di una nuova coda. Per impedire la scadenza di queste informazioni, i gestori code inviano automaticamente tutte le informazioni su se stessi dopo 27 giorni. Se un repository parziale invia una nuova richiesta di informazioni in parte per tutta la durata di 30 giorni, il tempo di scadenza rimane quello originale di 30 giorni.

Quando le informazioni scadono, non vengono rimosse immediatamente dal repository. Invece è tenuto per un periodo di grazia di 60 giorni. Se non viene ricevuto alcun aggiornamento entro il periodo di tolleranza, le informazioni vengono rimosse. Il periodo di dilazione consente il fatto che un gestore code potrebbe essere temporaneamente fuori servizio alla data di scadenza. Se un gestore code viene disconnesso da un cluster per più di 90 giorni, smette di far parte del cluster. Tuttavia, se si riconnette alla rete, diventa di nuovo parte del cluster. I repository completi non utilizzano le informazioni scadute per soddisfare le nuove richieste provenienti da altri gestori code.

Allo stesso modo, quando un gestore code invia una richiesta di informazioni aggiornate da un repository completo, la richiesta dura 30 giorni. Dopo 27 giorni IBM MQ controlla la richiesta. Se è stato fatto riferimento ad esso durante i 27 giorni, viene aggiornato automaticamente. In caso contrario, viene

lasciato scadere e viene aggiornato dal gestore code se è di nuovo necessario. La scadenza delle richieste impedisce la creazione di richieste di informazioni dai gestori code inattivi.

Nota: È necessario scaricare e installare la PTF per APAR PH43191, che corregge gli errori di sistema nel calcolo della scadenza di una sottoscrizione. Questi errori possono causare la scadenza anticipata della sottoscrizione (con conseguente emissione del messaggio CSQX456I) o la scadenza dopo la scadenza dell'oggetto (con conseguente errore MQRC 2085 (MQRC_UNKNOWN_OBJECT)).

Per i cluster di grandi dimensioni, può essere disruttivo se molti gestori code inviano automaticamente tutte le informazioni su se stessi contemporaneamente. Consultare Refreshing in a large cluster can affect performance and availability of the cluster.

Concetti correlati

"Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER" a pagina 70
Utilizzare il comando **REFRESH CLUSTER** per eliminare tutte le informazioni contenute localmente su un cluster e ricreare tali informazioni dai repository completi nel cluster. Non è necessario utilizzare questo comando, tranne in circostanze eccezionali. Se hai bisogno di usarlo, ci sono considerazioni speciali su come usarlo. Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

Cluster di esempio

Il primo esempio mostra il cluster più piccolo possibile di due gestori code. Il secondo e il terzo esempio mostrano due versioni di un cluster di gestori code.

Il cluster più piccolo possibile contiene solo due gestori code. In questo caso, entrambi i gestori code contengono repository completi. Sono necessarie solo poche definizioni per configurare il cluster, ma esiste un alto grado di autonomia in ogni gestore code.

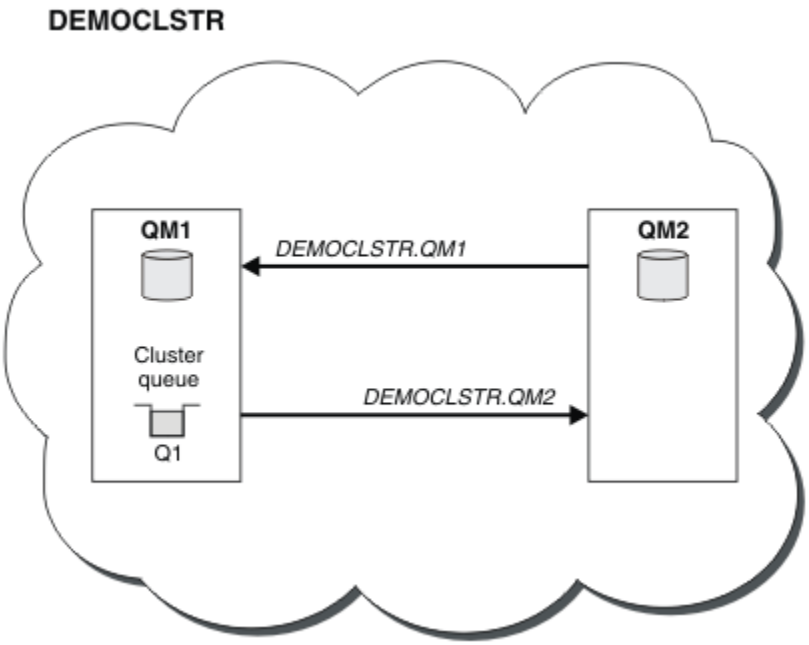


Figura 8. Un piccolo cluster di due gestori code

- I gestori code possono avere nomi lunghi come LONDON e NEWYORK. z/OS Su IBM MQ for z/OS, i nomi dei gestori code sono limitati a quattro caratteri.
- Ogni gestore code è generalmente configurato su una macchina separata. Tuttavia, è possibile avere più gestori code sulla stessa macchina.

Per istruzioni sulla configurazione di un cluster di esempio simile, consultare Configurazione di un nuovo cluster.

Figura 9 a pagina 41 mostra i componenti di un cluster denominato CLSTR1.

- In questo cluster, sono presenti tre gestori code, QM1, QM2e QM3.
- QM1 e QM2 ospitano repository di informazioni su tutti i gestori code e gli oggetti correlati al cluster nel cluster. Ad essi si fa riferimento come *gestori code repository completi*. I repository sono rappresentati nel diagramma dai cilindri ombreggiati.
- QM2 e QM3 ospitano alcune code accessibili a qualsiasi altro gestore code nel cluster. Le code accessibili a qualsiasi altro gestore code nel cluster vengono denominate *code cluster*. Le code cluster sono rappresentate nel diagramma dalle code ombreggiate. Le code cluster sono accessibili da qualsiasi punto del cluster. Il codice cluster IBM MQ garantisce che le definizioni di coda remota per le code cluster vengano create su qualsiasi gestore code a cui fanno riferimento.

  Come con l'accodamento distribuito, un'applicazione utilizza la chiamata MQPUT per inserire un messaggio su una coda del cluster in qualsiasi gestore code del cluster. Un'applicazione utilizza la chiamata MQGET per richiamare i messaggi da una coda cluster solo sul gestore code in cui risiede la coda.
- Ogni gestore code ha una definizione creata manualmente per l'estremità di ricezione di un canale denominato *cluster_name. queue_manager_name* su cui può ricevere messaggi. Sul gestore code di ricezione, *cluster_name. queue_manager_name* è un canale ricevente del cluster. Un canale ricevente del cluster è simile a un canale ricevente utilizzato nell'accodamento distribuito; riceve i messaggi per il gestore code. Inoltre, riceve anche informazioni sul cluster.
-

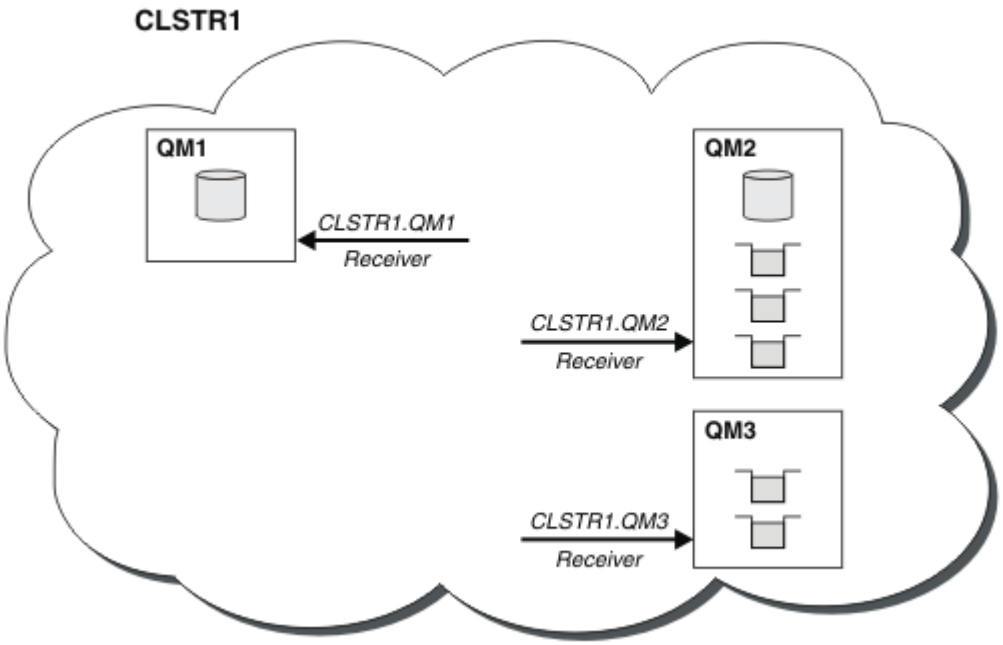


Figura 9. Un cluster di gestori code

- In Figura 10 a pagina 42 ogni gestore code ha anche una definizione per l'estremità di invio di un canale. Si collega al canale ricevente del cluster di uno dei gestori code del repository completo. Sul gestore code di invio, *cluster_name. queue_manager_name* è un canale mittente del cluster. QM1 e QM3 hanno canali mittenti del cluster che si collegano a CLSTR1.QM2, consultare la linea tratteggiata "2".

  QM2 ha un canale mittente del cluster che si connette a CLSTR1.QM1, vedi la riga tratteggiata "3". Un canale mittente del cluster è simile a un canale mittente utilizzato nell'accodamento distribuito; invia messaggi al gestore code di ricezione. Inoltre, invia anche informazioni sul cluster.

  Una volta definite sia l'estremità del ricevente del cluster che l'estremità del mittente del cluster di un canale, il canale viene avviato automaticamente.

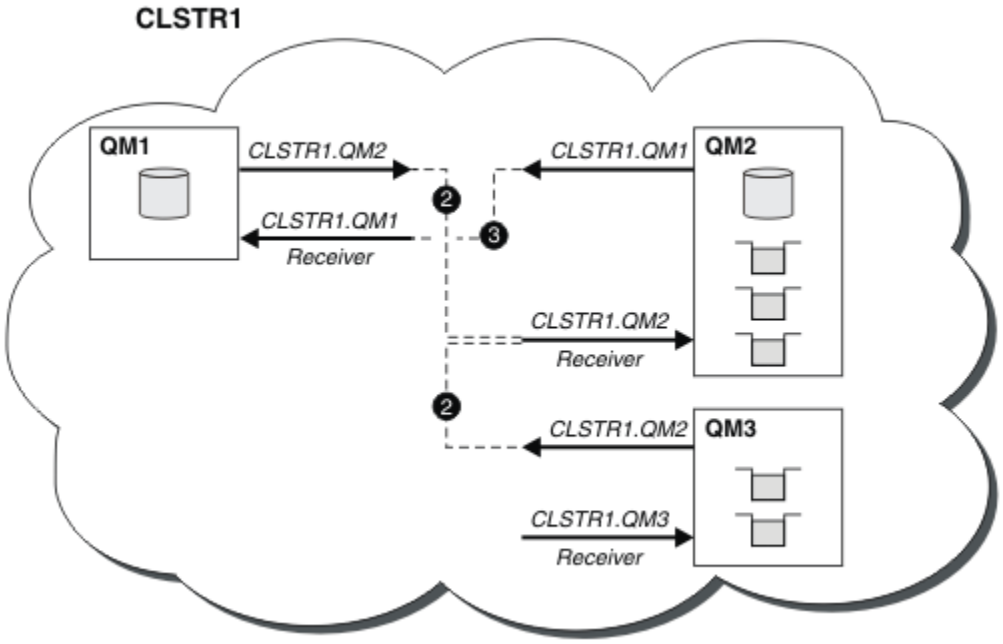


Figura 10. Un cluster di gestori code con canali mittente

La definizione di un canale mittente del cluster sul gestore code locale introduce tale gestore code a un gestore code del repository completo. Il gestore code del repository completo aggiorna le informazioni nel repository completo di conseguenza. Quindi crea automaticamente un canale mittente del cluster al gestore code originale e invia tali informazioni sul cluster. Pertanto, un gestore code apprende informazioni su un cluster e un cluster apprende informazioni su un gestore code.

Esaminare nuovamente Figura 9 a pagina 41. Si supponga che un'applicazione connessa al gestore code QM3 desideri inviare alcuni messaggi alle code in QM2. La prima volta che QM3 deve accedere a tali code, le rileva consultando un repository completo. Il repository completo in questo caso è QM2, a cui si accede utilizzando il canale mittente CLSTR1.QM2. Con le informazioni del repository, è possibile creare automaticamente definizioni remote per tali code. Se le code si trovano su QM1, questo meccanismo funziona ancora, poiché QM2 è un repository completo. Un repository completo ha un record completo di tutti gli oggetti nel cluster. In questo ultimo caso, QM3 crea automaticamente anche un canale mittente del cluster corrispondente al canale ricevente del cluster su QM1, consentendo la comunicazione diretta tra i due.

La Figura 11 a pagina 43 mostra lo stesso cluster, con i due canali mittente del cluster che sono stati creati automaticamente. I canali mittenti del cluster sono rappresentati dalle due linee tratteggiate che si uniscono con il canale ricevente del cluster CLSTR1.QM3. Mostra anche la coda di trasmissione del cluster, SYSTEM.CLUSTER.TRANSMIT.QUEUE, che QM1 utilizza per inviare i propri messaggi. Tutti i gestori code nel cluster hanno una coda di trasmissione cluster, da cui possono inviare messaggi a qualsiasi altro gestore code nello stesso cluster.

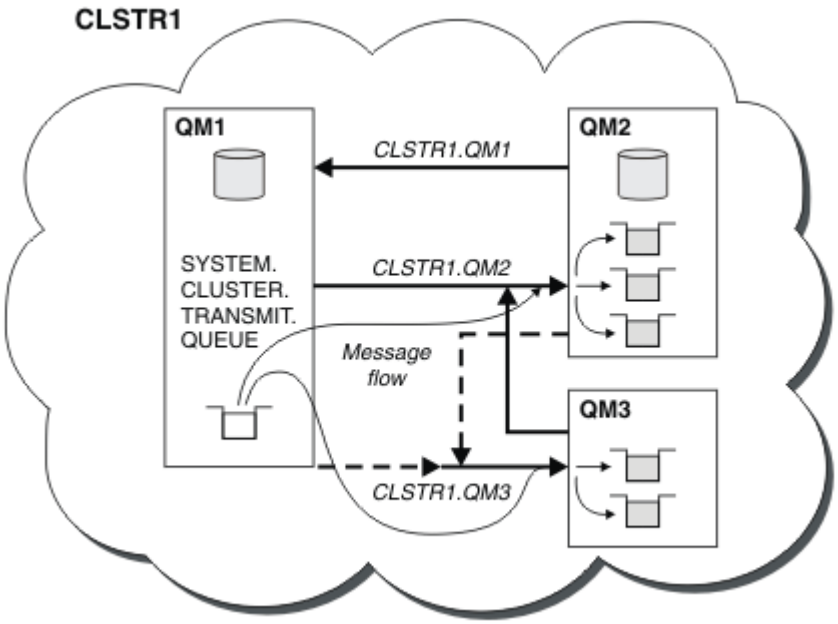


Figura 11. Un cluster di gestori code, che mostra canali definiti automaticamente

Nota: Altri diagrammi mostrano solo le estremità di ricezione dei canali per cui si effettuano definizioni manuali. Le estremità di invio vengono omesse perché sono per lo più definite automaticamente quando necessario. La definizione automatica della maggior parte dei canali mittente del cluster è fondamentale per la funzione e l'efficienza dei cluster.

Concetti correlati

“Confronto tra cluster e accodamento distribuito” a pagina 31
Confrontare i componenti che devono essere definiti per connettere i gestori code utilizzando l'accodamento distribuito e il cluster.

Componenti di un cluster

Attività correlate

Configurazione di un cluster di gestore code

Configurazione di un nuovo cluster

Clustering: procedure ottimali

I cluster forniscono un meccanismo per l'interconnessione dei gestori code. Le migliori pratiche descritte in questa sezione si basano su test e feedback da parte dei clienti.

Una corretta configurazione del cluster dipende da una buona pianificazione e da una conoscenza approfondita dei fondamentali di IBM MQ , come una buona gestione dell'applicazione e la progettazione della rete. Accertarsi di conoscere le informazioni contenute negli argomenti correlati prima di continuare.

Concetti correlati

Accodamento distribuito e cluster

Cluster

Attività correlate

“Progettazione di cluster” a pagina 24
I cluster forniscono un meccanismo per l'interconnessione dei gestori code in modo da semplificare sia la configurazione iniziale che la gestione in corso. I cluster devono essere attentamente progettati per garantire che funzionino correttamente e che raggiungano i livelli richiesti di disponibilità e reattività.

Monitoraggio dei cluster

Clustering: considerazioni speciali per i cluster che si sovrappongono
Questo argomento fornisce una guida per la pianificazione e la gestione dei cluster IBM MQ . Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

Proprietà del cluster

Acquisire dimestichezza con i cluster sovrapposti prima di leggere le seguenti informazioni. Per le informazioni necessarie, consultare “Cluster sovrapposti” a pagina 37 e Configurazione dei percorsi dei messaggi tra i cluster .

Quando si configura e si gestisce un sistema costituito da cluster sovrapposti, è preferibile attenersi a quanto segue:

- Sebbene i cluster IBM MQ siano 'liberamente accoppiati' come precedentemente descritto, è utile considerare un cluster come una singola unità di amministrazione. Questo concetto viene utilizzato perché l'interazione tra definizioni su singoli gestori code è fondamentale per il regolare funzionamento del cluster. Ad esempio: quando si utilizzano le code cluster bilanciate del carico di lavoro, è importante che un singolo amministratore o team comprenda la serie completa di destinazioni possibili per i messaggi, che dipende dalle definizioni diffuse in tutto il cluster. Più banalmente, le coppie di canali mittente / ricevente del cluster devono essere compatibili.
- Considerando questo concetto precedente, in cui si incontrano più cluster (che devono essere gestiti da team / individui separati), è importante disporre di politiche chiare che controllino l'amministrazione dei gestori code del gateway.
- È utile considerare i cluster sovrapposti come un singolo spazio dei nomi: i nomi dei canali e dei gestori code devono essere univoci in un singolo cluster. La gestione è molto più semplice quando è univoca nell'intera topologia. È consigliabile seguire una convenzione di denominazione appropriata, le convenzioni possibili sono descritte in “Convenzioni di denominazione cluster” a pagina 35.
- A volte la cooperazione amministrativa e di gestione del sistema è essenziale. Ad esempio, la cooperazione tra organizzazioni che possiedono cluster differenti che devono sovrapporsi. Una chiara comprensione di chi possiede cosa e le regole e le convenzioni applicabili aiuta il clustering a funzionare senza problemi quando si sovrappongono i cluster.

Sovrapposizione di cluster: gateway

In generale, un singolo cluster è più facile da gestire rispetto a più cluster. Pertanto, la creazione di un gran numero di piccoli cluster (uno per ogni applicazione, ad esempio) è qualcosa da evitare in generale.

Tuttavia, per fornire classi di servizio, è possibile implementare cluster sovrapposti. Ad esempio:

- Se si dispone di cluster concentrici in cui il più piccolo è per la pubblicazione / sottoscrizione. Per ulteriori informazioni, consultare Come dimensionare i sistemi .
- Se alcuni gestori code devono essere gestiti da team differenti. Consultare la sezione precedente “Proprietà del cluster” a pagina 44per ulteriori informazioni.
- Se ha senso dal punto di vista organizzativo o geografico.
- Se i cluster equivalenti funzionano con la risoluzione dei nomi, ad esempio quando si implementano TLS in un cluster esistente.

Non vi è alcun vantaggio per la sicurezza derivante dalla sovrapposizione di cluster; consentendo ai cluster gestiti da due diversi team di sovrapporsi, si uniscono efficacemente ai team e alla topologia:

- Qualsiasi nome pubblicizzato in un cluster di questo tipo è accessibile all'altro cluster.
- Qualsiasi nome pubblicizzato in un cluster può essere pubblicizzato nell'altro per estrarre i messaggi idonei.
- Qualsiasi oggetto non pubblicizzato su un gestore code adiacente al gateway può essere risolto da qualsiasi cluster di cui il gateway è membro.

Il namespace è l'unione di entrambi i cluster e deve essere considerato come un singolo namespace. Pertanto, la proprietà di un cluster sovrapposto viene condivisa tra tutti gli amministratori di entrambi i cluster.

Quando un sistema contiene più cluster, potrebbe essere necessario instradare i messaggi dai gestori code in un cluster alle code sui gestori code in un altro cluster. In questa situazione, i cluster multipli devono essere interconnessi in qualche modo: un buon modello da seguire è l'utilizzo dei gestori code gateway tra i cluster. Questa disposizione evita di creare una rete difficile da gestire di canali point - to - point e fornisce un buon posto per gestire questioni quali le politiche di sicurezza. Ci sono due modi distinti per raggiungere questo accordo:

1. Inserire uno o più gestori code in entrambi i cluster utilizzando una seconda definizione del destinatario del cluster. Questa disposizione comporta un minor numero di definizioni amministrative, ma, come precedentemente affermato, significa che la proprietà di un cluster sovrapposto è condivisa tra tutti gli amministratori di entrambi i cluster.
2. Associare un gestore code nel cluster uno con un gestore code nel cluster due utilizzando i canali point-to-point tradizionali.

In entrambi i casi, è possibile utilizzare vari strumenti per instradare il traffico in modo appropriato. In particolare, gli alias della coda o del gestore code possono essere utilizzati per eseguire l'instradamento nell'altro cluster e un alias del gestore code con la proprietà **RQMNAME** vuota riguida il bilanciamento del carico di lavoro nel punto desiderato.

Concetti correlati

“Convenzioni di denominazione cluster” a pagina 35
Considerare la denominazione dei gestori code nello stesso cluster utilizzando una convenzione di denominazione che identifica il cluster a cui appartiene il gestore code. Utilizzare una convenzione di denominazione simile per i nomi canale ed estenderla per descrivere le caratteristiche del canale.

Clustering: considerazioni sulla progettazione della topologia
Questo argomento fornisce una guida per la pianificazione e la gestione dei cluster IBM MQ . Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

Pensando a dove le applicazioni utente e i processi amministrativi interni saranno localizzati in anticipo, molti problemi possono essere evitati o ridotti in un secondo momento. Questo argomento contiene informazioni sulle decisioni di progettazione che possono migliorare le prestazioni e semplificare le attività di manutenzione in base alla scalabilità del cluster.

- “Prestazioni dell'infrastruttura di clustering” a pagina 45
- “Repository completi” a pagina 46
- “Le applicazioni devono utilizzare code su repository completi?” a pagina 47
- “Gestione delle definizioni di canale” a pagina 47
- “Bilanciamento del carico di lavoro su più canali” a pagina 48

Prestazioni dell'infrastruttura di clustering

Quando un'applicazione tenta di aprire una coda su un gestore code in un cluster, il gestore code registra il proprio interesse con i repository completi per tale coda in modo che possa scoprire dove si trova la coda nel cluster. Gli aggiornamenti alla posizione o alla configurazione della coda vengono inviati automaticamente dai repository completi al gestore code interessato. Questa registrazione di interesse è nota internamente come sottoscrizione (queste sottoscrizioni non sono le stesse di IBM MQ sottoscrizioni utilizzate per la messaggistica di pubblicazione / sottoscrizione in IBM MQ)

Tutte le informazioni su un cluster passano attraverso ogni repository completo. I repository completi vengono quindi sempre utilizzati in un cluster per il traffico di messaggi di gestione. L'elevato utilizzo delle risorse di sistema durante la gestione di queste sottoscrizioni e la loro trasmissione e i messaggi di configurazione risultanti, possono causare un carico considerevole sull'infrastruttura di cluster. Ci sono un certo numero di cose da considerare quando si assicura che questo carico sia compreso e minimizzato dove possibile:

- Maggiore è il numero di singoli gestori code che utilizzano una coda cluster, maggiore è il numero di sottoscrizioni nel sistema e, di conseguenza, maggiore è il sovraccarico di gestione quando si verificano le modifiche e i sottoscrittori interessati devono essere notificati, in particolare sui gestori code del repository completo. Un modo per ridurre il traffico non necessario e il carico del repository completo consiste nel collegare applicazioni simili (ovvero, quelle che gestiscono le stesse code) a un minor numero di gestori code.
- Oltre al numero di sottoscrizioni nel sistema che influiscono sulle prestazioni, la velocità di modifica nella configurazione degli oggetti cluster può influire sulle prestazioni, ad esempio la modifica frequente di una configurazione della coda cluster.
- Quando un gestore code è un membro di più cluster (ovvero, fa parte di un sistema cluster sovrapposto) qualsiasi interesse in una coda risulta in una sottoscrizione per ogni cluster di cui è membro, anche se gli stessi gestori code sono repository completi per più di uno dei cluster. Questa disposizione aumenta il carico sul sistema ed è uno dei motivi per considerare se sono necessari più cluster sovrapposti, piuttosto che un singolo cluster.
- Il traffico dei messaggi dell'applicazione (ossia i messaggi inviati dalle applicazioni IBM MQ alle code cluster) non passa attraverso i repository completi per raggiungere i gestori code di destinazione. Il traffico di questo messaggio viene inviato direttamente tra il gestore code in cui il messaggio entra nel cluster e il gestore code in cui si trova la coda del cluster. Non è pertanto necessario adattare le elevate frequenze del traffico dei messaggi dell'applicazione rispetto ai gestori code del repository completo, a meno che i gestori code del repository completo non siano uno dei due gestori code menzionati. Per questo motivo, si consiglia di non utilizzare i gestori code del repository completo per il traffico di messaggi dell'applicazione nei cluster in cui il carico dell'infrastruttura di cluster è significativo.

Repository completi

Un repository è una raccolta di informazioni sui gestori code che sono membri di un cluster. Un gestore code che ospita una serie completa di informazioni su ogni gestore code nel cluster ha un repository completo. Per ulteriori informazioni sui repository completi e parziali, consultare Repository del cluster.

I repository completi devono essere conservati su server affidabili e il più possibile disponibili e devono essere evitati i singoli punti di errore. La progettazione cluster deve sempre avere due repository completi. Se si verifica un errore di un repository completo, il cluster può ancora funzionare.

I dettagli di tutti gli aggiornamenti alle risorse del cluster effettuati da un gestore code in un cluster; ad esempio, le code con cluster, vengono inviate da tale gestore code a due repository completi al massimo in tale cluster (o a uno se nel cluster è presente un solo gestore code del repository completo). Tali repository completi contengono le informazioni e le propagano a tutti i gestori code nel cluster che mostrano un interesse per tali informazioni (ovvero, sottoscrivono le informazioni). Per garantire che ciascun membro del cluster abbia una vista aggiornata delle risorse del cluster, ciascun gestore code deve essere in grado di comunicare con almeno un gestore code del repository completo alla volta.

Se, per qualsiasi motivo, un gestore code non riesce a comunicare con repository completi, può continuare a funzionare nel cluster in base al livello di informazioni già memorizzato nella cache per un periodo di tempo, ma non sono disponibili nuovi aggiornamenti o accessi a risorse cluster precedentemente inutilizzate.

Per questo motivo, è necessario mantenere i due repository completi disponibili in ogni momento. Tuttavia, questa disposizione non significa che debbano essere prese misure estreme perché il cluster funziona adeguatamente per un breve periodo senza un repository completo.

Esiste un altro motivo per cui un cluster deve avere due gestori code del repository completi, diversi dalla disponibilità delle informazioni del cluster: questo motivo è per garantire che le informazioni del cluster contenute nella cache del repository completo esistano in due posizioni per scopi di ripristino. Se è presente un solo repository completo e perde le informazioni sul cluster, è necessario l'intervento manuale su tutti i gestori code all'interno del cluster per far funzionare nuovamente il cluster. Se ci sono due repository completi, tuttavia, poiché le informazioni vengono sempre pubblicate e sottoscritte da due repository completi, il repository completo non riuscito può essere recuperato con il minimo sforzo.

- È possibile eseguire la manutenzione su gestori code di repository completi in una progettazione di due cluster di repository completi senza impattare gli utenti di tale cluster: il cluster continua a funzionare con un solo repository, quindi, se possibile, disattivare i repository, applicare la manutenzione ed eseguire nuovamente il backup uno alla volta. Anche se si verifica un'interruzione sul secondo repository completo, le applicazioni in esecuzione rimangono inalterate per un minimo di tre giorni.
- A meno che non vi sia un buon motivo per utilizzare un terzo repository, ad esempio utilizzare un repository completo geograficamente locale per motivi geografici, utilizzare la progettazione di due repository. Avere tre repository completi significa che non si sa mai quali sono i due attualmente in uso e potrebbero esserci problemi di gestione causati dalle interazioni tra più parametri di gestione del carico di lavoro. Non è consigliabile avere più di due repository completi.
- Se hai ancora bisogno di una migliore disponibilità, considera di ospitare i gestori code del repository completo come gestori code a più istanze o di utilizzare il supporto di alta disponibilità specifico della piattaforma per migliorarne la disponibilità.
- È necessario collegare completamente tutti i gestori code del repository completo con canali mittenti del cluster definiti manualmente. È necessario prestare particolare attenzione quando il cluster ha, per qualche ragione giustificabile, più di due repository completi. In questa situazione è spesso possibile perdere uno o più canali e non essere immediatamente evidenti. Quando l'interconnessione completa non si verifica, spesso si verificano problemi difficili da diagnosticare. Sono difficili da diagnosticare perché alcuni repository completi non contengono tutti i dati del repository e, di conseguenza, i gestori code nel cluster hanno viste diverse del cluster a seconda dei repository completi a cui si connettono.

Le applicazioni devono utilizzare code su repository completi?

Un repository completo è nella maggior parte dei modi esattamente come qualsiasi altro gestore code, ed è quindi possibile ospitare le code dell'applicazione sul repository completo e connettere le applicazioni direttamente a questi gestori code. Le applicazioni devono utilizzare code su repository completi?

La risposta comunemente accettata è "No?". Sebbene questa configurazione sia possibile, molti clienti preferiscono mantenere questi gestori code dedicati alla gestione della cache del cluster del repository completo. I punti da considerare quando si decide su una delle due opzioni sono descritti qui, ma in definitiva l'architettura del cluster deve essere appropriata alle particolari esigenze dell'ambiente.

- Aggiornamenti: di solito, per poter utilizzare le nuove funzioni del cluster nelle nuove release di IBM MQ , è necessario aggiornare prima i gestori code del repository completo di tale cluster. Quando un'applicazione nel cluster desidera utilizzare nuove funzioni, potrebbe essere utile essere in grado di aggiornare i repository completi (e alcuni sottoinsiemi di repository parziali) senza eseguire il test di un certo numero di applicazioni co - ubicate.
- Manutenzione: in modo simile se è necessario applicare la manutenzione urgente ai repository completi, è possibile riavviarli o aggiornarli con il comando **REFRESH** senza toccare le applicazioni.
- Prestazioni: man mano che i cluster crescono e le richieste di manutenzione della cache del cluster del repository completo diventano maggiori, mantenere separate le applicazioni riduce il rischio che ciò influisca sulle prestazioni dell'applicazione attraverso il conflitto per le risorse di sistema.
- Requisiti hardware: in genere, i repository completi non devono essere potenti; ad esempio, un server UNIX semplice con una buona aspettativa di disponibilità è sufficiente. In alternativa, per cluster molto grandi o in continuo cambiamento, è necessario considerare le prestazioni del computer repository completo.
- Requisiti software: i requisiti sono di solito il motivo principale per cui si sceglie di ospitare le code dell'applicazione su un repository completo. In un cluster di piccole dimensioni, la collocazione potrebbe significare un requisito per un minor numero di gestori code / server su tutti.

Gestione delle definizioni di canale

Anche all'interno di un singolo cluster, possono esistere più definizioni di canale che forniscono più instradamenti tra due gestori code.

A volte c'è un vantaggio nell'avere canali paralleli all'interno di un singolo cluster, ma questa decisione di progettazione deve essere considerata a fondo; a parte l'aggiunta di complessità, questa progettazione

potrebbe risultare in un sottoutilizzo dei canali che riduce le prestazioni. Questa situazione si verifica perché il test di solito implica l'invio di molti messaggi a una velocità costante, quindi i canali paralleli sono completamente utilizzati. Ma con le condizioni reali di un flusso di messaggi non costante, l'algoritmo di bilanciamento del carico di lavoro causa il calo delle prestazioni quando il flusso di messaggi viene commutato da canale a canale.

Quando un gestore code è un membro di più cluster, esiste l'opzione di utilizzare una singola definizione di canale con un elenco nomi cluster, piuttosto che definire un canale CLUSRCVR separato per ciascun cluster. Tuttavia, questa configurazione può causare difficoltà di amministrazione in un secondo momento; considerare, ad esempio, il caso in cui TLS deve essere applicato a un cluster ma non a un secondo. È pertanto preferibile creare definizioni separate e la convenzione di denominazione suggerita in "Convenzioni di denominazione cluster" a pagina 35 lo supporta.

Bilanciamento del carico di lavoro su più canali

Queste informazioni sono intese come una comprensione avanzata del soggetto. Per la spiegazione di base di questo argomento (che deve essere compresa prima di utilizzare le informazioni qui), consultare Utilizzo dei cluster per la gestione del carico di lavoro, Bilanciamento del carico di lavoro in clustere L'algoritmo di gestione del carico di lavoro del cluster.

L'algoritmo di gestione del carico di lavoro del cluster fornisce una grande serie di strumenti, ma non tutti devono essere utilizzati l'uno con l'altro senza comprendere appieno come funzionano e interagiscono. Potrebbe non essere immediatamente ovvio quanto siano importanti i canali per il processo di bilanciamento del carico di lavoro: l'algoritmo round - robin di gestione del carico di lavoro si comporta come se più canali cluster per un gestore code che possiede una coda cluster, fossero considerati come più istanze di quella coda. Questo processo è spiegato in modo più dettagliato nel seguente esempio:

1. Esistono due gestori code che ospitano una coda in un cluster: QM1 e QM2.
2. Esistono cinque canali riceventi del cluster per QM1.
3. Esiste solo un canale ricevente del cluster per QM2.
4. Quando **MQPUT** o **MQOPEN** on QM3 sceglie un'istanza, l'algoritmo è cinque volte più probabile che invii il messaggio a QM1 che a QM2.
5. La situazione nel passo 4 si verifica perché l'algoritmo visualizza sei opzioni tra cui scegliere (5 + 1) e round-robins tra tutti e cinque i canali in QM1 e il singolo canale in QM2.

Un altro comportamento sottile è che anche quando si inseriscono i messaggi in una coda con cluster che ha un'istanza configurata sul gestore code locale, IBM MQ utilizza lo stato del canale ricevente del cluster locale per decidere se i messaggi devono essere inseriti nell'istanza locale della coda o nelle istanze remote della coda. In questo scenario:

1. Quando si inseriscono i messaggi, l'algoritmo di gestione del carico di lavoro non esamina le singole code cluster, ma i canali cluster che possono raggiungere tali destinazioni.
2. Per raggiungere le destinazioni locali, i canali riceventi locali sono inclusi in questo elenco (anche se non vengono utilizzati per inviare il messaggio).
3. Quando un canale ricevente locale viene arrestato, l'algoritmo di gestione del carico di lavoro preferisce un'istanza alternativa per impostazione predefinita se il relativo CLUSRCVR non viene arrestato. Se esistono più istanze CLUSRCVR locali per la destinazione e almeno una non è arrestata, l'istanza locale rimane idonea.

Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster
È possibile isolare i flussi di messaggi tra gestori code in un cluster. È possibile inserire i messaggi trasportati da canali mittenti del cluster differenti in code di trasmissione cluster differenti. È possibile utilizzare l'approccio in un singolo cluster o con cluster sovrapposti. L'argomento fornisce esempi e alcune procedure ottimali per guidare l'utente nella scelta di un approccio da utilizzare.

Quando si distribuisce un'applicazione, è possibile scegliere quali risorse IBM MQ condividere con altre applicazioni e quali non condividere. Esistono diversi tipi di risorse che possono essere condivise, le principali sono il server stesso, il gestore code, i canali e le code. È possibile scegliere di configurare

le applicazioni con meno risorse condivise; allocando code, canali, gestori code o anche server separati a singole applicazioni. In questo caso, la configurazione generale del sistema diventa più grande e complessa. L'utilizzo dei cluster IBM MQ riduce la complessità di gestione di più server, gestori code, code e canali, ma introduce un'altra risorsa condivisa, la coda di trasmissione cluster, SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Figura 12 a pagina 50 è una sezione di una grande distribuzione IBM MQ che illustra il significato della condivisione SYSTEM.CLUSTER.TRANSMIT.QUEUE. Nel diagramma, l'applicazione, Client App, è connessa al gestore code QM2 nel cluster CL1. Un messaggio da Client App viene elaborato dall'applicazione, Server App. Il messaggio viene richiamato da Server App dalla coda cluster Q1 sul gestore code QM3 in CLUSTER2. Poiché le applicazioni client e server non sono nello stesso cluster, il messaggio viene trasferito dal gestore code del gateway QM1.

Il modo normale per configurare un gateway del cluster consiste nel rendere il gestore code del gateway membro di tutti i cluster. Sul gestore code del gateway sono definite code alias cluster per le code cluster in tutti i cluster. Gli alias della coda cluster sono disponibili in tutti i cluster. I messaggi inseriti negli alias della coda cluster vengono instradati tramite il gestore code del gateway alla loro destinazione corretta. Il gestore code del gateway inserisce i messaggi inviati alle code alias del cluster in SYSTEM.CLUSTER.TRANSMIT.QUEUE su QM1comune.

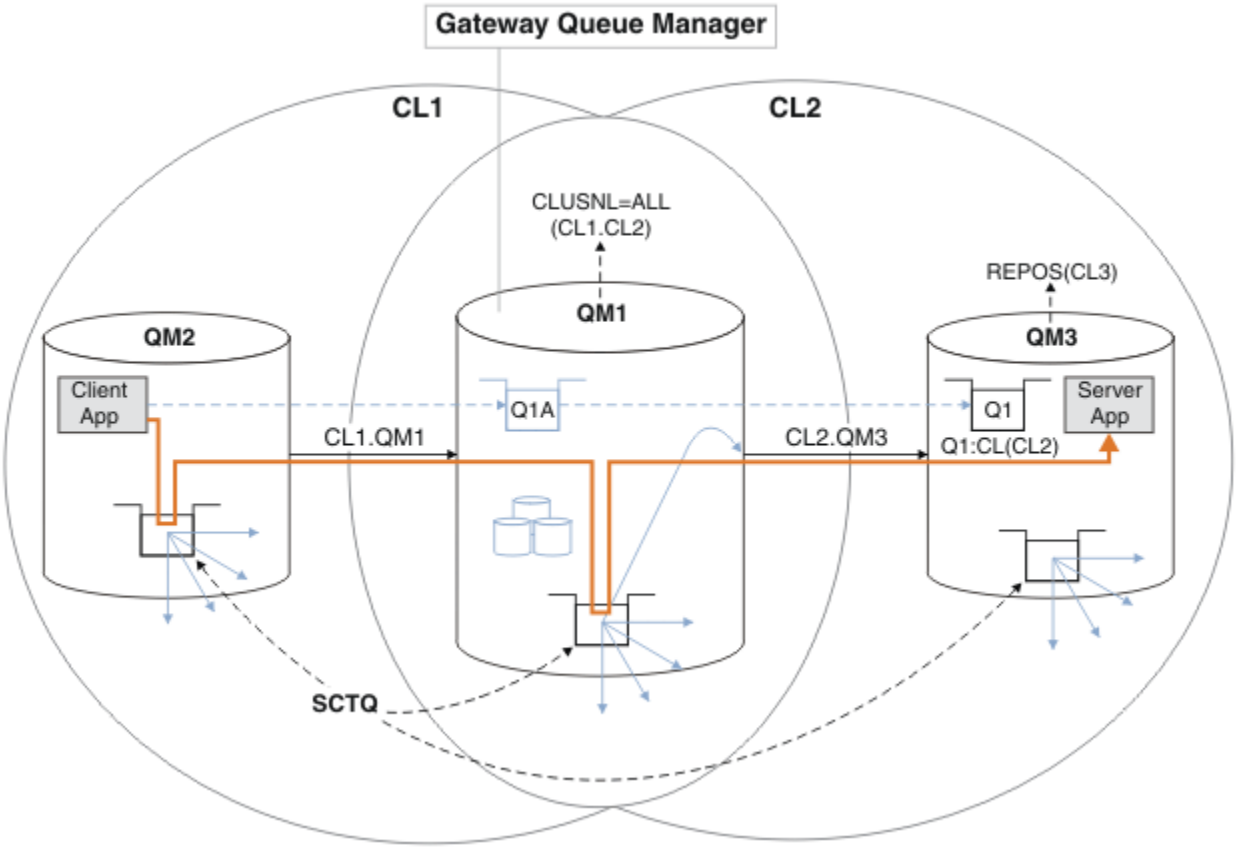
L'architettura hub e spoke richiede tutti i messaggi tra i cluster per passare attraverso il gestore code del gateway. Il risultato è che tutti i messaggi passano attraverso la singola coda di trasmissione del cluster su QM1, SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Dal punto di vista delle prestazioni, una coda singola non è un problema. Una coda di trasmissione comune generalmente non rappresenta un collo di bottiglia delle prestazioni. La velocità di trasmissione dei messaggi sul gateway è in gran parte determinata dalle prestazioni dei canali che si collegano ad esso. La velocità di trasmissione non è generalmente influenzata dal numero di code o dal numero di messaggi sulle code che utilizzano i canali.

Da altre prospettive, l'utilizzo di una singola coda di trasmissione per più applicazioni presenta degli inconvenienti:

- Non è possibile isolare il flusso di messaggi in una destinazione dal flusso di messaggi in un'altra. Non è possibile separare la memoria dei messaggi prima che vengano inoltrati, anche se le destinazioni si trovano in cluster differenti su gestori code differenti.

  Se una destinazione cluster diventa non disponibile, i messaggi per tale destinazione si accumulano nella singola coda di trasmissione e alla fine i messaggi la riempiono. Una volta che la coda di trasmissione è piena, interrompe l'inserimento dei messaggi nella coda di trasmissione per qualsiasi destinazione cluster.
- Non è facile monitorare il trasferimento dei messaggi a diverse destinazioni cluster. Tutti i messaggi sono sulla singola coda di trasmissione. La visualizzazione della profondità della coda di trasmissione fornisce poche indicazioni se i messaggi vengono trasferiti a tutte le destinazioni.



Nota: Le frecce in Figura 12 a pagina 50 e nelle figure seguenti sono di diversi tipi. Le frecce continue rappresentano flussi di messaggi. Le etichette sulle frecce continue sono nomi di canali di messaggi. Le frecce piene grigie sono potenziali flussi di messaggi da SYSTEM.CLUSTER.TRANSMIT.QUEUE sui canali mittente del cluster. Le linee tratteggiate nere collegano le etichette ai loro obiettivi. Le frecce tratteggiate grigie sono riferimenti, ad esempio da una MQOPEN chiamata di `Client` App alla definizione della coda alias del cluster Q1A.

Figura 12. Applicazione client-server distribuita all'architettura hub e spoke utilizzando i cluster IBM MQ

In Figura 12 a pagina 50, i client di `Server` App aprono la coda Q1A. I messaggi vengono collocati in SYSTEM.CLUSTER.TRANSMIT.QUEUE su QM2, trasferiti in SYSTEM.CLUSTER.TRANSMIT.QUEUE su QM1e quindi trasferiti in Q1 su QM3, dove vengono ricevuti dall'applicazione `Server` App .

Il messaggio da `Client` App passa attraverso code di trasmissione del cluster di sistemi su QM2 e QM1. In Figura 12 a pagina 50, l'obiettivo è isolare il flusso di messaggi sul gestore code del gateway dall'applicazione client, in modo che i messaggi non siano memorizzati in SYSTEM.CLUSTER.TRANSMIT.QUEUE. È possibile isolare i flussi su qualsiasi altro gestore code con cluster. È anche possibile isolare i flussi nell'altra direzione, di nuovo al client. Per mantenere brevi le descrizioni delle soluzioni, le descrizioni considerano solo un singolo flusso dall'applicazione client.

Soluzioni per isolare il traffico di messaggi del cluster su un gestore code del gateway cluster

Un modo per risolvere il problema consiste nell'utilizzare gli alias del gestore code o le definizioni di coda remota per collegare i cluster. Creare una definizione di coda remota con cluster, una coda di trasmissione e un canale, per separare ciascun flusso di messaggi sul gestore code del gateway; consultare Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway.

A partire da IBM WebSphere MQ 7.5 , i gestori code cluster non sono limitati a una singola coda di trasmissione cluster. Sono disponibili due opzioni:

1. Definire manualmente ulteriori code di trasmissione cluster e definire quali canali mittenti del cluster trasferiscono i messaggi da ciascuna coda di trasmissione; consultare Aggiunta di una coda di trasmissione cluster per isolare il traffico dei messaggi cluster inviati da un gestore code gateway.
2. Consente al gestore code di creare e gestire automaticamente ulteriori code di trasmissione cluster. Definisce una diversa coda di trasmissione cluster per ogni canale mittente del cluster; consultare Modifica del valore predefinito per separare le code di trasmissione cluster per isolare il traffico messaggi.

È possibile combinare manualmente le code di trasmissione del cluster definite per alcuni canali mittente del cluster con il gestore code che gestisce il resto. La combinazione di code di trasmissione è l'approccio utilizzato in Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code del gateway. In questa soluzione, la maggior parte dei messaggi tra i cluster utilizza il comune `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Un'applicazione è critica e tutti i suoi flussi di messaggi sono isolati da altri flussi utilizzando una coda di trasmissione cluster definita manualmente.

La configurazione in Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway è limitata. Non separa il traffico di messaggi diretto a una coda cluster sullo stesso gestore code nello stesso cluster di un'altra coda cluster. È possibile separare il traffico di messaggi in code individuali utilizzando le definizioni di code remote che fanno parte dell'accodamento distribuito. Con i cluster, utilizzando più code di trasmissione cluster, è possibile separare il traffico dei messaggi che va a canali mittenti del cluster differenti. Più code del cluster nello stesso cluster, sullo stesso gestore code, condividono un canale mittente del cluster. I messaggi per tali code vengono memorizzati nella stessa coda di trasmissione, prima di essere inoltrati dal gestore code gateway. Nella configurazione in Aggiunta di un cluster e di una coda di trasmissione del cluster per isolare il traffico di messaggi del cluster inviato da un gestore code del gateway, la limitazione viene annullata aggiungendo un altro cluster e rendendo il gestore code e la coda del cluster membri del nuovo cluster. Il nuovo gestore code potrebbe essere l'unico gestore code nel cluster. È possibile aggiungere più gestori code al cluster e utilizzare lo stesso cluster per isolare anche le code cluster su tali gestori code.

Concetti correlati

“Controllo accessi e code di trasmissione di più cluster” a pagina 30
Scegliere tra tre modalità di controllo quando un'applicazione inserisce i messaggi nelle code cluster remote. Le modalità sono la verifica in remoto rispetto alla coda del cluster, la verifica in locale rispetto a `SYSTEM.CLUSTER.TRANSMIT.QUEUE`o la verifica rispetto ai profili locali per la coda del cluster o il gestore code del cluster.

Utilizzo delle code di trasmissione del cluster e dei canali mittente del cluster

“Cluster sovrapposti” a pagina 37
I cluster sovrapposti forniscono ulteriori funzioni di gestione. Utilizzare gli elenchi nomi per ridurre il numero di comandi necessari per gestire i cluster che si sovrappongono.

Attività correlate

Autorizzazione all'inserimento di messaggi nelle code del cluster remoto

Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway

Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway

Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway

Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi

Creazione di cluster a due sovrapposizioni con un gestore code del gateway

Configurazione dei percorsi dei messaggi tra cluster

Protezione

Riferimenti correlati

setmqaut

Clustering: pianificazione della configurazione delle code di trasmissione del cluster
L'utente viene guidato nelle scelte delle code di trasmissione cluster. È possibile configurare una coda predefinita comune, code predefinite separate o code definite manualmente.

Prima di iniziare

Consultare “Come scegliere quale tipo di coda di trasmissione del cluster utilizzare” a pagina 54.

Informazioni su questa attività

Sono disponibili alcune scelte da effettuare quando si pianifica come configurare un gestore code per selezionare una coda di trasmissione cluster.

1. Qual è la coda di trasmissione cluster predefinita per i trasferimenti di messaggi cluster?
   a. Una coda di trasmissione cluster comune, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.
   b. Separare le code di trasmissione cluster. Il gestore code gestisce le code di trasmissione cluster separate. Le crea come code dinamiche permanenti dalla coda modello, `SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE`. Crea una coda di trasmissione cluster per ogni canale mittente del cluster che utilizza.
2. Per le code di trasmissione del cluster che si decide di creare manualmente, sono disponibili altre due opzioni:
   a. Definire una coda di trasmissione separata per ogni canale mittente del cluster che si decide di configurare manualmente. In questo caso, impostare l'attributo della coda **CLCHNAME** della coda di trasmissione sul nome di un canale mittente del cluster. Selezionare il canale mittente del cluster che deve trasferire i messaggi da questa coda di trasmissione.
   b. Combinare il traffico dei messaggi per un gruppo di canali mittente del cluster sulla stessa coda di trasmissione del cluster; consultare Figura 13 a pagina 53. In questo caso, impostare l'attributo della coda **CLCHNAME** di ogni coda di trasmissione comune su un nome canale mittente del cluster generico. Un nome canale mittente del cluster generico è un filtro per raggruppare i nomi canale mittente del cluster. Ad esempio, `SALES.*` raggruppa tutti i canali mittente del cluster che hanno nomi che iniziano con `SALES.`. È possibile inserire più caratteri jolly ovunque nella stringa filtro. Il carattere jolly è un asterisco, "`*`". Rappresenta da zero a qualsiasi numero di caratteri.

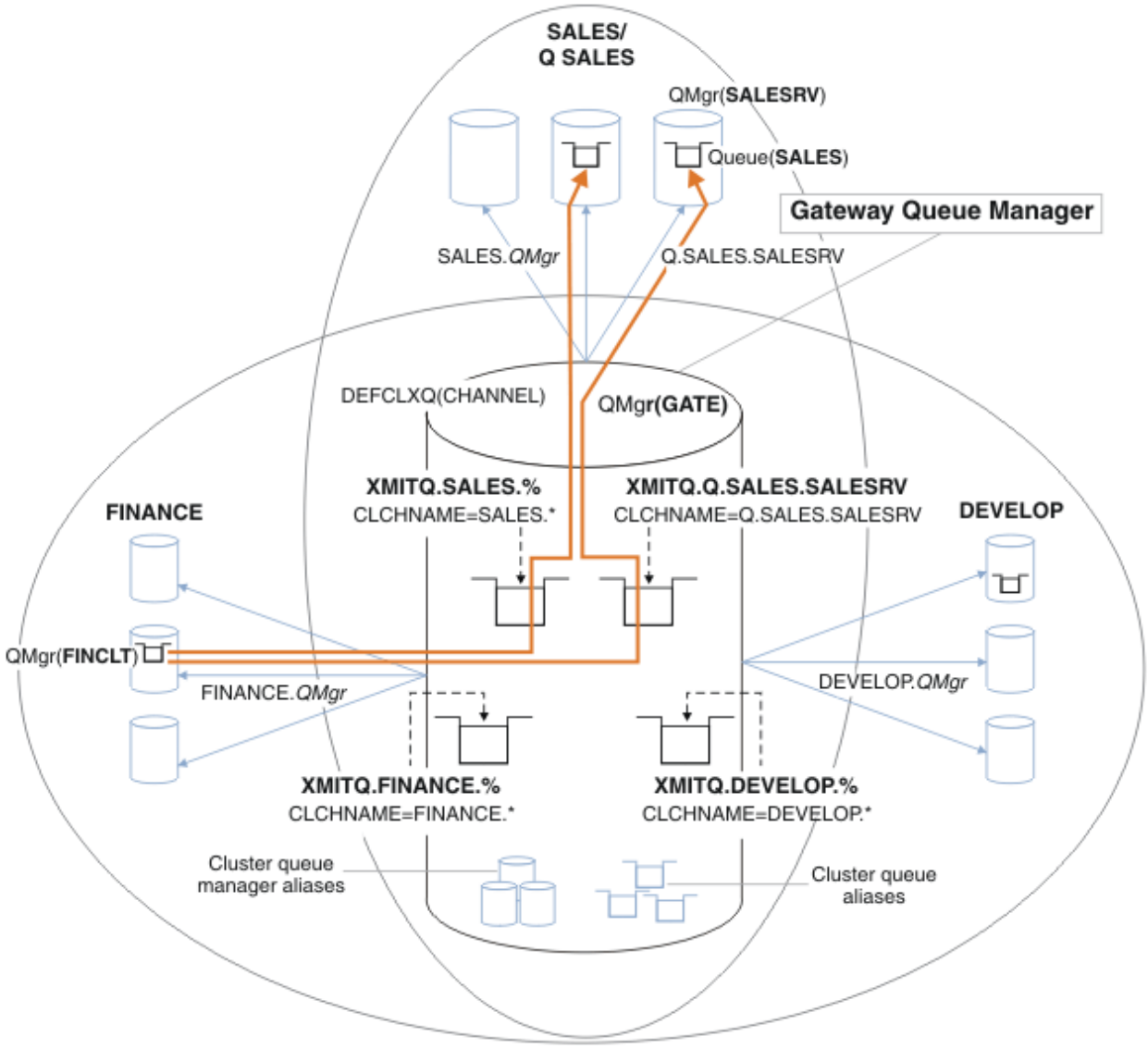


Figura 13. Esempio di code di trasmissione specifiche per cluster IBM MQ dipartimentali differenti

Procedura

1. Selezionare il tipo di coda di trasmissione cluster predefinita da utilizzare.
   - Scegliere una singola coda di trasmissione cluster o separare le code per ogni connessione cluster.

   Lasciare l'impostazione predefinita o eseguire il comando **MQSC** :

   ```
   ALTER QMGR DEFCLXQ(CHANNEL)
   ```
2. Isolare i flussi di messaggi che non devono condividere una coda di trasmissione cluster con altri flussi.
   - Consultare “Clustering: configurazione di esempio di più code di trasmissione cluster” a pagina 56. Nell'esempio, la coda SALES , che deve essere isolata, è un membro del cluster SALES , su SALESRV. Per isolare la coda SALES , creare un nuovo cluster `Q.SALES`, rendere membro il gestore code SALESRV e modificare la coda SALES in modo che appartenga a `Q.SALES`.
   - I gestori code che inviano messaggi a SALES devono essere anche membri del nuovo cluster. Se si utilizza un alias della coda del cluster e un gestore code del gateway, come nell'esempio, in molti casi è possibile limitare le modifiche per rendere il gestore code del gateway membro del nuovo cluster.

- Tuttavia, la separazione dei flussi dal gateway alla destinazione non separa i flussi al gateway dal gestore code di origine. Ma a volte risulta essere sufficiente per separare i flussi dal gateway e non i flussi verso il gateway. Se non è sufficiente, aggiungere il gestore code di origine nel nuovo cluster. Se si desidera che i messaggi passino attraverso il gateway, spostare l'alias del cluster sul nuovo cluster e continuare a inviare i messaggi all'alias del cluster sul gateway e non direttamente al gestore code di destinazione.

Seguire questa procedura per isolare i flussi di messaggi:

a) Configurare le destinazioni dei flussi in modo tale che ciascuna coda di destinazione sia l'unica coda in un cluster specifico su tale gestore code.

b) Creare i canali mittente e ricevente del cluster per tutti i nuovi cluster creati in base a una convenzione di denominazione sistematica.

- Consultare “Clustering: considerazioni speciali per i cluster che si sovrappongono” a pagina 44.

c) Definire una coda di trasmissione cluster per ogni destinazione isolata su ogni gestore code che invia messaggi alla coda di destinazione.

- Una convenzione di denominazione per le code di trasmissione del cluster consiste nell'utilizzare il valore dell'attributo del nome del canale cluster, `CLCHNAME`, con prefisso `XMITQ.`

3. Creare code di trasmissione del cluster per soddisfare i requisiti di governance o di controllo.

- I tipici requisiti di governance e di monitoraggio risultano in una coda di trasmissione per cluster o in una coda di trasmissione per gestore code. Se si segue la convenzione di denominazione per i canali cluster, *`ClusterName.  QueueManagerName`*, è semplice creare nomi di canali generici che selezionino un cluster di gestori code o tutti i cluster di cui è membro un gestore code; consultare “Clustering: configurazione di esempio di più code di trasmissione cluster” a pagina 56.
- Estendere la convenzione di denominazione per le code di trasmissione del cluster per soddisfare i nomi di canale generici, sostituendo il simbolo asterisco con un segno di percentuale. Ad esempio:

```
DEFINE QLOCAL(XMITQ.SALES.%) USAGE(XMITQ) CLCHNAME(SALES.*)
```

Concetti correlati

Utilizzo delle code di trasmissione del cluster e dei canali mittente del cluster

“Controllo accessi e code di trasmissione di più cluster” a pagina 30

Scegliere tra tre modalità di controllo quando un'applicazione inserisce i messaggi nelle code cluster remote. Le modalità sono la verifica in remoto rispetto alla coda del cluster, la verifica in locale rispetto a `SYSTEM.CLUSTER.TRANSMIT.QUEUE`o la verifica rispetto ai profili locali per la coda del cluster o il gestore code del cluster.

“Cluster sovrapposti” a pagina 37

I cluster sovrapposti forniscono ulteriori funzioni di gestione. Utilizzare gli elenchi nomi per ridurre il numero di comandi necessari per gestire i cluster che si sovrappongono.

Attività correlate

Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway

Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway

Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway

Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi

Creazione di cluster a due sovrapposizioni con un gestore code del gateway

Configurazione dei percorsi dei messaggi tra cluster

Come scegliere quale tipo di coda di trasmissione del cluster utilizzare

Come scegliere tra diverse opzioni di configurazione della coda di trasmissione del cluster.

È possibile scegliere quale coda di trasmissione cluster è associata a un canale mittente del cluster.

1. È possibile avere tutti i canali mittenti del cluster associati alla singola coda di trasmissione del cluster predefinita, SYSTEM.CLUSTER.TRANSMIT.QUEUE; questa è l'opzione predefinita.
2. È possibile impostare tutti i canali mittenti del cluster in modo che vengano associati automaticamente a una coda di trasmissione cluster separata. Le code vengono create dal gestore code dalla coda modello SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE e denominate SYSTEM.CLUSTER.TRANSMIT.*ChannelName*. I canali utilizzeranno la relativa coda di trasmissione cluster con nome univoco se l'attributo del gestore code **DEFCLXQ** è impostato su CHANNEL.
3. È possibile impostare canali mittenti del cluster specifici che devono essere serviti da una singola coda di trasmissione del cluster. Selezionare questa opzione creando una coda di trasmissione e impostandone il relativo attributo **CLCHNAME** sul nome del canale mittente del cluster.
4. È possibile selezionare gruppi di canali mittente del cluster che devono essere serviti da una singola coda di trasmissione del cluster. Selezionare questa opzione creando una coda di trasmissione e impostando l'attributo **CLCHNAME** su un nome canale generico, come *ClusterName*.*. Se si denominano i canali del cluster seguendo le convenzioni di denominazione in "Clustering: considerazioni speciali per i cluster che si sovrappongono" a pagina 44, questo nome seleziona tutti i canali del cluster connessi ai gestori code nel cluster *ClusterName*.

È possibile combinare una delle opzioni predefinite della coda di trasmissione del cluster per alcuni canali mittente del cluster con un numero qualsiasi di configurazioni specifiche e generiche della coda di trasmissione del cluster.

Best practice

Nella maggior parte dei casi, per le installazioni esistenti di IBM MQ , la configurazione predefinita è la scelta migliore. Un gestore code del cluster memorizza i messaggi cluster su una singola coda di trasmissione cluster, SYSTEM.CLUSTER.TRANSMIT.QUEUE. È possibile modificare il valore predefinito per memorizzare i messaggi per diversi gestori code e cluster su code di trasmissione separate oppure definire le proprie code di trasmissione.

Nella maggior parte dei casi, per le nuove installazioni di IBM MQ , la configurazione predefinita è anche la scelta migliore. Il processo di passaggio dalla configurazione predefinita al valore predefinito alternativo di avere una coda di trasmissione per ogni canale mittente del cluster è automatico. Anche il ritorno è automatico. La scelta dell'uno o dell'altro non è critica, si può invertire.

Il motivo per scegliere una configurazione diversa è più relativo alla governance e alla gestione che alla funzionalità o alle prestazioni. Con un paio di eccezioni, la configurazione di più code di trasmissione cluster non avvantaggia il comportamento del gestore code. Risulta in un numero maggiore di code e richiede la modifica delle procedure di monitoraggio e gestione già impostate che fanno riferimento alla singola coda di trasmissione. Questo è il motivo per cui, a conti fatti, rimanere con la configurazione predefinita è la scelta migliore, a meno che non si abbiano forti ragioni di governance o di gestione per una scelta diversa.

Le eccezioni sono entrambe relative a ciò che accade se il numero di messaggi memorizzati su SYSTEM.CLUSTER.TRANSMIT.QUEUE aumenta. Se si esegue ogni passo per separare i messaggi per una destinazione dai messaggi per un'altra destinazione, i problemi di canale e di consegna con una destinazione non dovrebbero influire sulla consegna ad un'altra destinazione. Tuttavia, il numero di messaggi memorizzati su SYSTEM.CLUSTER.TRANSMIT.QUEUE può aumentare a causa della mancata consegna dei messaggi abbastanza rapida a una destinazione. Il numero di messaggi su SYSTEM.CLUSTER.TRANSMIT.QUEUE per una destinazione può influire sulla consegna dei messaggi ad altre destinazioni.

Per evitare problemi derivanti dal riempimento di una singola coda di trasmissione, è necessario creare una capacità sufficiente nella configurazione. Quindi, se una destinazione non riesce e un backlog di messaggi inizia a crescere, hai tempo per risolvere il problema.

Se i messaggi vengono instradati tramite un gestore code hub, come un gateway cluster, condividono una coda di trasmissione comune, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Se il numero di messaggi memorizzati su SYSTEM.CLUSTER.TRANSMIT.QUEUE sul gestore code del gateway raggiunge la profondità massima, il gestore code inizia a rifiutare i nuovi messaggi per la coda di trasmissione fino a quando la profondità non si riduce. La congestione influisce sui messaggi per tutte le destinazioni

instradati attraverso il gateway. I messaggi eseguono il backup delle code di trasmissione di altri gestori code che inviano messaggi al gateway. Il problema si manifesta nei messaggi scritti nei log degli errori del gestore code, con un calo della velocità di trasmissione dei messaggi e tempi più lunghi tra l'invio di un messaggio e il momento in cui un messaggio arriva a destinazione.

L'effetto della congestione su una singola coda di trasmissione può diventare evidente, anche prima che sia piena. Se si dispone di un traffico di messaggi misto, con alcuni messaggi non persistenti di grandi dimensioni e alcuni messaggi di piccole dimensioni, il tempo di consegna dei messaggi di piccole dimensioni aumenta man mano che la coda di trasmissione si riempie. Il ritardo è dovuto alla scrittura di messaggi non persistenti di grandi dimensioni su disco che normalmente non vengono scritti su disco. Se si dispone di flussi di messaggi critici per il tempo, che condividono una coda di trasmissione cluster con altri flussi di messaggi misti, potrebbe essere utile configurare un percorso di messaggi speciale per isolarlo da altri flussi di messaggi; consultare Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviato da un gestore code gateway.

Gli altri motivi per configurare code di trasmissione cluster separate sono per soddisfare i requisiti di governance o per semplificare i messaggi di monitoraggio inviati a destinazioni cluster differenti. Ad esempio, potrebbe essere necessario dimostrare che i messaggi per una destinazione non condividono mai una coda di trasmissione con i messaggi per un'altra destinazione.

Modificare l'attributo del gestore code **DEFCLXQ** che controlla la coda di trasmissione cluster predefinita, per creare code di trasmissione cluster differenti per ogni canale mittente del cluster. Più destinazioni possono condividere un canale mittente del cluster, quindi devi pianificare i tuoi cluster per soddisfare pienamente questo obiettivo. Applicare sistematicamente il metodo Aggiunta di un cluster e di una coda di trasmissione del cluster per isolare il traffico di messaggi del cluster inviati da un gestore code del gateway a tutte le code del cluster. Il risultato che si desidera ottenere è che nessuna destinazione cluster condivida un canale mittente del cluster con un'altra destinazione cluster. Di conseguenza, nessun messaggio per una destinazione cluster condivide la propria coda di trasmissione cluster con un messaggio per un'altra destinazione.

La creazione di una coda di trasmissione cluster separata per un flusso di messaggi specifico rende più semplice il monitoraggio del flusso di messaggi verso tale destinazione. Per utilizzare una nuova coda di trasmissione cluster, definire la coda, associarla a un canale mittente del cluster e arrestare e avviare il canale. La modifica non deve essere permanente. È possibile isolare un flusso di messaggi per un certo periodo di tempo, per monitorare la coda di trasmissione e tornare quindi a utilizzare nuovamente la coda di trasmissione predefinita.

Attività correlate

Clustering: configurazione di esempio di più code di trasmissione cluster
In questa attività si applicano le operazioni per pianificare più code di trasmissione del cluster a tre cluster sovrapposti. I requisiti sono di separare i flussi di messaggi in una coda cluster, da tutti gli altri flussi di messaggi e di memorizzare i messaggi per cluster differenti su code di trasmissione cluster differenti.

Clustering: commutazione delle code di trasmissione del cluster
Pianificare come rendere effettive le modifiche alle code di trasmissione del cluster di un gestore code di produzione esistente.

Clustering: configurazione di esempio di più code di trasmissione cluster
In questa attività si applicano le operazioni per pianificare più code di trasmissione del cluster a tre cluster sovrapposti. I requisiti sono di separare i flussi di messaggi in una coda cluster, da tutti gli altri flussi di messaggi e di memorizzare i messaggi per cluster differenti su code di trasmissione cluster differenti.

Informazioni su questa attività

I passi in questa attività mostrano come applicare la procedura in “Clustering: pianificazione della configurazione delle code di trasmissione del cluster” a pagina 52 e arrivare alla configurazione mostrata in Figura 14 a pagina 57. È un esempio di tre cluster sovrapposti, con un gestore code del gateway, configurato con code di trasmissione del cluster separate. I comandi MQSC per definire i cluster sono descritti in “Creazione dei cluster di esempio” a pagina 59.

Ad esempio, ci sono due requisiti. Uno è separare il flusso di messaggi dal gestore code del gateway all'applicazione di vendita che registra le vendite. Il secondo è quello di interrogare quanti messaggi sono in attesa di essere inviati a diverse aree dipartimentali in qualsiasi momento. I cluster SALES, FINANCEe DEVELOP sono già definiti. I messaggi cluster vengono attualmente inoltrati da SYSTEM.CLUSTER.TRANSMIT.QUEUE.

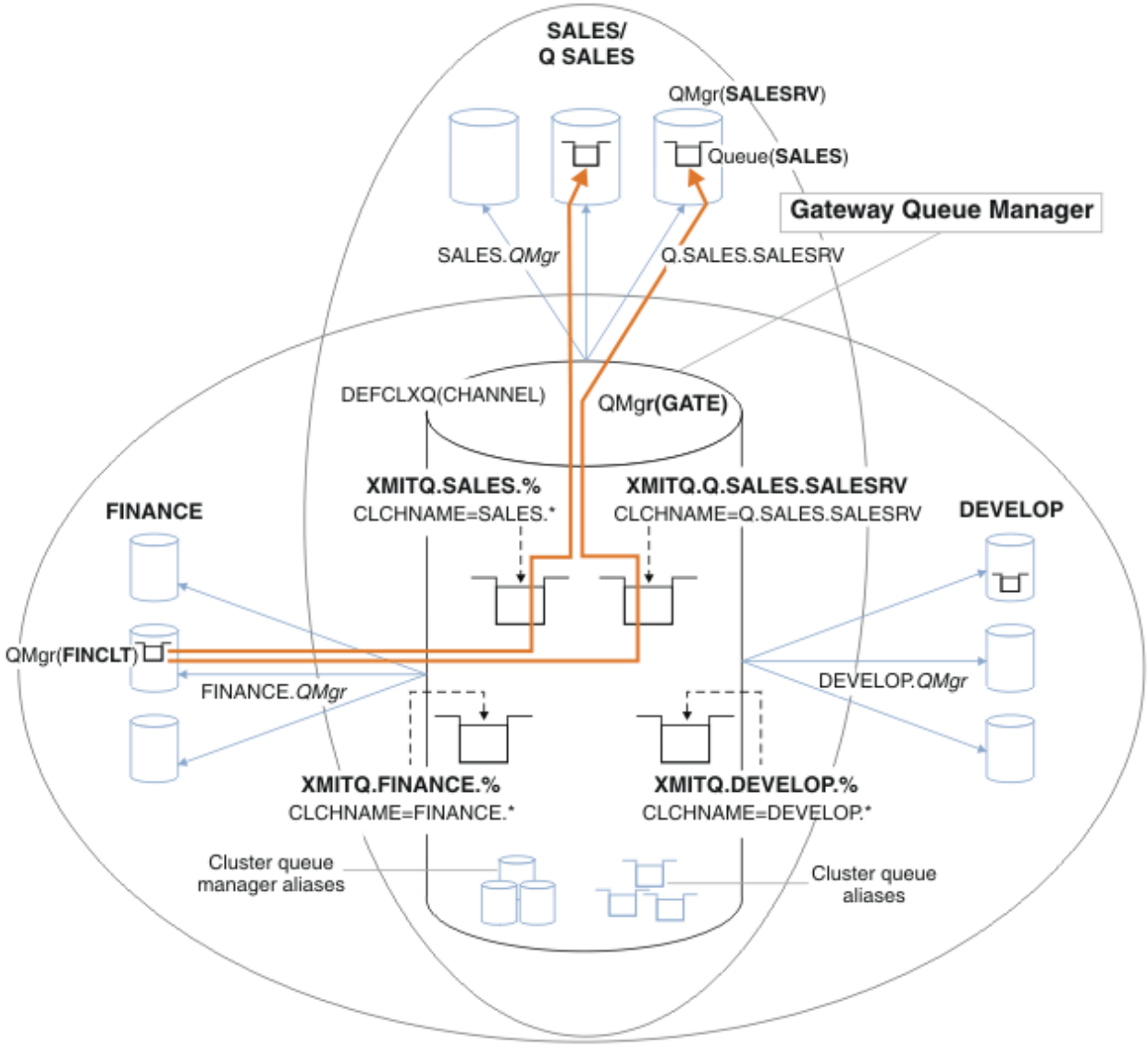


Figura 14. Esempio di code di trasmissione specifiche per cluster IBM MQ dipartimentali differenti

I passi per modificare i cluster sono i seguenti. Per le definizioni, vedi Modifiche per isolare la coda di vendite in un nuovo cluster e separare le code di trasmissione cluster gateway.

Procedura

1. Il primo passo di configurazione è " Selezionare il tipo di coda di trasmissione cluster predefinita da utilizzare ".

   La decisione è di creare code di trasmissione del cluster predefinite separate eseguendo il seguente comando **MQSC** sul gestore code GATE .

   ```
   ALTER QMGR DEFCLXQ(CHANNEL)
   ```

   Non esiste un motivo valido per scegliere questo valore predefinito, poiché l'intento è definire manualmente le code di trasmissione cluster. La scelta ha un valore diagnostico debole. Se una

definizione manuale viene eseguita in modo non corretto e un messaggio scorre in una coda di trasmissione del cluster predefinita, viene visualizzato nella creazione di una coda di trasmissione del cluster dinamica permanente.

2. Il secondo passo di configurazione è " Isolare i flussi di messaggi che non devono condividere una coda di trasmissione cluster con altri flussi ".

   In questo caso, l'applicazione di vendita che riceve i messaggi dalla coda SALES su SALESRV richiede isolamento. È richiesto solo l'isolamento dei messaggi dal gestore code del gateway. Le tre fasi secondarie sono:

   a) " Configurare le destinazioni dei flussi in modo tale che ciascuna coda di destinazione sia l'unica coda in un cluster specifico su tale gestore code ".

      L'esempio richiede l'aggiunta di un gestore code SALESRV a un nuovo cluster all'interno del reparto vendite. Se si hanno poche code che richiedono l'isolamento, è possibile decidere di creare un cluster specifico per la coda SALES . Una convenzione di denominazione possibile per il nome del cluster consiste nel denominare tali cluster, `Q. QueueName`, ad esempio `Q.SALES`. Un approccio alternativo, che potrebbe essere più pratico se si dispone di un numero elevato di code da isolare, consiste nel creare cluster di code isolate dove e quando necessario. I nomi dei cluster potrebbero essere `QUEUES. n`.

      Nell'esempio, il nuovo cluster è denominato `Q.SALES`. Per aggiungere il nuovo cluster, vedere le definizioni in Modifiche per isolare la coda di vendita in un nuovo cluster e separare le code di trasmissione cluster gateway. Il riepilogo delle modifiche di definizione è il seguente:

      i) Aggiungere `Q.SALES` all'elenco nomi dei cluster sui gestori code del repository. Si fa riferimento all'elenco nomi nel parametro **REPOSNL** del gestore code.

      ii) Aggiungere `Q.SALES` all'elenco dei nomi dei cluster sul gestore code gateway. Si fa riferimento all'elenco nomi in tutte le definizioni alias della coda cluster e alias del gestore code cluster sul gestore code del gateway.

      iii) Creare un elenco nomi sul gestore code SALESRV, per entrambi i cluster di cui è membro e modificare l'appartenenza del cluster della coda SALES :

      ```
      DEFINE NAMELIST(CLUSTERS) NAMES(SALES, Q.SALES) REPLACE
      ALTER QLOCAL(SALES) CLUSTER(' ') CLUSNL(SALESRV.CLUSTERS)
      ```

      La coda SALES è un membro di entrambi i cluster, solo per la transizione. Una volta eseguita la nuova configurazione, si rimuove la coda SALES dal cluster SALES ; consultare Figura 15 a pagina 62.

   b) " Creare i canali mittente e ricevente del cluster per tutti i nuovi cluster creati in base a una convenzione di denominazione sistematica ".

      i) Aggiungere il canale ricevente del cluster `Q.SALES. RepositoryQMgr` a ciascuno dei gestori code del repository

      ii) Aggiungere il canale mittente del cluster `Q.SALES. OtherRepositoryQMgr` a ciascuno dei gestori code del repository, per connettersi all'altro gestore repository. Avviare questi canali.

      iii) Aggiungere i canali riceventi del cluster `Q.SALES.SALESRV`e `Q.SALES.GATE` a uno dei gestori code del repository in esecuzione.

      iv) Aggiungere i canali mittente del cluster `Q.SALES.SALESRV`e `Q.SALES.GATE` ai gestori code SALESRV e GATE . Connetti il canale mittente del cluster al gestore code del repository su cui hai creato i canali riceventi del cluster.

   c) " Definire una coda di trasmissione cluster per ogni destinazione isolata su ogni gestore code che invia messaggi alla coda di destinazione ".

      Sul gestore code del gateway definire la coda di trasmissione del cluster `XMITQ.Q.SALES.SALESRV` per il canale mittente del cluster `Q.SALES.SALESRV` :

      ```
      DEFINE QLOCAL(XMITQ.Q.SALES.SALESRV) USAGE(XMITQ) CLCHNAME(Q.SALES.SALESRV) REPLACE
      ```

3. Il terzo passo di configurazione è " Creare code di trasmissione del cluster per soddisfare i requisiti di governance o di controllo ".

   Sul gestore code gateway definire le code di trasmissione del cluster:

```
DEFINE QLOCAL(XMITQ.SALES)  USAGE(XMITQ) CLCHNAME(SALES.*)  REPLACE
DEFINE QLOCAL(XMITQ.DEVELOP) USAGE(XMITQ) CLCHNAME(DEVELOP.*) REPLACE
DEFINE QLOCAL(XMITQ.FINANCE) USAGE(XMITQ) CLCHNAME(SALES.*)  REPLACE
```

Operazioni successive

Passare alla nuova configurazione sul gestore code gateway.

Lo switch viene attivato avviando i nuovi canali e riavviando i canali che ora sono associati a code di trasmissione differenti. In alternativa, è possibile arrestare e avviare il gestore code gateway.

1. Arrestare i canali seguenti sul gestore code gateway:

```
SALES. Qmgr
DEVELOP. Qmgr
FINANCE. Qmgr
```

2. Avviare i canali seguenti sul gestore code del gateway:

```
SALES. Qmgr
DEVELOP. Qmgr
FINANCE. Qmgr
Q.SALES.SAVESRV
```

Una volta completata la commutazione, rimuovere la coda SALES dal cluster SALES ; consultare Figura 15 a pagina 62.

Concetti correlati

Come scegliere quale tipo di coda di trasmissione del cluster utilizzare
Come scegliere tra diverse opzioni di configurazione della coda di trasmissione del cluster.

Attività correlate

Clustering: commutazione delle code di trasmissione del cluster
Pianificare come rendere effettive le modifiche alle code di trasmissione del cluster di un gestore code di produzione esistente.

Creazione dei cluster di esempio
Le definizioni e istruzioni per creare il cluster di esempio e modificarlo per isolare la coda SALES e separare i messaggi sul gestore code del gateway.

Informazioni su questa attività

I comandi **MQSC** completi per creare i cluster FINANCE, SALESe Q.SALES sono forniti in Definizioni per i cluster di base, Modifiche per isolare la coda di vendita in un nuovo cluster e separare le code di trasmissione del cluster gatewaye Rimuovi la coda di vendita sul gestore code SALESRV dal cluster di vendita. Il cluster DEVELOP viene omesso dalle definizioni, per mantenerle più brevi.

Procedura

1. Creare i cluster SALES e FINANCE e il gestore code del gateway.
   a) Creare i gestori code.

      Eseguire il comando: `crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE` *QmgrName* per ciascuno dei nomi gestore code in Tabella 4 a pagina 60.

Tabella 4. Nomi di gestori code e numeri di porta		
Descrizione	**Nome del gestore code**	**Numero di porta**
Repository finanziario	FINR1	1414
Repository finanziario	FINR2	1415
Cliente finanziario	FINCLT	1418
Archivio vendite	SALER1	1416
Archivio vendite	SALER2	1417
Server di vendita	SALESRV	1419
Gateway	GATE	1420

b) Avvia tutti i gestori code

Eseguire il comando: `strmqm` *QmgrName* per ciascuno dei nomi gestore code in Tabella 4 a pagina 60.

c) Creare le definizioni per ciascuno dei gestori code

Eseguire il seguente comando: `runmqsc` *QmgrName* < *filename* dove i file sono elencati in Definizioni per i cluster di basee il nome file corrisponde al nome del gestore code.

Definizioni per i cluster di base

finr1.txt

```
DEFINE LISTENER(1414) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1414) REPLACE
START LISTENER(1414)
ALTER QMGR REPOS(FINANCE)
DEFINE CHANNEL(FINANCE.FINR2) CHLTYPE(CLUSSDR) CONNAME('localhost(1415)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(FINANCE.FINR1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1414)')
CLUSTER(FINANCE) REPLACE
```

finr2.txt

```
DEFINE LISTENER(1415) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1415) REPLACE
START LISTENER(1415)
ALTER QMGR REPOS(FINANCE)
DEFINE CHANNEL(FINANCE.FINR1) CHLTYPE(CLUSSDR) CONNAME('localhost(1414)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(FINANCE.FINR2) CHLTYPE(CLUSRCVR) CONNAME('localhost(1415)')
CLUSTER(FINANCE) REPLACE
```

finclt.txt

```
DEFINE LISTENER(1418) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1418) REPLACE
START LISTENER(1418)
DEFINE CHANNEL(FINANCE.FINR1) CHLTYPE(CLUSSDR)  CONNAME('localhost(1414)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(FINANCE.FINCLT) CHLTYPE(CLUSRCVR) CONNAME('localhost(1418)')
CLUSTER(FINANCE) REPLACE
DEFINE QMODEL(SYSTEM.SAMPLE.REPLY) REPLACE
```

saler1.txt

```
DEFINE LISTENER(1416) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1416) REPLACE
START LISTENER(1416)
ALTER QMGR REPOS(SALES)
DEFINE CHANNEL(SALES.SALER2) CHLTYPE(CLUSSDR) CONNAME('localhost(1417)')
CLUSTER(SALES) REPLACE
DEFINE CHANNEL(SALES.SALER1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1416)')
CLUSTER(SALES) REPLACE
```

saler2.txt

```
DEFINE LISTENER(1417) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1417) REPLACE
START LISTENER(1417)
ALTER QMGR REPOS(SALES)
DEFINE CHANNEL(SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('localhost(1416)')
CLUSTER(SALES) REPLACE
DEFINE CHANNEL(SALES.SALER2) CHLTYPE(CLUSRCVR) CONNAME('localhost(1417)')
CLUSTER(SALES) REPLACE
```

salesrv.txt

```
DEFINE LISTENER(1419) TRPTYPE(TCP) IPADDR(localhost) CONTROL(QMGR) PORT(1419) REPLACE
START LISTENER(1419)
DEFINE CHANNEL(SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('localhost(1416)')
CLUSTER(SALES) REPLACE
DEFINE CHANNEL(SALES.SALESRV) CHLTYPE(CLUSRCVR) CONNAME('localhost(1419)')
CLUSTER(SALES) REPLACE
DEFINE QLOCAL(SALES) CLUSTER(SALES) TRIGGER INITQ(SYSTEM.DEFAULT.INITIATION.QUEUE)
PROCESS(ECHO) REPLACE
DEFINE PROCESS(ECHO) APPLICID(AMQSECH) REPLACE
```

gate.txt

```
DEFINE LISTENER(1420) TRPTYPE(TCP) IPADDR(LOCALHOST) CONTROL(QMGR) PORT(1420) REPLACE
START LISTENER(1420)
DEFINE NAMELIST(ALL) NAMES(SALES, FINANCE)
DEFINE CHANNEL(FINANCE.FINR1) CHLTYPE(CLUSSDR) CONNAME('LOCALHOST(1414)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(FINANCE.GATE) CHLTYPE(CLUSRCVR) CONNAME('LOCALHOST(1420)')
CLUSTER(FINANCE) REPLACE
DEFINE CHANNEL(SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('LOCALHOST(1416)')
CLUSTER(SALES) REPLACE
DEFINE CHANNEL(SALES.GATE)  CHLTYPE(CLUSRCVR) CONNAME('LOCALHOST(1420)')
CLUSTER(SALES) REPLACE
DEFINE QALIAS(A.SALES) CLUSNL(ALL) TARGET(SALES) TARGTYPE(QUEUE) DEFBIND(NOTFIXED)
REPLACE
DEFINE QREMOTE(FINCLT) RNAME(' ') RQMNAME(FINCLT) CLUSNL(ALL) REPLACE
DEFINE QREMOTE(SALESRV) RNAME(' ') RQMNAME(SALESRV) CLUSNL(ALL) REPLACE
```

2. Verificare la configurazione eseguendo il programma di richiesta di esempio.
   a) Avviare il programma di controllo dei trigger sul gestore code SALESRV

      Su Windows, aprire una finestra di comandi ed eseguire il comando `runmqtrm -m SALESRV`

   b) Eseguire il programma di richiesta di esempio e inviare una richiesta.

      Su Windows, aprire una finestra di comandi ed eseguire il comando `amqsreq A.SALES FINCLT`

      Il messaggio di richiesta viene ripetuto e dopo 15 secondi il programma di esempio termina.
3. Creare le definizioni per isolare la coda SALES nel cluster `Q.SALES` e separare i messaggi cluster per il cluster SALES e FINANCE nel gestore code gateway.

   Eseguire il comando: `runmqsc` *QmgrName* < *filename* dove i file sono elencati nel seguente elenco e il nome file quasi corrisponde al nome del gestore code.

   Modifiche per isolare la coda di vendita in un nuovo cluster e separare le code di trasmissione del cluster gateway
   chgsaler1.txt

```
DEFINE NAMELIST(CLUSTERS) NAMES(SALES, Q.SALES)
ALTER QMGR REPOS(' ') REPOSNL(CLUSTERS)
DEFINE CHANNEL(Q.SALES.SALER2) CHLTYPE(CLUSSDR) CONNAME('localhost(1417)')
CLUSTER(Q.SALES) REPLACE
DEFINE CHANNEL(Q.SALES.SALER1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1416)')
CLUSTER(Q.SALES) REPLACE
```

   chgsaler2.txt

```
DEFINE NAMELIST(CLUSTERS) NAMES(SALES, Q.SALES)
ALTER QMGR REPOS(' ') REPOSNL(CLUSTERS)
DEFINE CHANNEL(Q.SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('localhost(1416)')
CLUSTER(Q.SALES) REPLACE
```

```
DEFINE CHANNEL(Q.SALES.SALER2) CHLTYPE(CLUSRCVR) CONNAME('localhost(1417)')
CLUSTER(Q.SALES) REPLACE
```

chgsalesrv.txt

```
DEFINE NAMELIST (CLUSTERS) NAMES(SALES, Q.SALES)
DEFINE CHANNEL(Q.SALES.SALER1) CHLTYPE(CLUSSDR) CONNAME('localhost(1416)')
CLUSTER(Q.SALES) REPLACE
DEFINE CHANNEL(Q.SALES.SAVESRV) CHLTYPE(CLUSRCVR) CONNAME('localhost(1419)')
CLUSTER(Q.SALES) REPLACE
ALTER QLOCAL (SALES) CLUSTER(' ') CLUSNL(CLUSTERS)
```

chggate.txt

```
ALTER NAMELIST(ALL) NAMES(SALES, FINANCE, Q.SALES)
ALTER QMGR DEFCLXQ(CHANNEL)
DEFINE CHANNEL(Q.SALES.SALER1) CHLTYPE(CLUSSDR)  CONNAME('localhost(1416)')
CLUSTER(Q.SALES) REPLACE
DEFINE CHANNEL(Q.SALES.GATE)  CHLTYPE(CLUSRCVR) CONNAME('localhost(1420)')
CLUSTER(Q.SALES) REPLACE
DEFINE QLOCAL (XMITQ.Q.SALES.SALESRV) USAGE(XMITQ) CLCHNAME(Q.SALES.SALESRV) REPLACE
DEFINE QLOCAL (XMITQ.SALES)     USAGE(XMITQ) CLCHNAME(SALES.*)  REPLACE
DEFINE QLOCAL (XMITQ.FINANCE)    USAGE(XMITQ) CLCHNAME(FINANCE.*) REPLACE
```

4. Rimuovere la coda SALES dal cluster SALES .

   Eseguire il comando **MQSC** in Figura 15 a pagina 62:

   ```
   ALTER QLOCAL(SALES) CLUSTER('Q.SALES') CLUSNL(' ')
   ```

   Figura 15. Rimuovere la coda delle vendite sul gestore code SALESRV dal cluster delle vendite

5. Passare i canali alle nuove code di trasmissione.

   Il requisito è quello di arrestare e avviare tutti i canali utilizzati dal gestore code GATE . Per eseguire questa operazione con un numero minimo di comandi, arrestare e avviare il gestore code

   ```
   endmqm -i GATE
   strmqm GATE
   ```

Operazioni successive

1. Eseguire di nuovo il programma di richiesta di esempio per verificare il funzionamento della nuova configurazione; consultare il passo “2” a pagina 61
2. Monitorare i messaggi che passano attraverso tutte le code di trasmissione del cluster sul gestore code GATE :
   a. Modificare la definizione di ciascuna delle code di trasmissione del cluster per attivare il controllo della coda.

      ```
      ALTER QLOCAL(SYSTEM.CLUSTER.TRANSMIT.
      name) STATQ(ON)
      ```

   b. Controllare che il monitoraggio delle statistiche del gestore code sia OFF, per ridurre al minimo l'output e impostare l'intervallo di controllo su un valore inferiore per eseguire comodamente più verifiche.

      ```
      ALTER QMGR STATINT(60) STATCHL(OFF) STATQ(OFF) STATMQI(OFF) STATACLS(OFF)
      ```

   c. Riavviare il gestore code GATE .
   d. Eseguire il programma di richiesta di esempio alcune volte per verificare che un numero uguale di messaggi stia passando attraverso SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SALESRV e SYSTEM.CLUSTER.TRANSMIT.QUEUE. Le richieste passano attraverso SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SALESRV e le risposte attraverso SYSTEM.CLUSTER.TRANSMIT.QUEUE.

      ```
      amqsmon -m GATE -t statistics
      ```

e. I risultati su un paio di intervalli sono i seguenti:

```
C:\Documents and Settings\Admin>amqsmon -m GATE -t statistics
MonitoringType: QueueStatistics
QueueManager: 'GATE'
IntervalStartDate: '2012-02-27'
IntervalStartTime: '14.59.20'
IntervalEndDate: '2012-02-27'
IntervalEndTime: '15.00.20'
CommandLevel: 700
ObjectCount: 2
QueueStatistics: 0
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.QUEUE'
CreateDate: '2012-02-24'
CreateTime: '15.58.15'
...
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [435, 0]
GetCount: [1, 0]
GetBytes: [435, 0]
...
QueueStatistics: 1
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV'
CreateDate: '2012-02-24'
CreateTime: '16.37.43'
...
PutCount: [1, 0]
PutFailCount: 0
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [435, 0]
GetCount: [1, 0]
GetBytes: [435, 0]
...
MonitoringType: QueueStatistics
QueueManager: 'GATE'
IntervalStartDate: '2012-02-27'
IntervalStartTime: '15.00.20'
IntervalEndDate: '2012-02-27'
IntervalEndTime: '15.01.20'
CommandLevel: 700
ObjectCount: 2
QueueStatistics: 0
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.QUEUE'
CreateDate: '2012-02-24'
CreateTime: '15.58.15'
...
PutCount: [2, 0]
PutFailCount: 0
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [863, 0]
GetCount: [2, 0]
GetBytes: [863, 0]
...
```

```
QueueStatistics: 1
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV'
CreateDate: '2012-02-24'
CreateTime: '16.37.43'
...
PutCount: [2, 0]
PutFailCount: 0
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [863, 0]
GetCount: [2, 0]
GetBytes: [863, 0]
...
2 Records Processed.
```

Un messaggio di richiesta e risposta è stato inviato nel primo intervallo e due nel secondo. È possibile dedurre che i messaggi di richiesta sono stati collocati in `SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV`e i messaggi di risposta in `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Clustering: commutazione delle code di trasmissione del cluster
Pianificare come rendere effettive le modifiche alle code di trasmissione del cluster di un gestore code di produzione esistente.

Prima di iniziare

Se si riduce il numero di messaggi che il processo di commutazione deve trasferire alla nuova coda di trasmissione, la commutazione viene completata più rapidamente. Leggere Modalità di funzionamento del processo di commutazione del canale mittente del cluster in una coda di trasmissione differente per i motivi per cui si tenta di svuotare la coda di trasmissione prima di procedere ulteriormente.

Informazioni su questa attività

È possibile scegliere tra due modi per rendere effettive le modifiche alle code di trasmissione del cluster.

1. Consentire al gestore code di apportare le modifiche automaticamente. Questa è l'opzione predefinita. Il gestore code commuta i canali mittente del cluster con modifiche della coda di trasmissione in sospeso al successivo avvio di un canale mittente del cluster.
2. Apportare le modifiche manualmente. È possibile apportare le modifiche ad un canale mittente del cluster quando viene arrestato. È possibile passare da una coda di trasmissione cluster ad un'altra prima dell'avvio del canale mittente del cluster.

Quali fattori vengono presi in considerazione quando si decide quale delle due opzioni scegliere e come gestire l'interruttore?

Procedura

- Opzione 1: consentire al gestore code di apportare le modifiche automaticamente; consultare “Commutazione dei canali mittenti del cluster attivi in un'altra serie di code di trasmissione cluster” a pagina 66.

  Scegliere questa opzione se si desidera che il gestore code effettui lo switch.

  Un modo alternativo per descrivere questa opzione consiste nel dire che il gestore code commuta un canale mittente del cluster senza forzare l'arresto del canale. Hai la possibilità di forzare l'arresto del canale, e quindi avviare il canale, per fare in modo che lo switch avvenga prima. Lo switch viene avviato all'avvio del canale e viene eseguito mentre il canale è in esecuzione, il che è diverso dall'opzione 2. Nell'opzione 2, l'interruttore si verifica quando il canale viene arrestato.

Se si sceglie questa opzione consentendo allo switch di verificarsi automaticamente, il processo di commutazione inizia all'avvio di un canale mittente del cluster. Se il canale non è arrestato, viene avviato dopo che diventa inattivo, se è presente un messaggio da elaborare. Se il canale è arrestato, avviarlo con il comando START CHANNEL .

Il processo di commutazione viene completato non appena non rimangono messaggi per il canale mittente del cluster sulla coda di trasmissione che il canale stava servendo. Non appena questo è il caso, i messaggi appena arrivati per il canale mittente del cluster vengono memorizzati direttamente sulla nuova coda di trasmissione. Fino ad allora, i messaggi vengono memorizzati nella vecchia coda di trasmissione e il processo di commutazione trasferisce i messaggi dalla vecchia coda di trasmissione alla nuova coda di trasmissione. Il canale mittente del cluster inoltra i messaggi dalla nuova coda di trasmissione del cluster durante l'intero processo di commutazione.

Quando il processo di commutazione viene completato dipende dallo stato del sistema. Se si stanno apportando modifiche in una finestra di manutenzione, valutare in anticipo se il processo di commutazione verrà completato in tempo. Il completamento in tempo dipende dal fatto che il numero di messaggi in attesa di trasferimento dalla vecchia coda di trasmissione raggiunga o meno lo zero.

Il vantaggio del primo metodo è che è automatico. Uno svantaggio è che, se il tempo per apportare le modifiche alla configurazione è limitato a una finestra di manutenzione, è necessario essere certi di poter controllare il sistema per completare il processo di commutazione all'interno della finestra di manutenzione. Se non si è sicuri, l'opzione 2 potrebbe essere una scelta migliore.

- Opzione 2: apportare le modifiche manualmente; vedere “Commutazione di un canale mittente del cluster arrestato ad un'altra coda di trasmissione del cluster” a pagina 67.

  Scegliere questa opzione se si desidera controllare l'intero processo di commutazione manualmente o se si desidera commutare un canale arrestato o inattivo. È una buona scelta, se si stanno commutando alcuni canali mittente del cluster e si desidera eseguire lo switch durante una finestra di manutenzione.

  Una descrizione alternativa di questa opzione consiste nel commutare il canale mittente del cluster, mentre il canale mittente del cluster viene arrestato.

  Se si sceglie questa opzione, si ha il controllo completo quando si verifica l'interruttore.

  È possibile essere certi di completare il processo di commutazione in un periodo di tempo fisso, all'interno di una finestra di manutenzione. Il tempo impiegato dallo switch dipende dal numero di messaggi che devono essere trasferiti da una coda di trasmissione all'altra. Se i messaggi continuano ad arrivare, potrebbe essere necessario del tempo prima che il processo trasferisca tutti i messaggi.

  È possibile commutare il canale senza trasferire i messaggi dalla vecchia coda di trasmissione. Lo switch è "istantaneo".

  Quando si riavvia il canale mittente del cluster, inizia l'elaborazione dei messaggi sulla coda di trasmissione appena assegnata ad esso.

  Il vantaggio del secondo metodo è che si ha il controllo sul processo di commutazione. Lo svantaggio è che è necessario identificare i canali mittente del cluster da commutare, eseguire i comandi necessari e risolvere i canali in dubbio che potrebbero impedire l'arresto del canale mittente del cluster.

Concetti correlati

Come scegliere quale tipo di coda di trasmissione del cluster utilizzare
Come scegliere tra diverse opzioni di configurazione della coda di trasmissione del cluster.

Come funziona il processo di commutazione del canale mittente del cluster in una coda di trasmissione differente

Attività correlate

Clustering: configurazione di esempio di più code di trasmissione cluster
In questa attività si applicano le operazioni per pianificare più code di trasmissione del cluster a tre cluster sovrapposti. I requisiti sono di separare i flussi di messaggi in una coda cluster, da tutti gli altri flussi di messaggi e di memorizzare i messaggi per cluster differenti su code di trasmissione cluster differenti.

Commutazione dei canali mittenti del cluster attivi in un'altra serie di code di trasmissione cluster
Questa attività fornisce tre opzioni per la commutazione dei canali mittenti del cluster attivi. Un'opzione consiste nel consentire al gestore code di effettuare lo switch automaticamente, il che non influisce sulle applicazioni in esecuzione. Le altre opzioni sono l'arresto e l'avvio manuale dei canali o il riavvio del gestore code.

Prima di iniziare

Modificare la configurazione della coda di trasmissione cluster. È possibile modificare l'attributo del gestore code **DEFCLXQ** oppure aggiungere o modificare l'attributo **CLCHNAME** delle code di trasmissione.

Se si riduce il numero di messaggi che il processo di commutazione deve trasferire alla nuova coda di trasmissione, la commutazione viene completata più rapidamente. Leggere Modalità di funzionamento del processo di commutazione del canale mittente del cluster in una coda di trasmissione differente per i motivi per cui si tenta di svuotare la coda di trasmissione prima di procedere ulteriormente.

Informazioni su questa attività

Utilizzare i passaggi dell'attivit ... come base per elaborare un proprio piano per apportare modifiche alla configurazione della coda di trasmissione cluster.

Procedura

1. Opzionale: Registra lo stato del canale corrente

   Registrare lo stato dei canali correnti e salvati che servono le code di trasmissione del cluster. I seguenti comandi visualizzano lo stato associato alle coda di trasmissione del cluster di sistema. Aggiungere i propri comandi per visualizzare lo stato associato alle code di trasmissione cluster definite. Utilizzare una convenzione, come ad esempio XMITQ. *ChannelName*, per denominare le code di trasmissione del cluster definite per semplificare la visualizzazione dello stato del canale per tali code di trasmissione.

   ```
   DISPLAY CHSTATUS(*) WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
   DISPLAY CHSTATUS(*) SAVED WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
   ```

2. Commutare le code di trasmissione.

   - Non eseguire alcuna azione. Il gestore code commuta i canali mittenti del cluster quando vengono riavviati dopo essere stati arrestati o inattivi.

     Scegliere questa opzione se non si hanno regole o dubbi sulla modifica di una configurazione del gestore code. Le applicazioni in esecuzione non sono influenzate dalle modifiche.
   - Riavviare il gestore code. Tutti i canali mittente del cluster vengono arrestati e riavviati automaticamente su richiesta.

     Scegliere questa opzione per avviare immediatamente tutte le modifiche. Le applicazioni in esecuzione vengono interrotte dal gestore code quando viene arrestato e riavviato.
   - Arrestare i singoli canali mittente del cluster e riavviarli.

     Scegliere questa opzione per modificare immediatamente alcuni canali. Le applicazioni in esecuzione riscontrano un breve ritardo nel trasferimento dei messaggi tra l'avvio e l'arresto del canale di messaggi. Il canale mittente del cluster rimane in esecuzione, tranne durante il periodo di tempo in cui è stato arrestato. Durante il processo di commutazione i messaggi vengono consegnati alla vecchia coda di trasmissione, trasferiti alla nuova coda di trasmissione dal processo di commutazione e inoltrati dalla nuova coda di trasmissione dal canale mittente del cluster.

3. Opzionale: Monitora i canali mentre cambiano

   Visualizzare lo stato del canale e la profondità della coda di trasmissione durante lo switch. Il seguente esempio visualizza lo stato delle code di trasmissione del cluster di sistema.

```
DISPLAY CHSTATUS(*) WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
DISPLAY CHSTATUS(*) SAVED WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
DISPLAY QUEUE('SYSTEM.CLUSTER.TRANSMIT.*') CURDEPTH
```

4. Opzionale: Monitorare i messaggi AMQ7341 `La coda di trasmissione per il canale` *`ChannelName`* `passato dalla coda` *`QueueName`* `a` *`QueueName`* scritti nel log degli errori del gestore code.

Commutazione di un canale mittente del cluster arrestato ad un'altra coda di trasmissione del cluster
Se si sceglie di apportare modifiche manualmente, si apportano le modifiche ad un canale mittente del cluster quando viene arrestato e si passa da una coda di trasmissione cluster ad un'altra prima dell'avvio del canale mittente del cluster.

Prima di iniziare

È possibile apportare alcune modifiche alla configurazione e ora si desidera renderle effettive senza avviare i canali mittenti del cluster interessati. In alternativa, effettuare le modifiche di configurazione richieste come una delle fasi dell'attività.

Se si riduce il numero di messaggi che il processo di commutazione deve trasferire alla nuova coda di trasmissione, la commutazione viene completata più rapidamente. Leggere Modalità di funzionamento del processo di commutazione del canale mittente del cluster in una coda di trasmissione differente per i motivi per cui si tenta di svuotare la coda di trasmissione prima di procedere ulteriormente.

Informazioni su questa attività

Questa attività commuta le code di trasmissione servite da canali mittenti del cluster arrestati o inattivi. È possibile eseguire questa attività perché un canale mittente del cluster è stato arrestato e si desidera commutarne immediatamente la coda di trasmissione. Ad esempio, per qualche motivo un canale mittente del cluster non è in fase di avvio o ha qualche altro problema di configurazione. Per risolvere il problema, si decide di creare un canale mittente del cluster e di associare la coda di trasmissione per il vecchio canale mittente del cluster al nuovo canale mittente del cluster definito.

Uno scenario più probabile è quello in cui si desidera controllare quando viene eseguita la riconfigurazione delle code di trasmissione del cluster. Per controllare completamente la riconfigurazione, arrestare i canali, modificare la configurazione e quindi commutare le code di trasmissione.

Procedura

1. Arrestare i canali che si intende commutare
   a) Arrestare tutti i canali in esecuzione o inattivi che si intende commutare. L'arresto di un canale mittente del cluster inattivo ne impedisce l'avvio mentre si stanno apportando modifiche alla configurazione.

   ```
   STOP CHANNEL(ChannelName) MODE(QUIESCE) STATUS(STOPPED)
   ```

2. Opzionale: Apportare le modifiche alla configurazione.

   Ad esempio, consultare “Clustering: configurazione di esempio di più code di trasmissione cluster” a pagina 56.
3. Passare i canali mittente del cluster alle nuove code di trasmissione del cluster.

   Multi Su Multipiattaforma, immettere il seguente comando:

   ```
   runswchl -m QmgrName -c ChannelName
   ```

   z/OS Su z/OS, utilizzare la funzione SWITCH del comando CSQUTIL per commutare i messaggi o monitorare ciò che accade. utilizzare il seguente comando.

   ```
   SWITCH CHANNEL(channel_name) MOVEMSGS(YES)
   ```

Per ulteriori informazioni, consultare Funzione SWITCH.

Il comando **runswchl**, o CSQUTIL SWITCH, trasferisce i messaggi sulla vecchia coda di trasmissione alla nuova coda di trasmissione. Quando il numero di messaggi sulla vecchia coda di trasmissione per questo canale raggiunge lo zero, lo switch viene completato. Il comando è sincrono. Il comando scrive i messaggi di avanzamento nella finestra durante il processo di commutazione.

Durante la fase di trasferimento, i messaggi nuovi ed esistenti destinati al canale mittente del cluster vengono trasferiti alla nuova coda di trasmissione.

Poiché il canale mittente del cluster è arrestato, i messaggi si accumulano nella nuova coda di trasmissione. Confrontare il canale mittente del cluster arrestato con il passo "2" a pagina 66 in "Commutazione dei canali mittenti del cluster attivi in un'altra serie di code di trasmissione cluster" a pagina 66. In questo passo, il canale mittente del cluster è in esecuzione, quindi i messaggi non si accumulano necessariamente sulla nuova coda di trasmissione.

4. Opzionale: Monitora i canali mentre cambiano

   In una finestra comandi differente, visualizzare la profondità della coda di trasmissione durante lo switch. Il seguente esempio visualizza lo stato delle code di trasmissione del cluster di sistema.

   ```
   DISPLAY QUEUE('SYSTEM.CLUSTER.TRANSMIT.*') CURDEPTH
   ```

5. Opzionale: Monitorare i messaggi AMQ7341 `La coda di trasmissione per il canale` *`ChannelName`* `passato dalla coda` *`QueueName`* `a` *`QueueName`* scritti nel log degli errori del gestore code.
6. Riavviare i canali mittenti del cluster arrestati.

   I canali non vengono avviati automaticamente, poiché sono stati arrestati e vengono inseriti nello stato ARRESTATO .

   ```
   START CHANNEL(ChannelName)
   ```

Riferimenti correlati

runswchl
Risolvi canale
Arresto canale

Clustering: procedure ottimali di migrazione e modifica
Questo argomento fornisce una guida per la pianificazione e la gestione dei cluster IBM MQ . Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

1. "Spostamento di oggetti in un cluster" a pagina 68 (Procedure ottimali per spostare gli oggetti all'interno di un cluster, senza installare fix pack o nuove versioni di IBM MQ).
2. "Aggiornamenti e installazioni di manutenzione" a pagina 70 (Procedure ottimali per mantenere attiva e in esecuzione un'architettura cluster funzionante, applicando la manutenzione o gli aggiornamenti e testando la nuova architettura).

Spostamento di oggetti in un cluster

Applicazioni e relative code

Quando è necessario spostare un'istanza della coda ospitata su un gestore code per essere ospitata su un altro gestore code, è possibile lavorare con i parametri di bilanciamento del carico di lavoro per garantire una transizione graduale.

Creare un'istanza della coda in cui deve essere ospitata di nuovo, ma utilizzare le impostazioni di bilanciamento del carico di lavoro del cluster per continuare a inviare messaggi all'istanza originale fino a quando la propria applicazione non è pronta per lo switch. Ciò si ottiene con la seguente procedura:

1. Impostare la proprietà **CLWLRANK** della coda esistente su un valore elevato, ad esempio cinque.

2. Creare la nuova istanza della coda e impostare la relativa proprietà **CLWLRANK** su zero.
3. Completare qualsiasi ulteriore configurazione del nuovo sistema, ad esempio la distribuzione e l'avvio dell'utilizzo delle applicazioni rispetto alla nuova istanza della coda.
4. Impostare la proprietà **CLWLRANK** della nuova istanza della coda in modo che sia superiore all'istanza originale, ad esempio nove.
5. Consentire all'istanza della coda originale di elaborare i messaggi accodati nel sistema e quindi eliminare la coda.

Spostamento di interi gestori code

Se il gestore code rimane sullo stesso host, ma l'indirizzo IP viene modificato, il processo è il seguente:

- Il DNS, se usato correttamente, può aiutare a semplificare il processo. Per informazioni sull'utilizzo di DNS impostando l'attributo del canale Nome connessione (CONNAME) , consultare ALTER CHANNEL.
- Se si sposta un repository completo, assicurarsi di disporre di almeno un altro repository completo che sia in esecuzione senza problemi (ad esempio, nessun problema con lo stato del canale) prima di apportare le modifiche.
- Sospendere il gestore code utilizzando il comando SUSPEND QMGR per evitare la creazione di traffico.
- Modificare l'indirizzo IP del computer. Se la definizione di canale CLUSRCVR utilizza un indirizzo IP nel campo CONNAME, modificare questa voce di indirizzo IP. Potrebbe essere necessario eseguire il flush della cache DNS per garantire che gli aggiornamenti siano disponibili ovunque.
- Quando il gestore code si riconnette ai repository completi, le definizioni automatiche del canale si risolvono automaticamente.
- Se il gestore code ospitava un repository completo e l'indirizzo IP cambia, è importante assicurarsi che le parti vengano commutate il prima possibile per puntare i canali CLUSSDR definiti manualmente alla nuova ubicazione. Finché questo switch non viene eseguito, questi gestori code potrebbero essere in grado di contattare solo il repository completo rimanente (non modificato) e potrebbero essere visualizzati messaggi di avvertenza relativi alla definizione di canale non corretta.
- Riprendere il gestore code utilizzando il comando RESUME QMGR .

Se il gestore code deve essere spostato su un altro host, è possibile copiare i dati del gestore code e ripristinare da un backup. Questo processo non è tuttavia consigliato, a meno che non vi siano altre opzioni; potrebbe essere preferibile creare un gestore code su una nuova macchina e replicare le code e le applicazioni come descritto nella sezione precedente. Questa situazione fornisce un meccanismo di rollover / rollback semplice.

Se si è determinati a spostare un gestore code completo utilizzando il backup, attenersi alle seguenti procedure ottimali:

- Considerare l'intero processo come un ripristino di un gestore code dal backup, applicando tutti i processi che di solito si utilizzano per il recupero del sistema come appropriato per l'ambiente del sistema operativo.
- Utilizzare il comando **REFRESH CLUSTER** dopo la migrazione per eliminare tutte le informazioni sul cluster conservate localmente (inclusi i canali definiti automaticamente che sono in dubbio) e forzarne la ricostruzione.

  Nota: Per i cluster di grandi dimensioni, l'utilizzo del comando **REFRESH CLUSTER** può danneggiare il cluster mentre è in esecuzione e, di nuovo, a intervalli di 27 giorni, quando gli oggetti del cluster inviano automaticamente aggiornamenti sullo stato a tutti i gestori code interessati. Consultare Refreshing in a large cluster can affect performance and availability of the cluster.

Quando si crea un gestore code e si replica l'impostazione da un gestore code esistente nel cluster (come descritto in precedenza in questo argomento), non considerare mai i due gestori code differenti come se fossero gli stessi. In particolare, non assegnare a un nuovo gestore code lo stesso nome e indirizzo IP. Il tentativo di 'inserire ' un gestore code di sostituzione è una causa frequente di problemi

nei cluster IBM MQ . La cache prevede di ricevere gli aggiornamenti incluso l'attributo **QMID** e lo stato può essere danneggiato.

Se due gestori code differenti vengono creati accidentalmente con lo stesso nome, si consiglia di utilizzare il comando RESET CLUSTER **QMID** per espellere la voce non corretta dal cluster.

Aggiornamenti e installazioni di manutenzione

Evitare il cosiddetto scenario big bang (ad esempio, l'arresto di tutte le attività del cluster e del gestore code, l'applicazione di tutti gli aggiornamenti e la manutenzione a tutti i gestori code, quindi l'avvio di tutto contemporaneamente). I cluster sono progettati per funzionare ancora con più versioni di gestori code coesistenti, quindi si consiglia un approccio di manutenzione pianificato e graduale.

Disporre di un piano di backup:

- Hai fatto dei backup?
- Evitare di utilizzare immediatamente la nuova funzionalità del cluster: attendere fino a quando non si è certi che tutti i gestori code siano aggiornati al nuovo livello e si è certi che non verrà eseguito il rollback di nessuno di essi. L'utilizzo di una nuova funzione cluster in un cluster in cui alcuni gestori code sono ancora a un livello precedente può portare a un comportamento non definito.

  Un repository memorizza un record ricevuto nella propria versione. Se il record che riceve è di una versione successiva, gli attributi della versione successiva vengono eliminati quando il record viene memorizzato. Un gestore code IBM MQ 9.2 che riceve informazioni su un gestore code IBM MQ 9.3 memorizza solo IBM MQ 9.2 informazioni. Un repository IBM MQ 9.3 che riceve un record IBM MQ 9.2 memorizza i valori predefiniti per gli attributi introdotti nella versione successiva. I valori predefiniti definiscono i valori per gli attributi che non vengono inclusi nel record ricevuto.

Migrare prima i repository completi. Anche se possono trasmettere informazioni che non comprendono, non possono persistere, quindi non è l'approccio raccomandato a meno che non sia assolutamente necessario. Per ulteriori informazioni, fare riferimento alla sezione Migrazione del cluster del gestore code.

Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER
Utilizzare il comando **REFRESH CLUSTER** per eliminare tutte le informazioni contenute localmente su un cluster e ricreare tali informazioni dai repository completi nel cluster. Non è necessario utilizzare questo comando, tranne in circostanze eccezionali. Se hai bisogno di usarlo, ci sono considerazioni speciali su come usarlo. Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

Eseguire REFRESH CLUSTER solo se necessario

La tecnologia del cluster IBM MQ garantisce che qualsiasi modifica alla configurazione del cluster, ad esempio una modifica a una coda cluster, diventi automaticamente nota a qualsiasi membro del cluster che deve conoscere le informazioni. Non è necessario adottare ulteriori misure amministrative per ottenere tale diffusione delle informazioni.

Se tali informazioni non raggiungono i gestori code nel cluster in cui sono richieste, ad esempio una coda cluster non è riconosciuta da un altro gestore code nel cluster quando un'applicazione tenta di aprirla per la prima volta, ciò implica un problema nell'infrastruttura del cluster. Ad esempio, è possibile che un canale non possa essere avviato tra un gestore code e un gestore code del repository completo. Pertanto, qualsiasi situazione in cui si osservino incongruenze deve essere esaminata. Se possibile, risolvere la situazione senza utilizzare il comando **REFRESH CLUSTER** .

In rare circostanze documentate altrove in questa documentazione del prodotto, o quando richiesto dal supporto IBM , è possibile utilizzare il comando **REFRESH CLUSTER** per eliminare tutte le informazioni conservate localmente su un cluster e ricreare tali informazioni dai repository completi nel cluster.

L'aggiornamento in un cluster di grandi dimensioni può influire sulle prestazioni e sulla disponibilità del cluster

L'utilizzo del comando **REFRESH CLUSTER** può essere disruttivo per il cluster mentre è in corso, ad esempio creando un aumento improvviso del lavoro per i repository completi mentre elaborano la propagazione delle risorse del cluster del gestore code. Se si sta aggiornando in un cluster di grandi dimensioni (ovvero, molte centinaia di gestori code) è necessario evitare l'utilizzo del comando nel lavoro quotidiano, se possibile, e utilizzare metodi alternativi per correggere specifiche incongruenze. Ad esempio, se una coda cluster non viene propagata correttamente nel cluster, una tecnica di analisi iniziale di aggiornamento della definizione della coda cluster, ad esempio la modifica della relativa descrizione, propaga la configurazione della coda nel cluster. Questo processo può aiutare a identificare il problema e potenzialmente a risolvere un'incongruenza temporanea.

Se non è possibile utilizzare metodi alternativi e si deve eseguire **REFRESH CLUSTER** in un cluster di grandi dimensioni, è necessario farlo in orari non di punta o durante una finestra di manutenzione per evitare l'impatto sui carichi di lavoro degli utenti. Si dovrebbe anche evitare di aggiornare un cluster di grandi dimensioni in un singolo batch, e di sfalsare l'attività come spiegato in “Evitare problemi di prestazioni e disponibilità quando gli oggetti cluster inviano aggiornamenti automatici” a pagina 71.

Evitare problemi di prestazioni e disponibilità quando gli oggetti cluster inviano aggiornamenti automatici

Dopo che un nuovo oggetto cluster è stato definito su un gestore code, un aggiornamento per questo oggetto viene generato ogni 27 giorni dal momento della definizione e inviato a ogni repository completo nel cluster e in seguito a qualsiasi altro gestore code interessato. Quando si immette il comando **REFRESH CLUSTER** su un gestore code, si reimposta l'orologio per questo aggiornamento automatico su tutti gli oggetti definiti localmente nel cluster specificato.

Se si aggiorna un cluster di grandi dimensioni (ossia, molte centinaia di gestori code) in un singolo batch o in altre circostanze, come la ricreazione di un sistema dal backup della configurazione, dopo 27 giorni tutti questi gestori code pubblicizzeranno nuovamente tutte le relative definizioni di oggetti nei repository completi contemporaneamente. Ciò potrebbe di nuovo causare un'esecuzione del sistema significativamente più lenta, o addirittura diventare non disponibile, fino a quando tutti gli aggiornamenti non sono stati completati. Pertanto, quando è necessario aggiornare o ricreare più gestori code in un cluster di grandi dimensioni, è necessario scaglionare l'attività per diverse ore o diversi giorni, in modo che i successivi aggiornamenti automatici non influiscono regolarmente sulle prestazioni del sistema.

La coda di cronologia cluster di sistema

Quando viene eseguito un **REFRESH CLUSTER** , il gestore code acquisisce un'istantanea dello stato del cluster prima dell'aggiornamento e la memorizza su `SYSTEM.CLUSTER.HISTORY.QUEUE` (SCHQ) se è definito sul gestore code. Questa istantanea è solo per scopi di servizio IBM , in caso di problemi successivi con il sistema.

SCHQ è definito per impostazione predefinita sui gestori code distribuiti all'avvio. Per la migrazione z/OS , SCHQ deve essere definito manualmente.

I messaggi sullo SCHQ scadono dopo tre mesi.

Concetti correlati

“REFRESH CLUSTER considerazioni per i cluster di pubblicazione / sottoscrizione” a pagina 107
Immettendo il comando **REFRESH CLUSTER** il gestore code elimina temporaneamente le informazioni conservate localmente su un cluster, inclusi gli argomenti del cluster e le relative sottoscrizioni proxy associate.

Riferimenti correlati

Problemi dell'applicazione durante l'esecuzione di REFRESH CLUSTER

Riferimento comandi MQSC: REFRESH CLUSTER

Clustering: disponibilità, più istanze e ripristino di emergenza
Questo argomento fornisce una guida per la pianificazione e la gestione dei cluster IBM MQ . Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

IBM MQ Il clustering stesso non è una soluzione ad alta disponibilità, ma in alcune circostanze può essere utilizzato per migliorare la disponibilità dei servizi utilizzando IBM MQ, ad esempio disponendo di più istanze di una coda su gestori code differenti. Questa sezione fornisce una guida per garantire che l'infrastruttura IBM MQ sia il più disponibile possibile in modo che possa essere utilizzata in tale architettura.

Nota: Altre soluzioni di alta disponibilità e ripristino di emergenza sono disponibili per IBM MQ, consultare Configurazione dell'alta disponibilità, ripristino e riavvio.

Disponibilità di risorse cluster
Il motivo per cui si consiglia di conservare due repository completi è che la perdita di uno non è critica per il corretto funzionamento del cluster. Anche se entrambi diventano non disponibili, esiste un periodo di tolleranza di 60 giorni per le conoscenze esistenti detenute da repository parziali, anche se le risorse nuove o non precedentemente accedute (code ad esempio) non sono disponibili in questo evento.

Utilizzo dei cluster per migliorare la disponibilità delle applicazioni
Un cluster può aiutare nella progettazione di applicazioni ad alta disponibilità (ad esempio un'applicazione server di tipo richiesta / risposta), utilizzando più istanze della coda e dell'applicazione. Se necessario, gli attributi di priorità possono dare la preferenza all'applicazione 'live', a meno che un gestore code o un canale non diventino, ad esempio, non disponibili. Ciò è utile per passare rapidamente all'elaborazione di nuovi messaggi quando si verifica un problema.

Tuttavia, i messaggi che sono stati consegnati a un determinato gestore code in un cluster vengono conservati solo su tale istanza della coda e non sono disponibili per l'elaborazione fino a quando tale gestore code non viene recuperato. Per questo motivo, per l'alta disponibilità dei dati reali, è possibile considerare altre tecnologie come i gestori code a più istanze.

Gestori code a più istanze
Software High Availability (multi - istanza) è un'offerta integrata per mantenere disponibili i messaggi esistenti. Fare riferimento a Utilizzo di IBM MQ con configurazioni ad alta disponibilità, Creazione di un gestore code a più istanzee alla seguente sezione per ulteriori informazioni. Qualsiasi gestore code in un cluster può essere reso altamente disponibile utilizzando questa tecnica, purché tutti i gestori code nel cluster siano in esecuzione almeno IBM WebSphere MQ 7.0.1. Se i gestori code nel cluster si trovano a livelli precedenti, potrebbero perdere la connettività con i gestori code a più istanze se viene eseguito il failover su un IP secondario.

Come discusso precedentemente in questo argomento, finché sono configurati due repository completi, sono quasi per loro natura altamente disponibili. Se necessario, è possibile utilizzare i gestori code del software IBM MQ ad alta disponibilità / a più istanze per repository completi. Non esiste un motivo valido per utilizzare questi metodi e, in effetti, per interruzioni temporanee, tali metodi potrebbero causare ulteriori costi di prestazioni durante il failover. L'utilizzo della HA del software invece di eseguire due repository completi è sconsigliato perché in caso di interruzione di un singolo canale, ad esempio, non necessariamente eseguirebbe il failover, ma potrebbe lasciare repository parziali non in grado di eseguire la query per le risorse cluster.

Ripristino di emergenza
Il ripristino di emergenza, ad esempio il ripristino da quando i dischi che memorizzano i dati di un gestore code diventano danneggiati, è difficile da eseguire correttamente; IBM MQ può aiutare, ma non può farlo automaticamente. L'unica opzione di ripristino di emergenza 'true' in IBM MQ (escludendo qualsiasi sistema operativo o altre tecnologie di replica sottostanti) è il ripristino da un backup. Ci sono alcuni punti specifici del cluster da considerare in queste situazioni:

- Prestare attenzione quando si verificano scenari di ripristino di emergenza. Ad esempio, se si verifica l'operazione dei gestori code di backup, prestare attenzione quando si portano in linea nella stessa rete poiché è possibile unirsi accidentalmente al cluster attivo e iniziare a 'rubare' i messaggi ospitando le stesse code denominate dei gestori code del cluster attivo.
- Il test del ripristino di emergenza non deve interferire con un cluster attivo in esecuzione. Le tecniche per evitare interferenze includono:

  - Completare la separazione o la separazione della rete a livello di firewall.
  - z/OS Non avvio dell'avvio del canale o dello spazio di indirizzo z/OS **chinit** .
  - Non emettere il certificato TLS attivo per il sistema di ripristino di emergenza fino a quando, o a meno che, non si verifichi uno scenario di ripristino di emergenza effettivo.
- Quando si ripristina un backup di un gestore code nel cluster, è possibile che il backup non sia sincronizzato con il resto del cluster. Il comando **REFRESH CLUSTER** può risolvere gli aggiornamenti e sincronizzarli con il cluster, ma il comando **REFRESH CLUSTER** deve essere utilizzato come ultima risorsa. Consultare “Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER” a pagina 70. Esaminare tutta la documentazione del processo interno e la documentazione di IBM MQ per vedere se è stato mancato un semplice passo prima di ricorrere all'utilizzo del comando.
- Come per qualsiasi ripristino, le applicazioni devono gestire la ripetizione e la perdita di dati. È necessario decidere se cancellare le code in uno stato noto o se ci sono informazioni sufficienti altrove per gestire le ripetizioni.

Pianificazione della rete di pubblicazione / sottoscrizione distribuita

È possibile creare una rete di gestori code in cui le sottoscrizioni create su un gestore code riceveranno i messaggi corrispondenti pubblicati da un'applicazione connessa a un altro gestore code nella rete. Per scegliere una topologia adatta, è necessario considerare i requisiti per il controllo manuale, la dimensione della rete, la frequenza di modifica, la disponibilità e la scalabilità.

Prima di iniziare

Questa attività presuppone che l'utente comprenda quali sono le reti di pubblicazione / sottoscrizione distribuite e come funzionano. Per una panoramica tecnica, consultare Distributed publish/subscribe networks.

Informazioni su questa attività

Esistono tre topologie di base per una rete di pubblicazione / sottoscrizione:

- Cluster instradato direttamente
- Cluster instradato host argomento
- Gerarchia

Per le prime due topologie, il punto di partenza è una configurazione cluster IBM MQ . La terza topologia può essere creata con o senza un cluster. Consultare“Pianificazione delle code e dei cluster distribuiti” a pagina 20per informazioni sulla pianificazione della rete di gestori code sottostante.

Un *cluster instradato direttamente* è la topologia più semplice da configurare quando un cluster è già presente. Qualsiasi argomento definito su qualsiasi gestore code viene automaticamente reso disponibile su ogni gestore code nel cluster e le pubblicazioni vengono instradate direttamente da qualsiasi gestore code a cui si connette un'applicazione di pubblicazione, a ciascuno dei gestori code in cui esistono sottoscrizioni corrispondenti. Questa semplicità di configurazione si basa sul fatto che IBM MQ mantiene un alto livello di condivisione di informazioni e connettività tra ogni gestore code nel cluster. Per reti piccole e semplici (ossia un numero ridotto di gestori code e un insieme abbastanza statico di publisher e sottoscrittori), ciò è accettabile. Tuttavia, se utilizzato in ambienti più grandi o più dinamici, il sovraccarico potrebbe essere proibitivo. Consultare“Instradamento diretto nei cluster di pubblicazione / sottoscrizione” a pagina 78.

Un *cluster instradato all'host dell'argomento* fornisce lo stesso vantaggio di un cluster instradato direttamente, rendendo qualsiasi argomento definito su qualsiasi gestore code nel cluster automaticamente disponibile su ogni gestore code nel cluster. Tuttavia, i cluster instradati dell'host argomento richiedono di scegliere attentamente i gestori code che ospitano ciascun argomento, poiché tutte le informazioni e le pubblicazioni per tale argomento passano attraverso tali gestori code dell'host argomento. Ciò significa che il sistema non deve gestire i canali e i flussi di informazioni tra tutti i gestori code. Tuttavia, significa anche che le pubblicazioni potrebbero non essere più inviate direttamente ai sottoscrittori, ma potrebbero essere instradate tramite un gestore code dell'host argomento. Per questi

motivi, potrebbe essere necessario un ulteriore carico sul sistema, in particolare sui gestori code che ospitano gli argomenti, pertanto è necessaria un'attenta pianificazione della topologia. Questa topologia è particolarmente efficace per le reti che contengono molti gestori code o che ospitano una serie dinamica di publisher e sottoscrittori (ossia, publisher o sottoscrittori che vengono aggiunti o rimossi di frequente). È possibile definire ulteriori host argomento per migliorare la disponibilità degli instradamenti e per scalare orizzontalmente il carico di lavoro di pubblicazione. Consultare"Instradamento host argomento nei cluster di pubblicazione / sottoscrizione" a pagina 83.

Una *gerarchia* richiede la maggior parte della configurazione manuale per essere impostata ed è la topologia più difficile da modificare. È possibile configurare manualmente le relazioni tra ciascun gestore code nella gerarchia e le sue relazioni dirette. Una volta configurate le relazioni, le pubblicazioni (come per le due topologie precedenti) verranno instradate alle sottoscrizioni su altri gestori code nella gerarchia. Le pubblicazioni vengono instradate utilizzando le relazioni della gerarchia. Ciò consente la configurazione di topologie molto specifiche per soddisfare requisiti differenti, ma può anche risultare in pubblicazioni che richiedono molti "hop" tramite gestori code intermedi per raggiungere le sottoscrizioni. Esiste sempre un solo instradamento attraverso una gerarchia per una pubblicazione, quindi la disponibilità di ogni gestore code è critica. Le gerarchie sono generalmente preferibili solo quando non è possibile configurare un singolo cluster, ad esempio quando si estendono più organizzazioni. Consultare"Instradamento nelle gerarchie di pubblicazione / sottoscrizione" a pagina 108.

Se necessario, le tre topologie di cui sopra possono essere combinate per risolvere specifici requisiti topografici. Per un esempio, consultare Combinazione degli spazi argomento di più cluster.

Per scegliere una topologia adatta per la propria rete di pubblicazione / sottoscrizione distribuita, è necessario considerare le seguenti domande generali:

- Quanto sarà grande la tua rete?
- Di quale controllo manuale hai bisogno per la sua configurazione?
- Quanto sarà dinamico il sistema, sia in termini di argomenti e sottoscrizioni, sia in termini di gestori code?
- Quali sono i requisiti di disponibilità e scalabilità?
- Tutti i gestori code possono connettersi direttamente tra loro?

Procedura

- Stimare la dimensione della rete.
  a) Stimare il numero di argomenti necessari.
  b) Stimare quanti publisher e sottoscrittori si prevede di avere.
  c) Stimare il numero di gestori code coinvolti nelle attività di pubblicazione / sottoscrizione.

     Consultare anche"Clustering di pubblicazione / sottoscrizione: procedure ottimali" a pagina 93, in particolare le seguenti sezioni:

     – Modalità di dimensionamento del sistema
     – Motivi per limitare il numero di gestori code del cluster coinvolti nell'attività di pubblicazione / sottoscrizione
     – Come decidere quali argomenti raggruppare

  Se la rete avrà molti gestori code e gestirà molti publisher e sottoscrittori, è probabilmente necessario utilizzare un cluster instradato dell'host argomento o una gerarchia. I cluster instradati direttamente non richiedono quasi alcuna configurazione manuale e possono essere una buona soluzione per reti piccole o statiche.
- Considerare quanto controllo manuale è necessario su quale gestore code ospita ciascun argomento, publisher o sottoscrittore.
  a) Considerare se alcuni dei gestori code sono meno capaci di altri.
  b) Considerare se i collegamenti di comunicazione ad alcuni dei gestori code sono più fragili rispetto ad altri.

c) Identificare i casi in cui si prevede che un argomento abbia molte pubblicazioni e pochi sottoscrittori.

d) Identificare i casi in cui si prevede che un argomento abbia molti sottoscrittori e poche pubblicazioni.

In tutte le topologie, le pubblicazioni vengono consegnate alle sottoscrizioni su altri gestori code. In un cluster instradato direttamente tali pubblicazioni prendono il percorso più breve alle sottoscrizioni. In un cluster instradato dell'host argomento o in una gerarchia, è possibile controllare l'instradamento seguito dalle pubblicazioni. Se i gestori code differiscono per capacità o hanno livelli differenti di disponibilità e connettività, è probabile che si desideri assegnare carichi di lavoro specifici a gestori code specifici. È possibile effettuare questa operazione utilizzando un cluster instradato dell'host argomento o una gerarchia.

In tutte le topologie, la co - localizzazione delle applicazioni di pubblicazione sullo stesso gestore code delle sottoscrizioni, quando possibile, riduce i sovraccarichi e massimizza le prestazioni. Per i cluster instradati dell'host argomento, considerare l'inserimento di publisher o sottoscrittori sui gestori code che ospitano l'argomento. Questa operazione rimuove eventuali "hop" supplementari tra i gestori code per passare una pubblicazione a un sottoscrittore. Questo approccio è particolarmente efficace nei casi in cui un argomento ha molti editori e pochi sottoscrittori, o molti sottoscrittori e pochi editori. Consultare, ad esempio, Instradamento host argomento utilizzando publisher o sottoscrittori centralizzati.

Consultare anche“Clustering di pubblicazione / sottoscrizione: procedure ottimali” a pagina 93, in particolare le seguenti sezioni:

– Come decidere quali argomenti raggruppare
– Posizione di pubblicazione e sottoscrizione

- Considerare la dinamica dell'attività di rete.

  a) Stimare la frequenza con cui i sottoscrittori verranno aggiunti e rimossi su argomenti differenti.

  Ogni volta che una sottoscrizione viene aggiunta o rimossa da un gestore code ed è la prima o l'ultima sottoscrizione per quella specifica stringa di argomenti, tali informazioni vengono comunicate ad altri gestori code nella topologia. In un cluster instradato direttamente e in una gerarchia, queste informazioni di sottoscrizione vengono propagate a tutti i gestori code nella topologia, indipendentemente dal fatto che abbiano o meno dei publisher sull'argomento. Se la topologia è composta da molti gestori code, questo potrebbe essere un sovraccarico delle prestazioni significativo. In un cluster instradato dell'host argomento, queste informazioni vengono propagate solo ai gestori code che ospitano un argomento del cluster associato alla stringa di argomenti della sottoscrizione.

  Consultare anche la sezione Modifica della sottoscrizione e stringhe di argomenti dinamici di“Clustering di pubblicazione / sottoscrizione: procedure ottimali” a pagina 93.

  Nota: In sistemi molto dinamici, in cui l'insieme di molte stringhe di argomenti univoci viene modificato in modo rapido e costante, potrebbe essere meglio passare alla modalità "pubblica ovunque" . Vedere Prestazioni della sottoscrizione nelle reti di pubblicazione / sottoscrizione.

  b) Considerare quanto sono dinamici i gestori code nella topologia.

  Una gerarchia richiede che ogni modifica nel gestore code nella topologia venga inserita o rimossa manualmente dalla gerarchia, con attenzione quando si modificano i gestori code ai livelli più alti della gerarchia. I gestori code in una gerarchia generalmente utilizzano anche connessioni di canale configurate manualmente. È necessario mantenere queste connessioni, aggiungendo e rimuovendo canali quando i gestori code vengono aggiunti e rimossi dalla gerarchia.

  In un cluster di pubblicazione / sottoscrizione, i gestori code vengono automaticamente connessi a qualsiasi altro gestore code richiesto quando si uniscono per la prima volta al cluster e diventano automaticamente consapevoli degli argomenti e delle sottoscrizioni.

- Considera la disponibilità del tuo instradamento e i requisiti di scalabilità del traffico di pubblicazione.

  a) Decidere se è necessario disporre sempre di un instradamento disponibile da un gestore code di pubblicazione a un gestore code di sottoscrizione, anche quando un gestore code non è disponibile.

b) Considera la scalabilità di cui hai bisogno per la rete. Decidere se il livello di traffico di pubblicazione è troppo alto per essere instradato attraverso un singolo gestore code o canale e se tale livello di traffico di pubblicazione deve essere gestito da un singolo ramo di argomento o può essere distribuito su più rami di argomento.

c) Considerare se è necessario mantenere l'ordine dei messaggi.

Poiché un cluster instradato direttamente invia i messaggi direttamente dai gestori code di pubblicazione ai gestori code di sottoscrizione, non è necessario considerare la disponibilità dei gestori code intermedi lungo la rotta. Allo stesso modo, il ridimensionamento ai gestori code intermedi non è una considerazione. Tuttavia, come precedentemente menzionato, il sovraccarico di gestione automatica dei canali e dei flussi di informazioni tra tutti i gestori code nel cluster può influire in modo significativo sulle prestazioni, soprattutto in un ambiente di grandi dimensioni o dinamico.

Un cluster di host argomento instradato può essere ottimizzato per singoli argomenti. È possibile garantire che ogni ramo della struttura ad albero degli argomenti che ha un considerevole carico di lavoro di pubblicazione sia definito su un gestore code differente e che ogni gestore code sia sufficientemente performante e disponibile per il carico di lavoro previsto per tale ramo della struttura ad albero degli argomenti. È inoltre possibile migliorare ulteriormente la disponibilità e il ridimensionamento orizzontale definendo ogni argomento su più gestori code. Ciò consente al sistema di instradare i gestori code dell'host argomento non disponibili e di bilanciare il traffico di pubblicazione tra di essi. Tuttavia, quando si definisce un determinato argomento su più gestori code, vengono introdotti anche i seguenti vincoli:

- Si perde l'ordine dei messaggi tra le pubblicazioni.
- Non è possibile utilizzare pubblicazioni conservate. Consultare"Considerazioni di progettazione per le pubblicazioni conservate nei cluster di pubblicazione / sottoscrizione" a pagina 106.

Non è possibile configurare l'alta disponibilità o la scalabilità dell'instradamento in una gerarchia attraverso più instradamenti.

Vedi anche la sezione Traffico di pubblicazione di"Clustering di pubblicazione / sottoscrizione: procedure ottimali" a pagina 93.

- In base a questi calcoli, utilizzare i link forniti per decidere se utilizzare un cluster instradato dell'host argomento, un cluster instradato direttamente, una gerarchia o una combinazione di queste topologie.

Operazioni successive

Si è ora pronti a configurare la rete di pubblicazione / sottoscrizione distribuita.

Attività correlate

Configurazione di un cluster di gestore code

Configurazione dell'accodamento distribuito

Configurazione di un cluster di pubblicazione / sottoscrizione

Connessione di un gestore code a una gerarchia di pubblicazione / sottoscrizione

Progettazione di cluster di pubblicazione / sottoscrizione

Esistono due topologie cluster di pubblicazione / sottoscrizione di base: *instradamento diretto* e *instradamento host argomento*. Ognuno ha vantaggi diversi. Quando si progetta il cluster di pubblicazione / sottoscrizione, scegliere la topologia che meglio si adatta ai requisiti di rete previsti.

Per una panoramica delle due topologie di cluster di pubblicazione / sottoscrizione, vedere Cluster di pubblicazione / sottoscrizione. Per aiutarti a valutare i tuoi requisiti di rete, vedi "Pianificazione della rete di pubblicazione / sottoscrizione distribuita" a pagina 73 e "Clustering di pubblicazione / sottoscrizione: procedure ottimali" a pagina 93.

In generale, entrambe le topologie di cluster forniscono i seguenti vantaggi:

- Configurazione semplice su una topologia di cluster point - to - point.
- Gestione automatica dei gestori code che si uniscono e escono dal cluster.

- Facilità di ridimensionamento per ulteriori sottoscrizioni e publisher, aggiungendo ulteriori gestori code e distribuendo le sottoscrizioni e i publisher aggiuntivi.

Tuttavia, le due topologie hanno vantaggi diversi quando i requisiti diventano più specifici.

Cluster di pubblicazione / sottoscrizione instradati diretti

Con l'instradamento diretto, tutti i gestori code nel cluster inviano le pubblicazioni dalle applicazioni connesse direttamente a qualsiasi altro gestore code nel cluster con una sottoscrizione corrispondente.

Un cluster di pubblicazione / sottoscrizione instradato direttamente fornisce i seguenti vantaggi:

- I messaggi destinati a una sottoscrizione su un gestore code specifico nello stesso cluster vengono trasportati direttamente a tale gestore code e non è necessario passare attraverso un gestore code intermedio. Ciò può migliorare le prestazioni rispetto a una topologia instradata dell'host argomento o a una topologia gerarchica.
- Poiché tutti i gestori code sono direttamente connessi tra loro, non esiste un singolo punto di errore nell'infrastruttura di instradamento di questa topologia. Se un gestore code non è disponibile, le sottoscrizioni su altri gestori code nel cluster sono ancora in grado di ricevere messaggi dai publisher sui gestori code disponibili.
- È molto semplice da configurare, soprattutto su un cluster esistente.

Elementi da considerare quando si utilizza un cluster di pubblicazione / sottoscrizione instradato direttamente:

- Tutti i gestori code nel cluster vengono a conoscenza di tutti gli altri gestori code nel cluster.
- I gestori code in un cluster che ospitano una o più sottoscrizioni a un argomento cluster, creano automaticamente i canali mittente del cluster per tutti gli altri gestori code nel cluster, anche quando tali gestori code non pubblicano messaggi su argomenti cluster.
- La prima sottoscrizione su un gestore code a una stringa di argomenti in un argomento cluster comporta l'invio di un messaggio a tutti gli altri gestori code nel cluster. Allo stesso modo, l'ultima sottoscrizione su una stringa di argomenti da eliminare risulta anche in un messaggio. Maggiore è il numero di stringhe di argomenti individuali utilizzate in un argomento in cluster e maggiore è la frequenza di modifica delle sottoscrizioni, maggiore è la comunicazione tra gestori code.
- Ogni gestore code nel cluster conserva la conoscenza delle stringhe di argomenti sottoscritte di cui è informato, anche quando il gestore code non pubblica né sottoscrive tali argomenti.

Per questi motivi, tutti i gestori code in un cluster con un argomento di instradamento diretto definito subiranno un ulteriore sovraccarico. Maggiore è il numero di gestori code presenti nel cluster, maggiore è il sovraccarico. Allo stesso modo, maggiore è il numero di stringhe di argomenti sottoscritte e maggiore è il loro tasso di modifica, maggiore è il sovraccarico. Ciò può comportare un carico eccessivo sui gestori code in esecuzione su sistemi di piccole dimensioni in un cluster di pubblicazione / sottoscrizione instradato direttamente, di grandi dimensioni o dinamico. Per ulteriori informazioni, vedi Prestazioni di pubblicazione / sottoscrizione instradate in modo diretto .

Quando si sa che un cluster non è in grado di gestire i sovraccarichi della pubblicazione / sottoscrizione del cluster instradata diretta, è possibile utilizzare invece la pubblicazione / sottoscrizione instradata dell'host argomento. In alternativa, in situazioni estreme, è possibile disabilitare completamente la funzionalità di pubblicazione / sottoscrizione del cluster impostando l'attributo del gestore code **PSCLUS** su DISABLED su ogni gestore code nel cluster. Consultare “Blocco della pubblicazione / sottoscrizione in cluster” a pagina 103. Ciò impedisce la creazione di qualsiasi argomento in cluster e garantisce che la rete non subisca alcun sovraccarico associato alla pubblicazione / sottoscrizione in cluster.

Cluster di pubblicazione / sottoscrizione instradati host argomento

Con l'instradamento dell'host argomento, i gestori code in cui sono definiti amministrativamente gli argomenti del cluster diventano router per le pubblicazioni. Le pubblicazioni dei gestori code non host nel cluster vengono instradate tramite il gestore code host a qualsiasi gestore code nel cluster con una sottoscrizione corrispondente.

Un cluster di pubblicazione / sottoscrizione instradato dall'host dell'argomento fornisce i seguenti vantaggi aggiuntivi su un cluster di pubblicazione / sottoscrizione instradato direttamente:

- Solo i gestori code su cui sono definiti gli argomenti instradati dell'host argomento vengono informati di tutti gli altri gestori code nel cluster.
- Solo i gestori code dell'host argomento devono essere in grado di connettersi a tutti gli altri gestori code nel cluster e generalmente si connetteranno solo a quelli in cui esistono le sottoscrizioni. Pertanto, vi è un numero significativamente inferiore di canali in esecuzione tra i gestori code.
- I gestori code del cluster che ospitano una o più sottoscrizioni a un argomento in cluster creano automaticamente i canali mittente del cluster solo per i gestori code che ospitano un argomento del cluster associato alla stringa dell'argomento della sottoscrizione.
- La prima sottoscrizione su un gestore code a una stringa di argomenti in un argomento in cluster determina l'invio di un messaggio a un gestore code nel cluster che ospita l'argomento in cluster. Allo stesso modo, l'ultima sottoscrizione su una stringa di argomenti da eliminare risulta anche in un messaggio. Maggiore è il numero di stringhe di argomenti individuali utilizzate in un argomento in cluster e maggiore è la frequenza di modifica delle sottoscrizioni, maggiore è la comunicazione tra gestori code, ma solo tra host di sottoscrizioni e host di argomenti.
- Più controllo sulla configurazione fisica. Con l'instradamento diretto, tutti i gestori code devono partecipare al cluster di pubblicazione / sottoscrizione, aumentando i propri costi generali. Con l'instradamento dell'host argomento, solo i gestori code dell'host argomento sono a conoscenza di altri gestori code e delle relative sottoscrizioni. È possibile scegliere esplicitamente i gestori code dell'host argomento, quindi è possibile verificare che tali gestori code siano in esecuzione su un'apparecchiatura adeguata ed è possibile utilizzare sistemi meno potenti per gli altri gestori code.

Elementi da considerare quando si utilizza un cluster di pubblicazione / sottoscrizione instradato dell'host argomento:

- Un ulteriore "hop" tra un gestore code di pubblicazione e un gestore code di sottoscrizione viene introdotto quando il publisher o il sottoscrittore non si trova su un gestore code che ospita l'argomento. La latenza causata dall' "hop" aggiuntivo può significare che l'instradamento dell'host argomento è meno efficace di quello diretto.
- Su cluster di grandi dimensioni, l'instradamento dell'host argomento facilita le prestazioni significative e i problemi di ridimensionamento che è possibile ottenere con l'instradamento diretto.
- È possibile definire tutti gli argomenti su un singolo gestore code o su un numero molto piccolo di gestori code. In questo caso, verificare che i gestori code dell'host argomento siano ospitati su sistemi potenti con una buona connettività.
- È possibile definire lo stesso argomento su più di un gestore code. Ciò migliora la disponibilità dell'argomento e migliora anche la scalabilità perché il carico di lavoro IBM MQ bilancia le pubblicazioni per un argomento tra tutti gli host per tale argomento. Si noti, tuttavia, che la definizione dello stesso argomento su più di un gestore code perde l'ordine dei messaggi per tale argomento.
- Ospitando diversi argomenti su gestori code differenti, è possibile migliorare la scalabilità senza perdere l'ordine dei messaggi.

Attività correlate

Scenario: creazione di un cluster di pubblicazione / sottoscrizione

Configurazione di un cluster di pubblicazione / sottoscrizione

Ottimizzazione delle reti di pubblicazione / sottoscrizione distribuite

Risoluzione dei problemi di pubblicazione / sottoscrizione distribuiti

Instradamento diretto nei cluster di pubblicazione / sottoscrizione

Le pubblicazioni da qualsiasi gestore code di pubblicazione vengono instradate direttamente a qualsiasi altro gestore code nel cluster con una sottoscrizione corrispondente.

Per un'introduzione al modo in cui i messaggi vengono instradati tra i gestori code nelle gerarchie di pubblicazione / sottoscrizione e nei cluster, consultare Reti di pubblicazione / sottoscrizione distribuite.

Un cluster di pubblicazione / sottoscrizione instradato si comporta come segue:

- Tutti i gestori code conoscono automaticamente tutti gli altri gestori code.
- Tutti i gestori code con sottoscrizioni agli argomenti del cluster creano canali per tutti i gestori code nel cluster e li informano delle relative sottoscrizioni.
- I messaggi pubblicati da un'applicazione vengono instradati dal gestore code a cui è connessa, direttamente a ciascun gestore code in cui esiste una sottoscrizione corrispondente.

Il seguente diagramma mostra un cluster del gestore code che non è attualmente utilizzato per attività di pubblicazione / sottoscrizione o point - to - point. Tenere presente che ogni gestore code nel cluster si connette solo ai gestori code del repository completo.

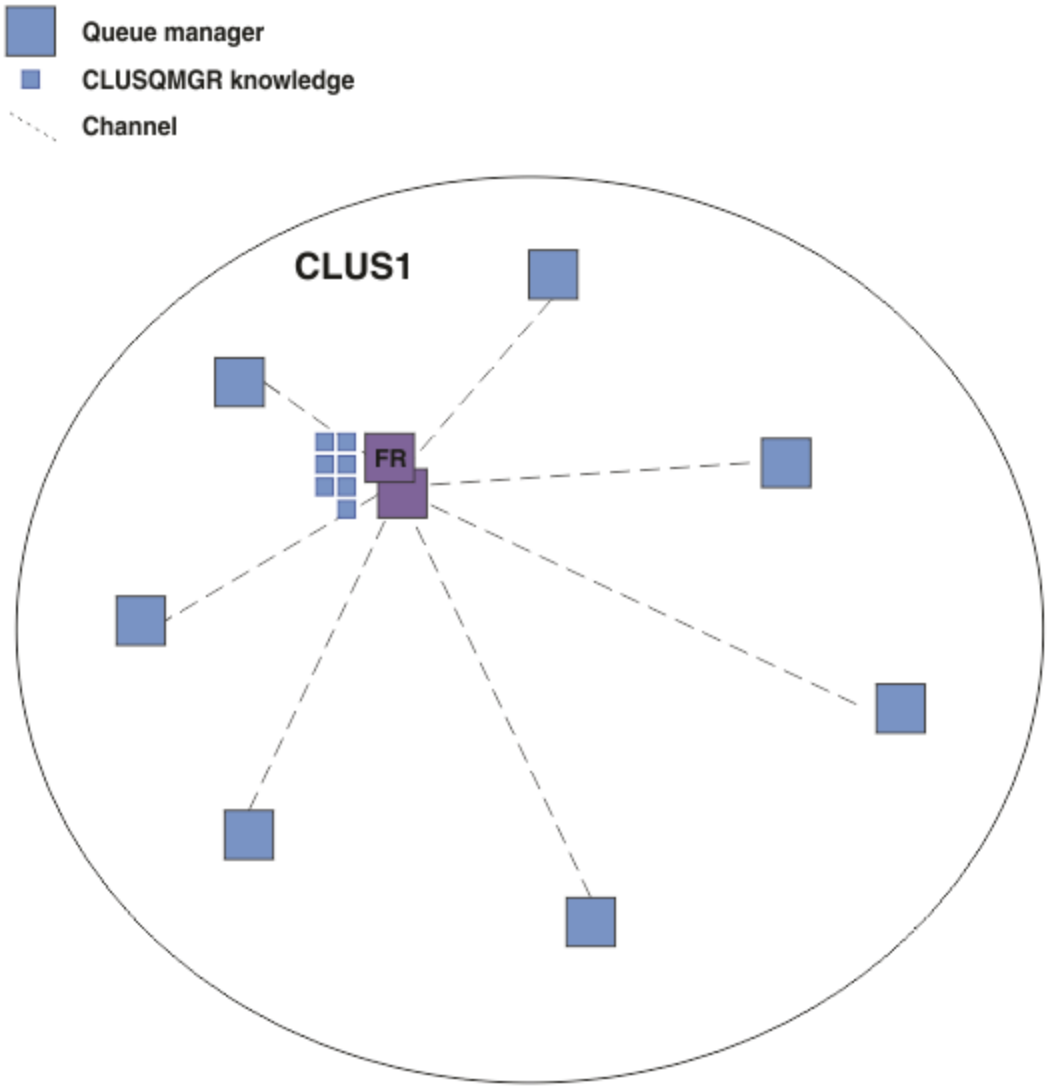


Figura 16. Un cluster di gestore code

Per consentire il flusso delle pubblicazioni tra gestori code in un cluster instradato direttamente, si crea il cluster di un ramo della struttura ad albero degli argomenti come descritto in Configurazione di un cluster di pubblicazione / sottoscrizionee si specifica *instradamento diretto* (impostazione predefinita).

In un cluster di pubblicazione / sottoscrizione instradato direttamente, si definisce l'oggetto argomento su qualsiasi gestore code nel cluster. Quando si esegue questa operazione, la conoscenza dell'oggetto e di tutti gli altri gestori code nel cluster viene automaticamente inviata a tutti i gestori code nel cluster dai gestori code del repository completo. Ciò si verifica prima che un gestore code faccia riferimento all'argomento:

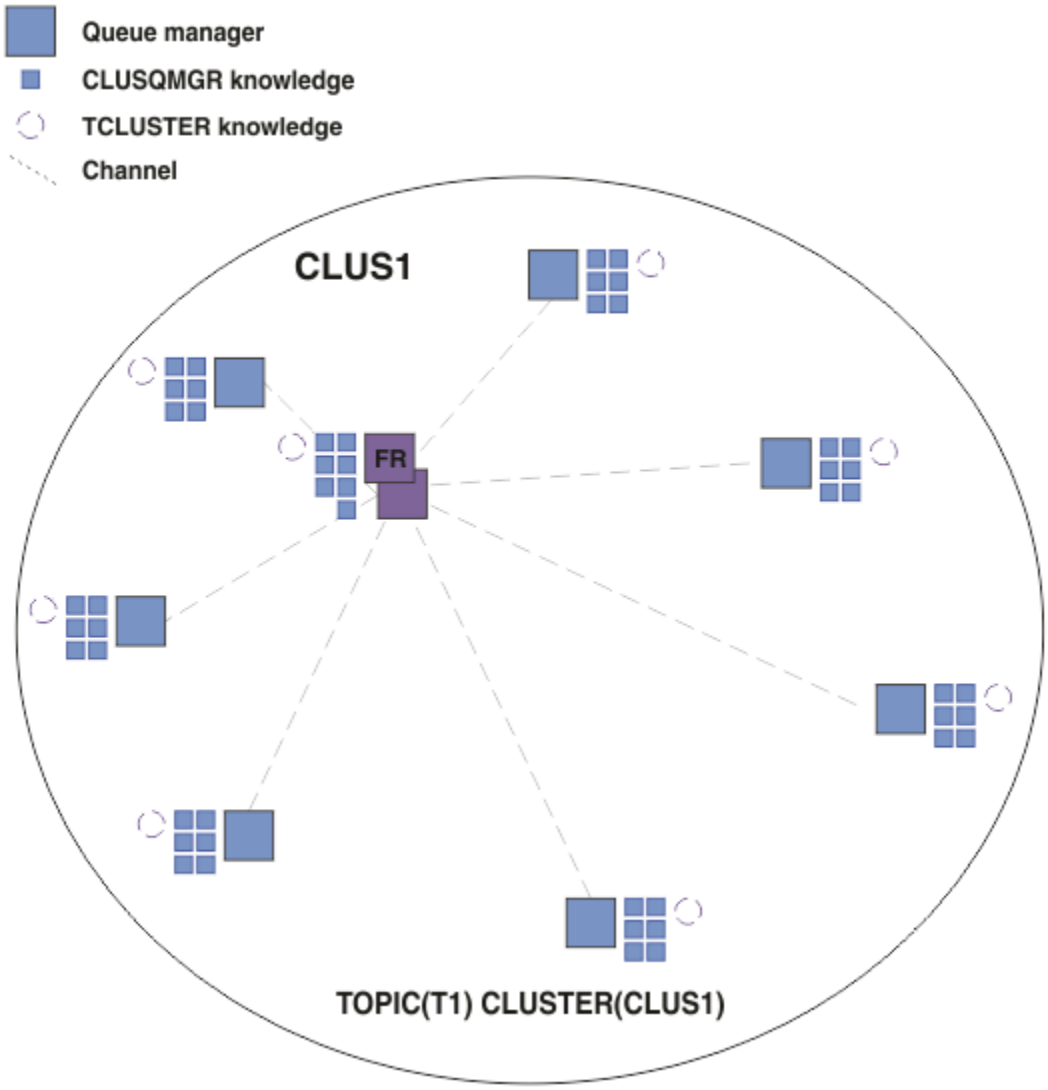


Figura 17. Un cluster di pubblicazione / sottoscrizione instradato direttamente

Quando viene creata una sottoscrizione, il gestore code che ospita la sottoscrizione stabilisce un canale per ogni gestore code nel cluster e invia i dettagli della sottoscrizione. Questa conoscenza della sottoscrizione distribuita è rappresentata da una sottoscrizione proxy su ciascun gestore code. Quando una pubblicazione viene prodotta su un qualsiasi gestore code nel cluster che corrisponde alla stringa di argomenti della sottoscrizione proxy, viene stabilito un canale cluster dal gestore code del publisher a ciascun gestore code che ospita una sottoscrizione e il messaggio viene inviato a ognuno di essi.

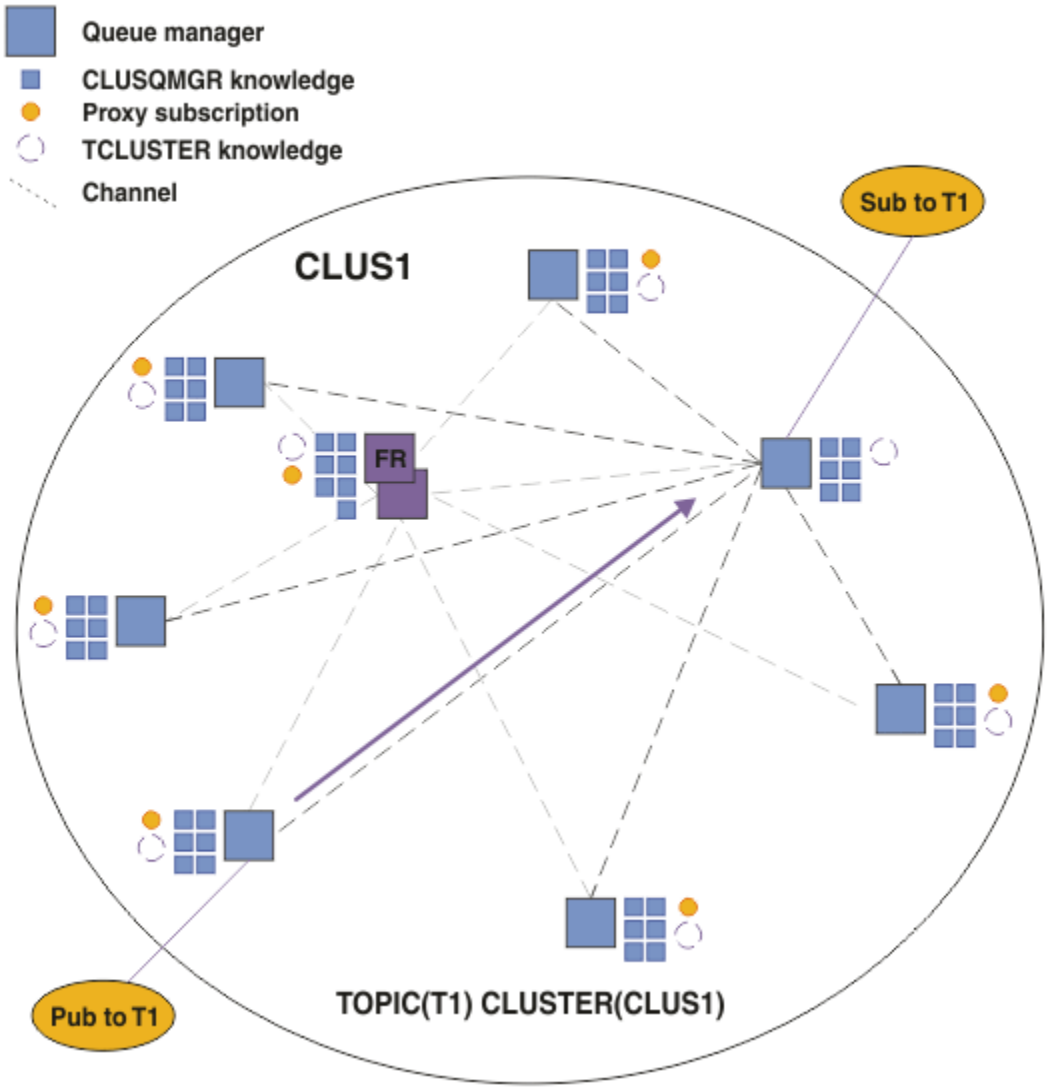


Figura 18. Un cluster di pubblicazione / sottoscrizione instradato direttamente con un publisher e un sottoscrittore a un argomento in cluster

L'instradamento diretto delle pubblicazioni ai gestori code che ospitano le sottoscrizioni semplifica la configurazione e riduce la latenza nella consegna delle pubblicazioni alle sottoscrizioni.

Tuttavia, a seconda dell'ubicazione delle sottoscrizioni e dei publisher, il cluster può diventare rapidamente completamente interconnesso, con ogni gestore code che ha una connessione diretta a ogni altro gestore code. Ciò potrebbe essere o meno accettabile nel proprio ambiente. Allo stesso modo, se la serie di stringhe di argomenti sottoscritte viene modificata di frequente, anche il sovraccarico di propagazione di tali informazioni tra tutti i gestori code può diventare significativo. Tutti i gestori code in un cluster di pubblicazione / sottoscrizione instradato devono essere in grado di far fronte a questi costi generali.

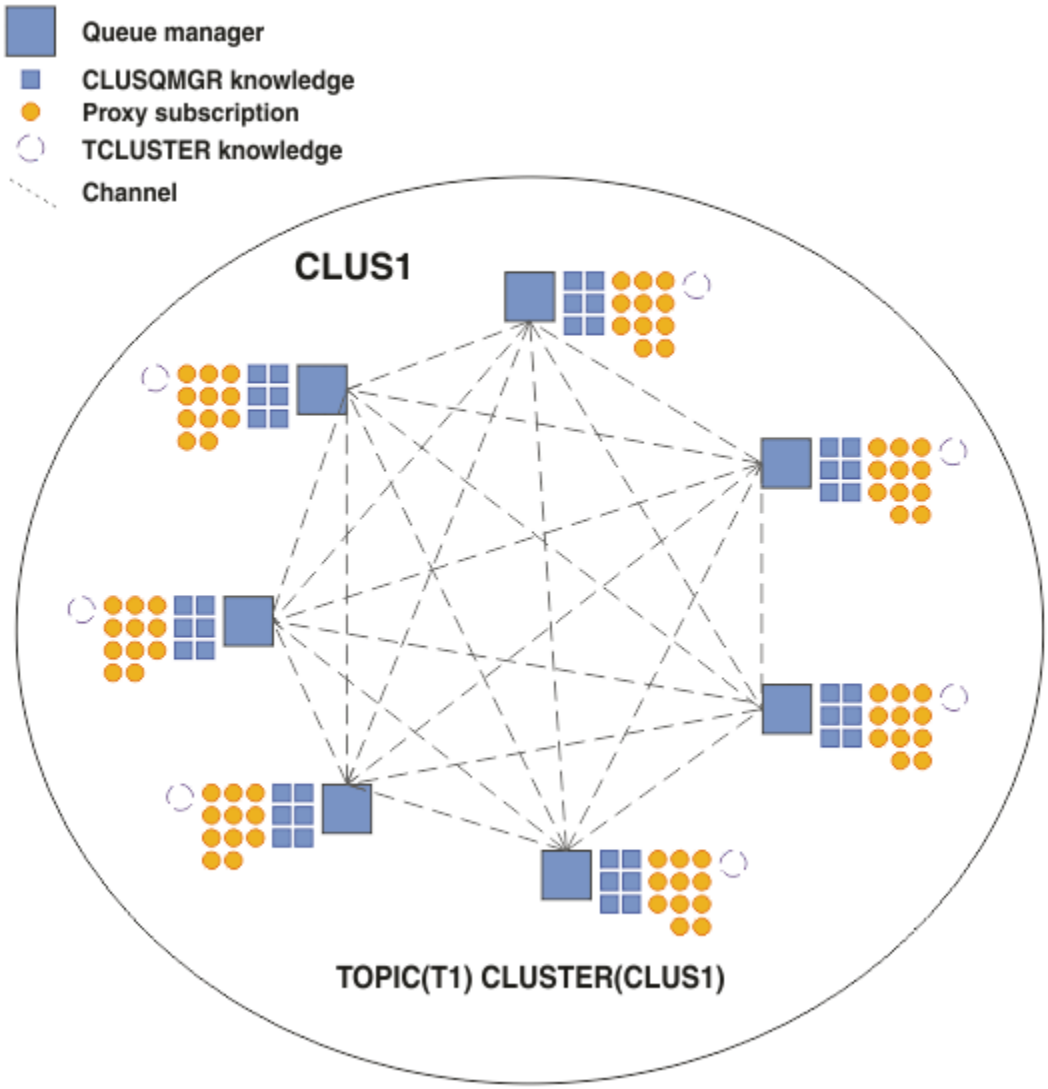


Figura 19. Un cluster di pubblicazione / sottoscrizione instradato che è completamente interconnesso

Sintesi e considerazioni aggiuntive

Un cluster di pubblicazione / sottoscrizione diretto ha bisogno di un piccolo intervento manuale per creare o amministrare e fornisce un instradamento diretto tra i publisher e i sottoscrittori. Per alcune configurazioni, di solito è la topologia più appropriata, in particolare i cluster con pochi gestori code o dove la connettività elevata dei gestori code è accettabile e le sottoscrizioni cambiano raramente. Tuttavia, impone anche alcuni vincoli al sistema:

- Il carico su ciascun gestore code è proporzionale al numero totale di gestori code nel cluster. Pertanto, in cluster più grandi, i singoli gestori code e il sistema nel suo complesso possono riscontrare problemi di prestazioni.
- Per impostazione predefinita, tutte le stringhe di argomenti in cluster sottoscritte vengono propagate in tutto il cluster e le pubblicazioni sono propagate solo ai gestori code remoti che hanno una sottoscrizione all'argomento associato. Pertanto, le rapide modifiche all'insieme delle sottoscrizioni possono diventare un fattore limitante. È possibile modificare questo comportamento predefinito e fare in modo che tutte le pubblicazioni vengano propagate a tutti i gestori code, il che elimina la necessità di sottoscrizioni proxy. Ciò riduce il traffico di conoscenza delle sottoscrizioni, ma è probabile che aumenti il traffico di pubblicazione e il numero di canali stabilito da ogni gestore code. Vedere Prestazioni della sottoscrizione nelle reti di pubblicazione / sottoscrizione.

  Nota: Una restrizione simile si applica anche alle gerarchie.

- A causa della natura interconnessa dei gestori code di pubblicazione / sottoscrizione, la propagazione delle sottoscrizioni proxy su tutti i nodi nella rete richiede tempo. Le pubblicazioni remote non iniziano necessariamente ad essere sottoscritte immediatamente, quindi le pubblicazioni iniziali potrebbero non essere inviate in seguito ad una sottoscrizione ad una nuova stringa di argomenti. È possibile rimuovere i problemi causati dal ritardo della sottoscrizione facendo in modo che tutte le pubblicazioni vengano propagate a tutti i gestori code, eliminando la necessità di sottoscrizioni proxy. Consultare Prestazioni della sottoscrizione nelle reti di pubblicazione / sottoscrizione.

  Nota: Questa limitazione si applica anche alle gerarchie.

Prima di utilizzare l'instradamento diretto, esplorare gli approcci alternativi descritti in “Instradamento host argomento nei cluster di pubblicazione / sottoscrizione” a pagina 83e “Instradamento nelle gerarchie di pubblicazione / sottoscrizione” a pagina 108.

Instradamento host argomento nei cluster di pubblicazione / sottoscrizione

Le pubblicazioni dei gestori code non host nel cluster vengono instradate tramite il gestore code host a qualsiasi gestore code nel cluster con una sottoscrizione corrispondente.

Per un'introduzione al modo in cui i messaggi vengono instradati tra i gestori code nelle gerarchie di pubblicazione / sottoscrizione e nei cluster, consultare Reti di pubblicazione / sottoscrizione distribuite.

Per comprendere il comportamento e i vantaggi dell'instradamento dell'host argomento, è preferibile prima comprendere “Instradamento diretto nei cluster di pubblicazione / sottoscrizione” a pagina 78.

Un cluster di pubblicazione / sottoscrizione instradato dell'host argomento si comporta come segue:

- Gli oggetti argomento gestiti in cluster vengono definiti manualmente sui singoli gestori code nel cluster. A questi si fa riferimento come *gestori code host argomento*.
- Quando viene effettuata una sottoscrizione su un gestore code cluster, i canali vengono creati dal gestore code dell'host di sottoscrizione ai gestori code dell'host argomento e le sottoscrizioni proxy vengono create solo sui gestori code che ospitano l'argomento.
- Quando un'applicazione pubblica le informazioni su un argomento, il gestore code connesso inoltra sempre la pubblicazione a un gestore code su cui è presente l'argomento, che le trasmette a tutti i gestori code nel cluster che hanno sottoscrizioni corrispondenti all'argomento.

Questo processo è spiegato in modo più dettagliato nei seguenti esempi.

Instradamento host argomento utilizzando un singolo host argomento

Per il flusso delle pubblicazioni tra i gestori code in un cluster instradato di host argomento, si crea un cluster di una sezione della struttura ad albero degli argomenti come descritto in Configurazione di un cluster di pubblicazione / sottoscrizionee si specifica *Instradamento host argomento*.

Esistono diversi motivi per definire un oggetto argomento instradato dell'host argomento su più gestori code in un cluster. Tuttavia, per semplicità iniziamo con un singolo host di argomento.

Il seguente diagramma mostra un cluster del gestore code che non è attualmente utilizzato per attività di pubblicazione / sottoscrizione o point - to - point. Tenere presente che ogni gestore code nel cluster si connette solo ai gestori code del repository completo.

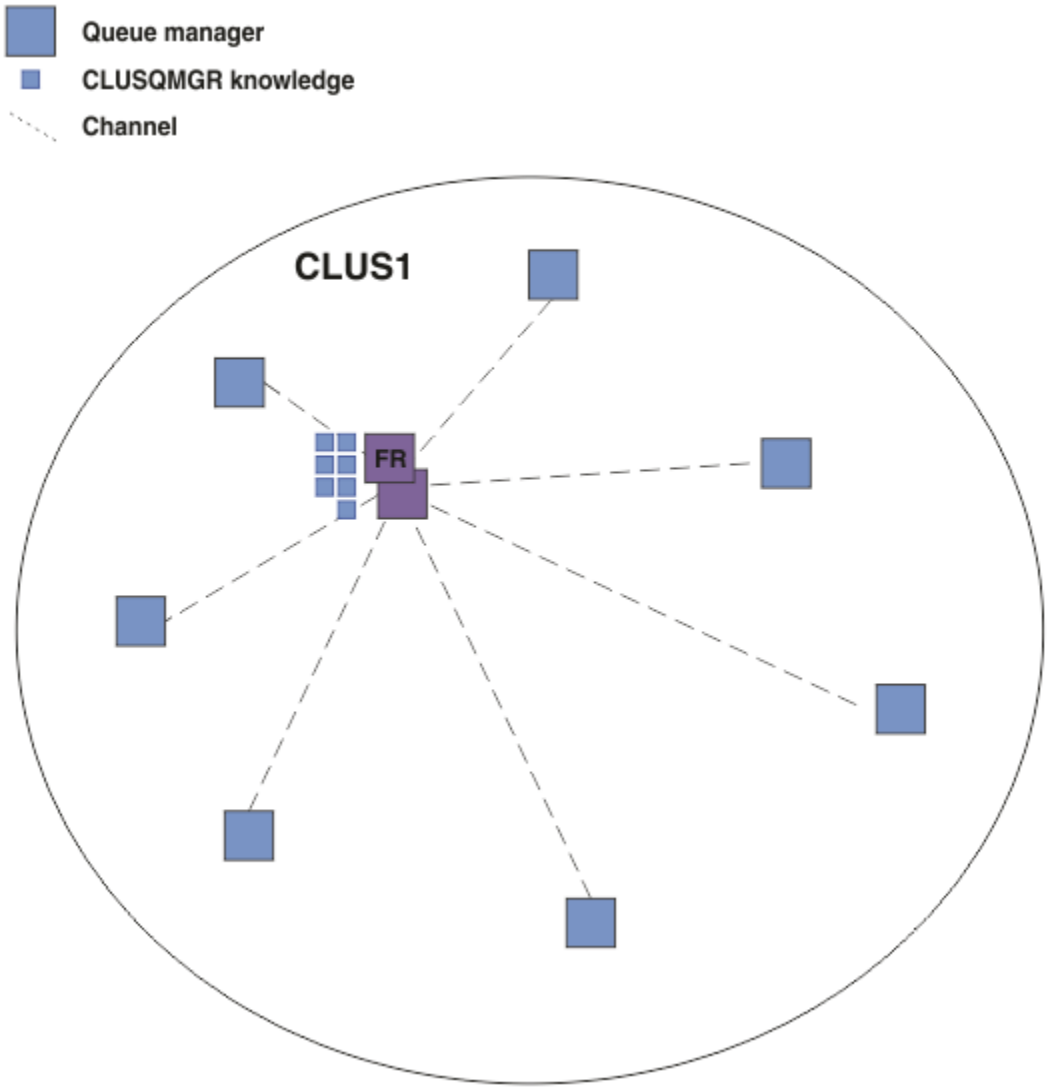


Figura 20. Un cluster di gestore code

In un cluster di pubblicazione / sottoscrizione instradato dell'host argomento, si definisce l'oggetto argomento su un gestore code specifico nel cluster. Il traffico di pubblicazione / sottoscrizione passa quindi attraverso tale gestore code, rendendolo un gestore code critico nel cluster e aumentandone il carico di lavoro. Per questi motivi si consiglia di non utilizzare un gestore code del repository completo, ma un altro gestore code nel cluster. Quando si definisce l'oggetto argomento sul gestore code host, la conoscenza dell'oggetto e del suo host viene automaticamente inviata, dai gestori code del repository completo, a tutti gli altri gestori code nel cluster. Notare che, a differenza dell' *instradamento diretto*, a ciascun gestore code non viene comunicato alcun altro gestore code nel cluster.

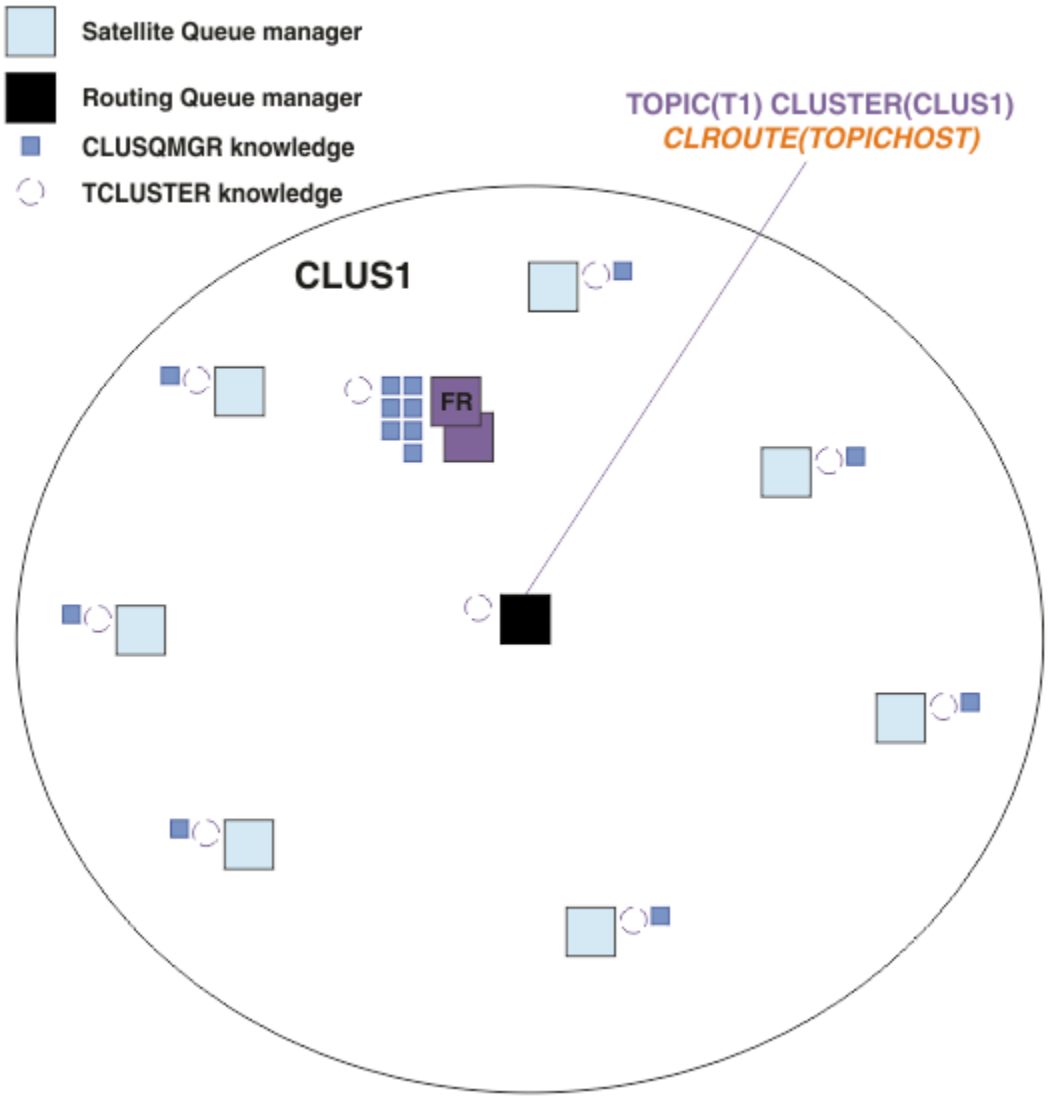


Figura 21. Un cluster di pubblicazione / sottoscrizione instradato dell'host argomento con un argomento definito su un host argomento

Quando una sottoscrizione viene creata su un gestore code, viene creato un canale tra il gestore code di sottoscrizione e il gestore code dell'host argomento. Il gestore code di sottoscrizione si connette solo al gestore code dell'host dell'argomento e invia i dettagli della sottoscrizione (sotto forma di *sottoscrizione proxy*). Il gestore code dell'host argomento non inoltra queste informazioni di sottoscrizione ad altri gestori code nel cluster.

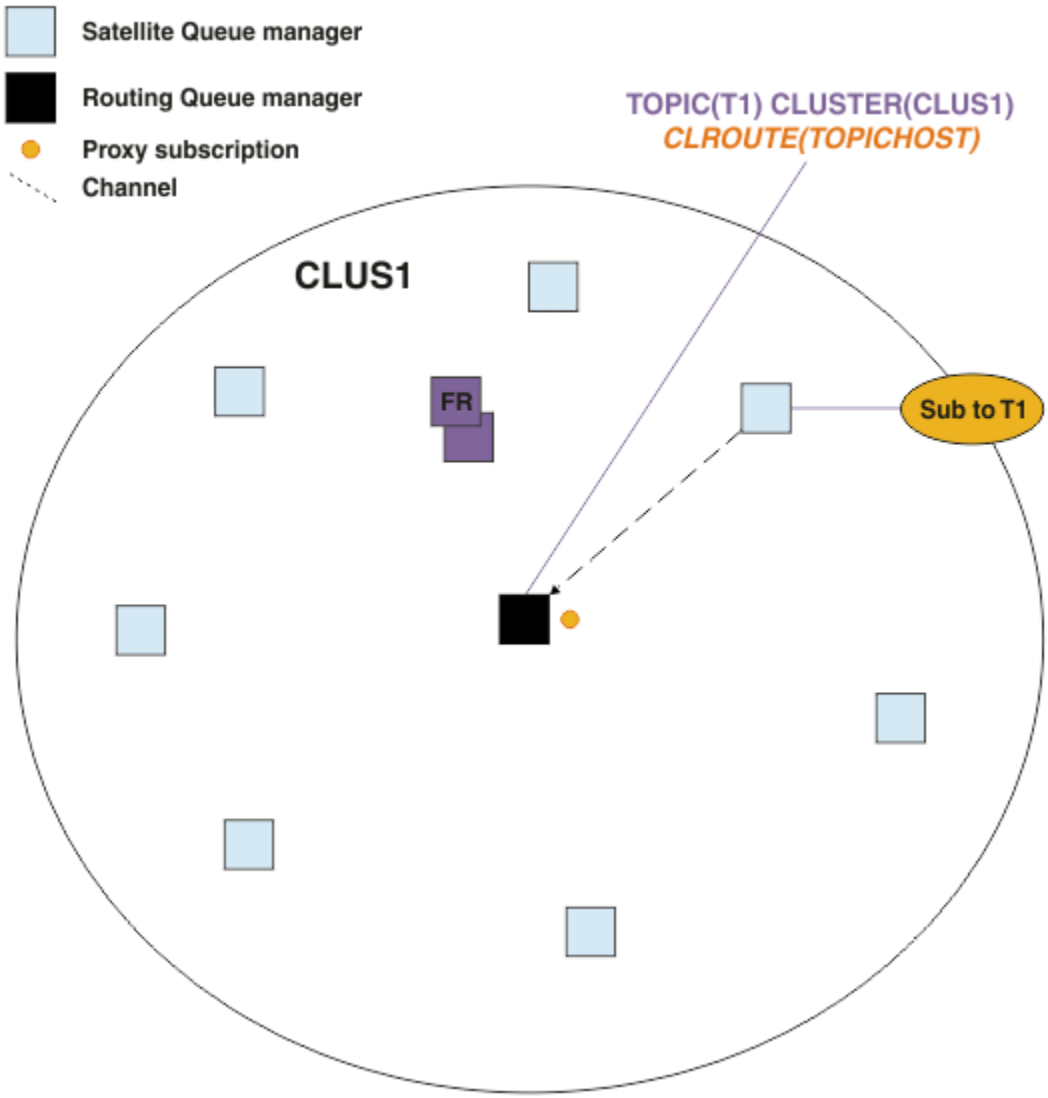


Figura 22. Un cluster di pubblicazione / sottoscrizione instradato dell'host argomento con un argomento definito su un host argomento e un sottoscrittore

Quando un'applicazione di pubblicazione si connette a un'altra gestore code e viene pubblicato un messaggio, viene creato un canale tra il gestore code di pubblicazione e il gestore code dell'host argomento e il messaggio viene inoltrato a tale gestore code. Il gestore code di pubblicazione non è a conoscenza di eventuali sottoscrizioni su altri gestori code nel cluster, quindi il messaggio viene inoltrato al gestore code dell'host argomento anche se non vi sono sottoscrittori a tale argomento nel cluster. Il gestore code di pubblicazione si collega solo al gestore code dell'host argomento. Le pubblicazioni vengono instradate tramite l'host argomento ai gestori code di sottoscrizione, se presenti.

Le sottoscrizioni sullo stesso gestore code del publisher vengono soddisfatte direttamente, senza inviare prima i messaggi a un gestore code dell'host argomento.

Tenere presente che, a causa del ruolo critico svolto da ciascun gestore code dell'host argomento, è necessario scegliere i gestori code che possono gestire i requisiti di carico, disponibilità e connettività dell'hosting dell'argomento.

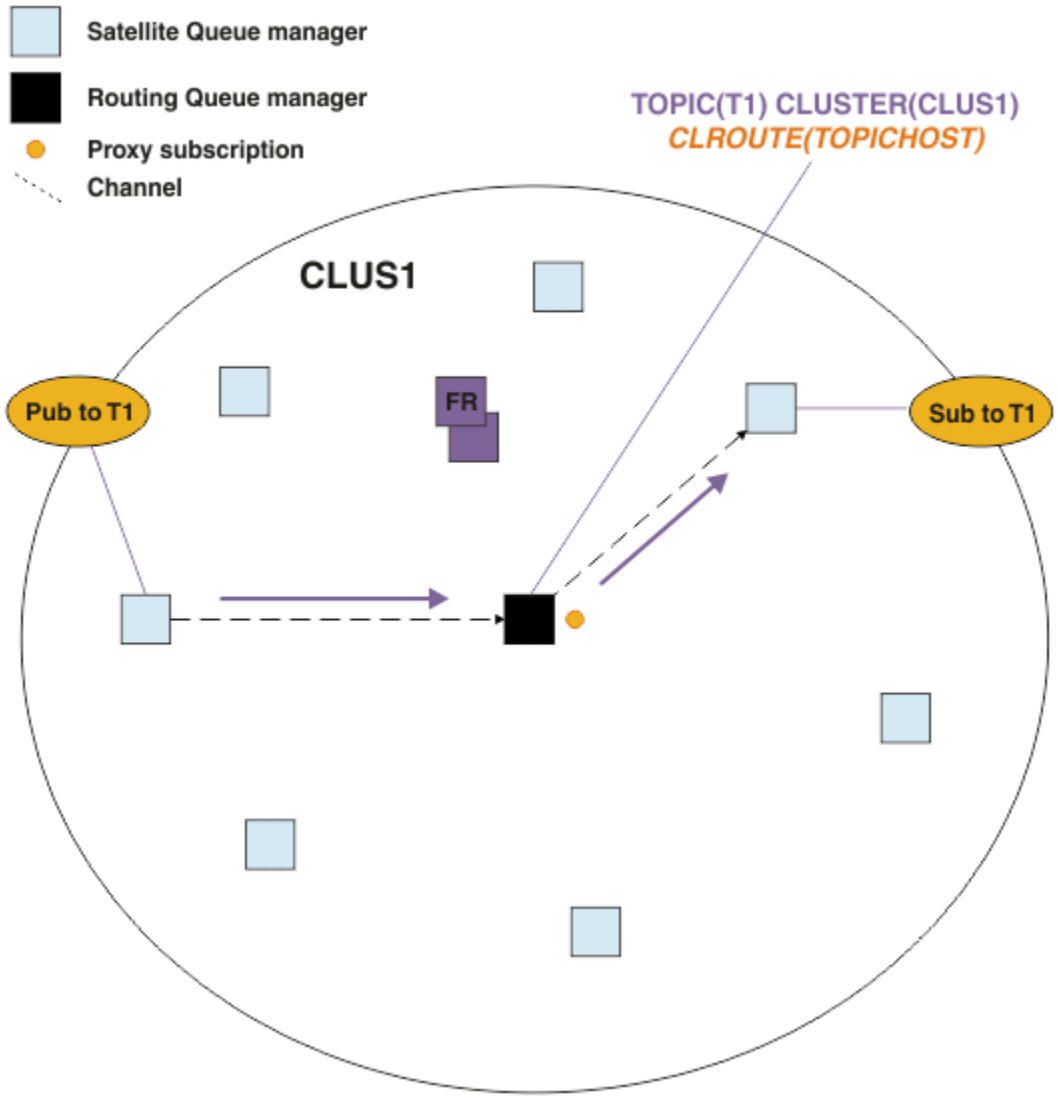


Figura 23. Un cluster di pubblicazione / sottoscrizione instradato dell'host argomento con un argomento, un sottoscrittore e un publisher

Divisione della struttura ad albero degli argomenti tra più gestori code

Un gestore code che ospita un argomento instradato è responsabile solo della conoscenza della sottoscrizione e dei messaggi di pubblicazione relativi al ramo della struttura ad albero dell'argomento per cui è configurato il suo oggetto argomento gestito. Se argomenti differenti vengono utilizzati da applicazioni di pubblicazione / sottoscrizione differenti nel cluster, è possibile configurare gestori code differenti per ospitare rami cluster differenti della struttura ad albero degli argomenti. Ciò consente la scalabilità riducendo il traffico di pubblicazione, la conoscenza della sottoscrizione e i canali su ciascun gestore code dell'host argomento nel cluster. Utilizzare questo metodo per i rami di volumi elevati distinti della struttura ad albero degli argomenti:

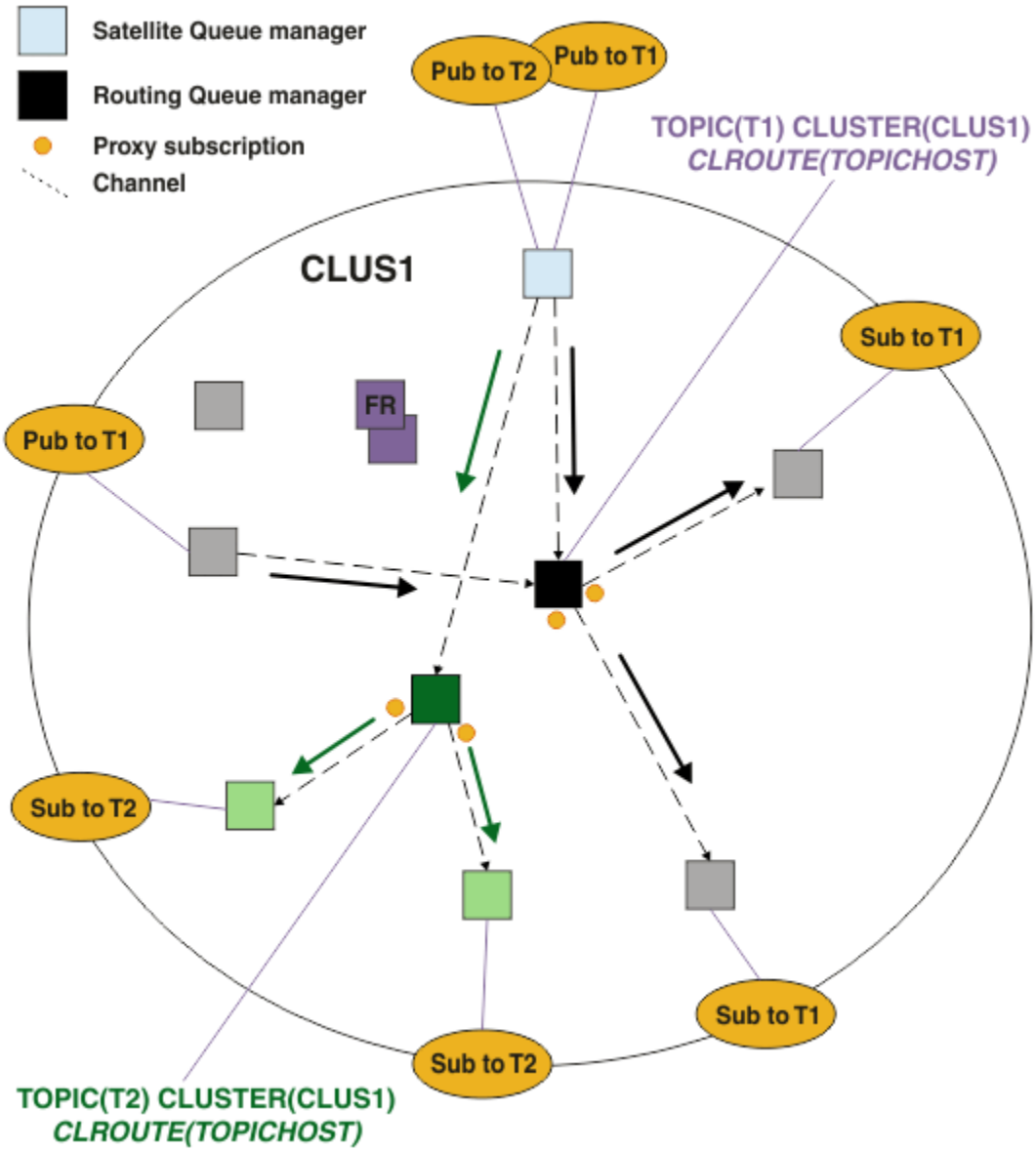


Figura 24. Un cluster di pubblicazione / sottoscrizione instradato dell'host argomento con due argomenti, ciascuno definito su un host argomento

Ad esempio, utilizzando gli argomenti descritti in Alberi argomenti, se l'argomento T1 è stato configurato con una stringa di argomenti `/USA/Alabamae` l'argomento T2 è stato configurato con una stringa di argomenti `/USA/Alaska`, un messaggio pubblicato in `/USA/Alabama/Mobile` verrà instradato tramite il gestore code che ospita T1, e un messaggio pubblicato in `/USA/Alaska/Juneau` verrà instradato tramite il gestore code su cui si trova T2.

Nota: Non è possibile eseguire una singola sottoscrizione su più rami cluster della struttura ad albero degli argomenti utilizzando un carattere jolly più in alto nella struttura ad albero degli argomenti rispetto ai punti raggruppati. Vedere Sottoscrizioni jolly.

Instradamento host argomento utilizzando più host argomento per un singolo argomento

Se un singolo gestore code ha la responsabilità dell'instradamento di un argomento e tale gestore code diventa non disponibile o non è in grado di gestire il carico di lavoro, le pubblicazioni non fluiranno prontamente nelle sottoscrizioni.

Se hai bisogno di maggiore resilienza, scalabilità e bilanciamento del carico di lavoro rispetto a quando definisci un argomento su un solo gestore code, puoi definire un argomento su più di un gestore code. Ogni singolo messaggio pubblicato viene instradato attraverso un unico host argomento. Quando esistono più definizioni host argomento corrispondenti, viene scelto uno degli host argomento. La scelta viene effettuata nello stesso modo delle code cluster. Ciò consente l'instradamento dei messaggi agli host argomento disponibili, evitando quelli non disponibili, e consente il bilanciamento del carico di lavoro del carico di lavoro tra più gestori code e canali dell'host argomento. Tuttavia, l'ordinamento tra più messaggi non viene mantenuto quando si utilizzano più host argomento per lo stesso argomento nel cluster.

Il seguente diagramma mostra un cluster di host argomento instradato in cui lo stesso argomento è stato definito su due gestori code. In questo esempio, i gestori code di sottoscrizione inviano informazioni sull'argomento sottoscritto a entrambi i gestori code dell'host argomento sotto forma di sottoscrizione proxy:

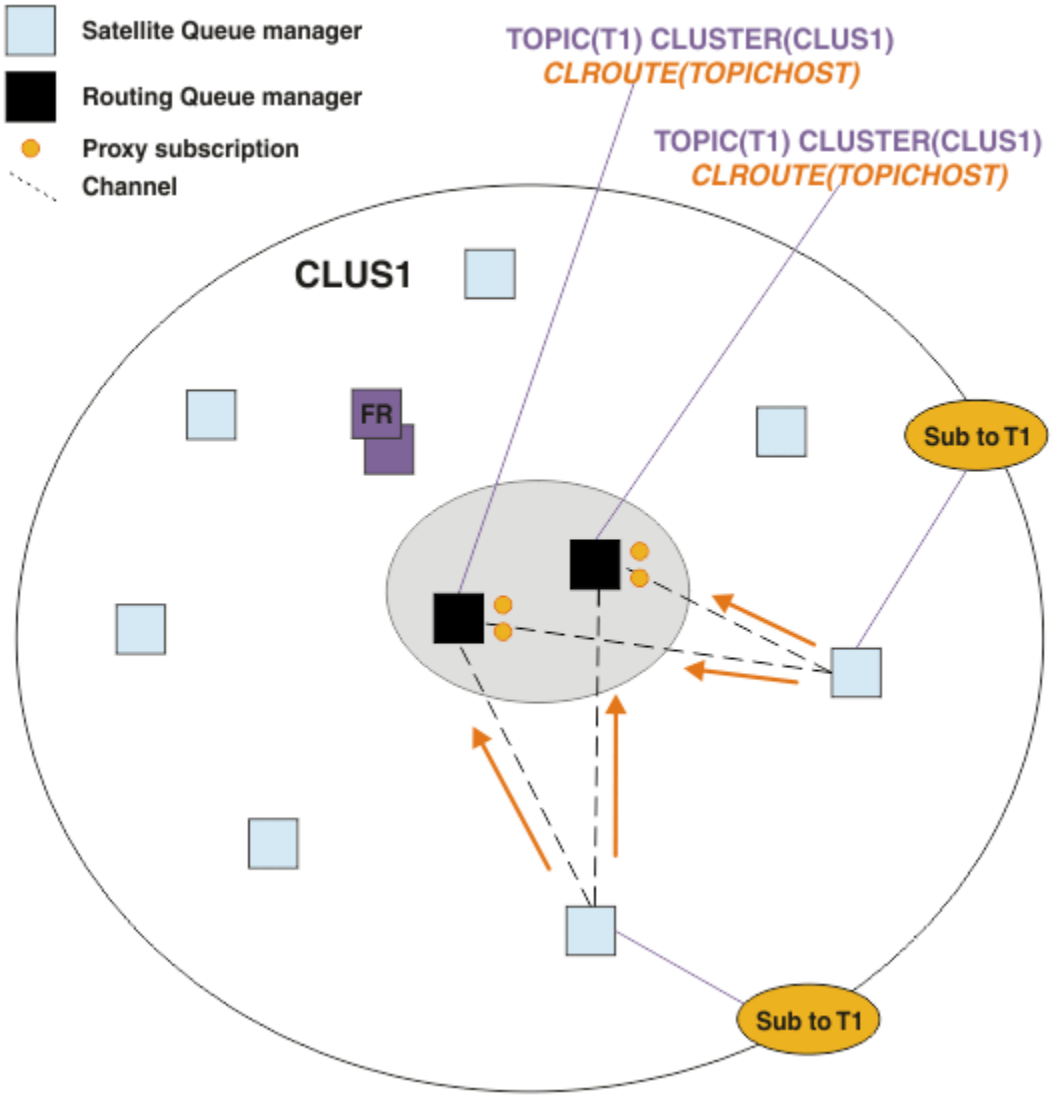


Figura 25. Creazione di sottoscrizioni proxy in un cluster di pubblicazione / sottoscrizione di più host argomento

Quando una pubblicazione viene effettuata da un gestore code non host, il gestore code invia una copia della pubblicazione a *uno* dei gestori code dell'host argomento per tale argomento. Il sistema sceglie l'host in base al comportamento predefinito dell' algoritmo di gestione del carico di lavoro del cluster. In un sistema tipico, questo valore si avvicina a una distribuzione round robin su ciascun gestore code dell'host argomento. Non esiste alcuna affinità tra i messaggi dalla stessa applicazione di pubblicazione; ciò equivale all'utilizzo di un bind cluster di tipo `NOTFIXED`.

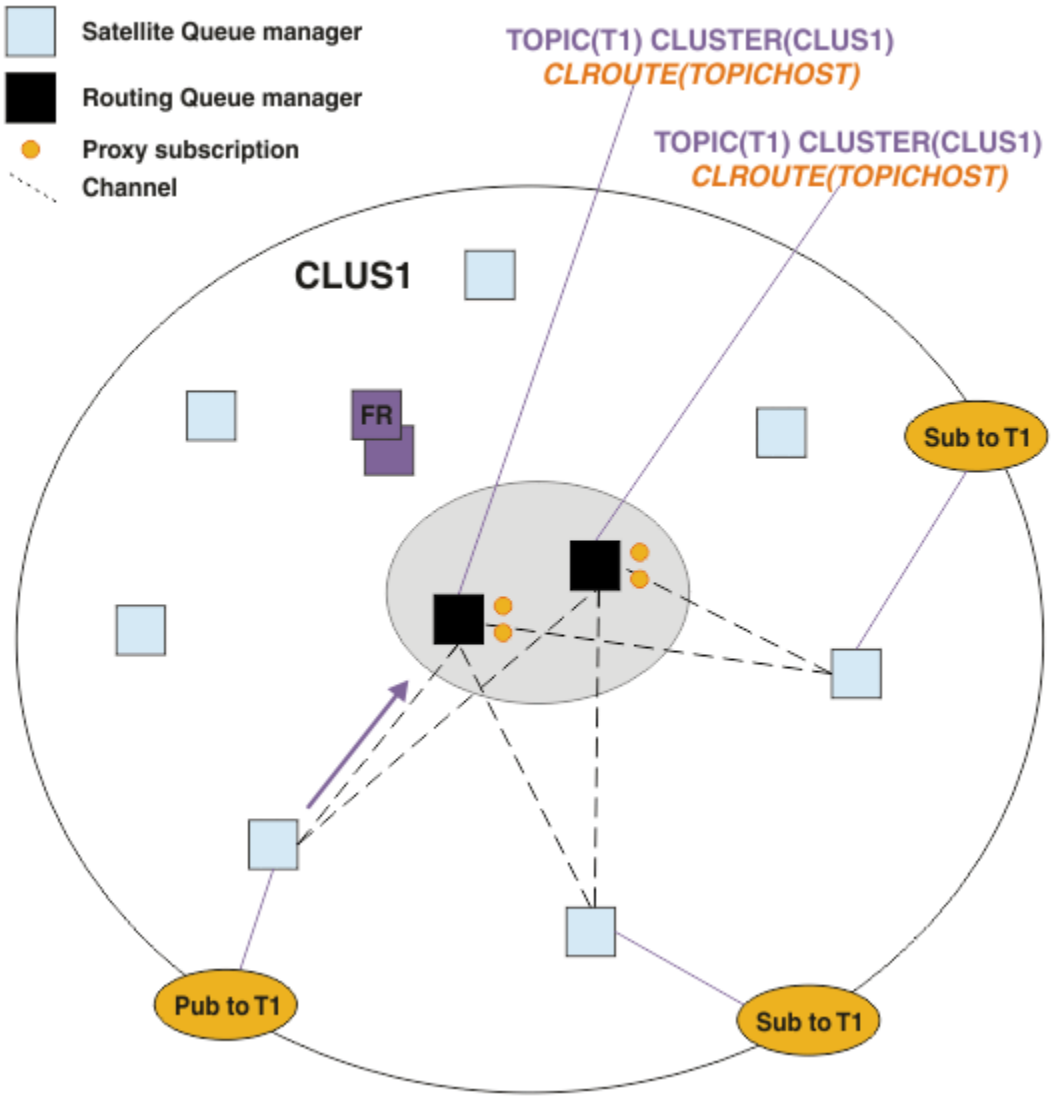


Figura 26. Ricezione di pubblicazioni in un cluster di pubblicazione / sottoscrizione di più host argomento

Le pubblicazioni in entrata per il gestore code dell'host argomento scelto vengono quindi inoltrate a tutti i gestori code che hanno registrato una sottoscrizione proxy corrispondente:

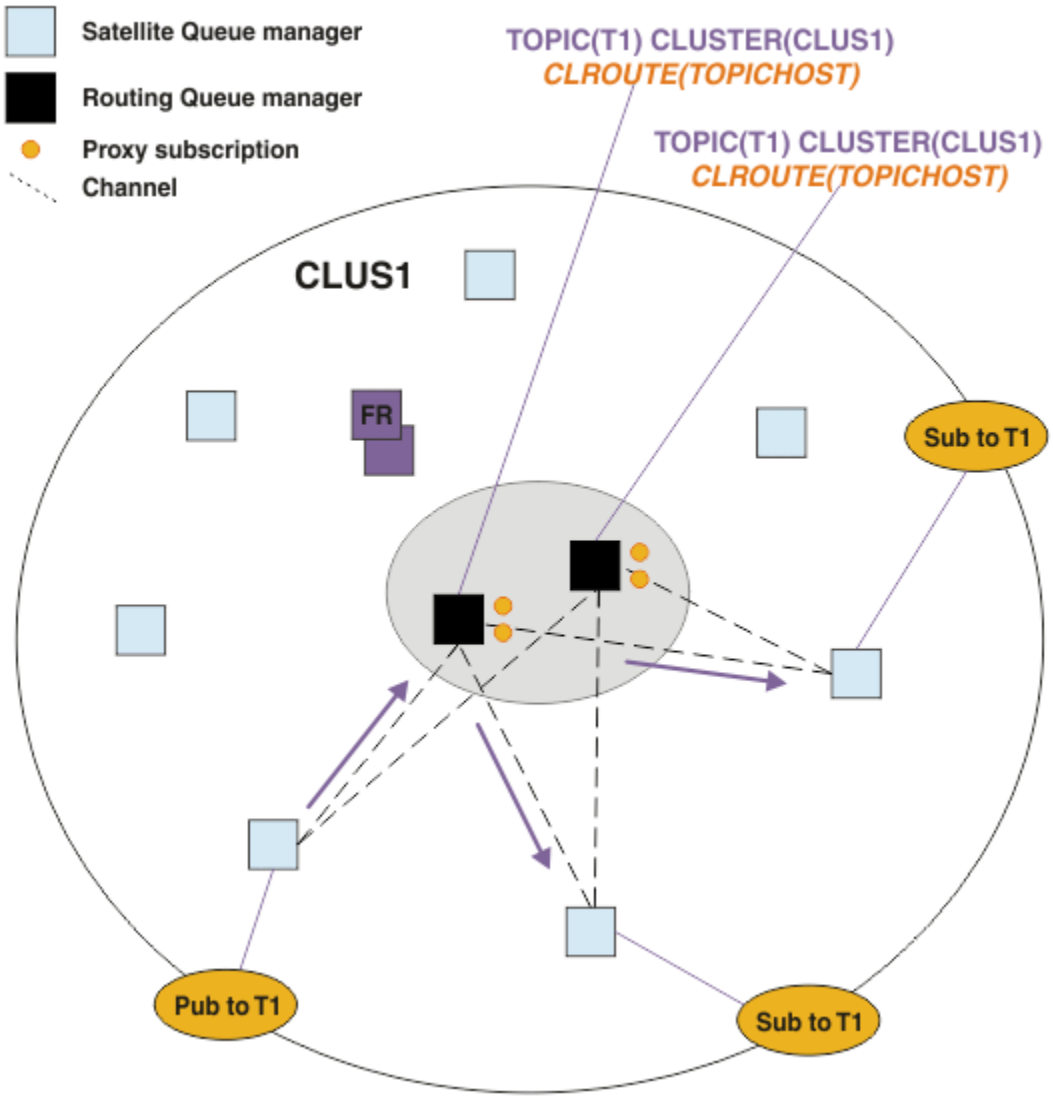


Figura 27. Instradamento delle pubblicazioni ai sottoscrittori in un cluster di pubblicazione / sottoscrizione di più host argomento

Come rendere le sottoscrizioni e i publisher locali per un gestore code dell'host argomento

Gli esempi precedenti mostrano l'instradamento tra i publisher e i sottoscrittori sui gestori code che non ospitano gli oggetti argomento instradati gestiti. In queste topologie, i messaggi richiedono più *hop* per raggiungere le sottoscrizioni.

Laddove l'hop aggiuntivo non è desiderato, potrebbe essere appropriato connettere i publisher di chiavi ai gestori code che ospitano gli argomenti. Tuttavia, se sono presenti più host argomento per un argomento e un solo publisher, tutto il traffico di pubblicazione verrà instradato attraverso il gestore code dell'host argomento a cui è connesso il publisher.

Allo stesso modo, se sono presenti sottoscrizioni chiave, queste potrebbero essere ubicate su un gestore code dell'host argomento. Tuttavia, se vi sono più host dell'argomento instradato, solo una parte delle pubblicazioni eviterà l'hop aggiuntivo, mentre il resto verrà instradato prima attraverso gli altri gestori code dell'host argomento.

Topologie come queste sono descritte più avanti: Instradamento host argomento utilizzando publisher o sottoscrittori centralizzati.

Nota: Una pianificazione speciale è necessaria se si modifica la configurazione dell'argomento instradato quando si co - localizzano i publisher o le sottoscrizioni con gli host dell'argomento instradati. Ad esempio, consultare Aggiunta di ulteriori host argomento a un cluster instradato host argomento.

Sintesi e considerazioni aggiuntive

Un cluster di pubblicazione / sottoscrizione instradato dell'host argomento fornisce un controllo preciso su quali gestori code ospitano ciascun argomento e tali gestori code diventano i gestori code di *instradamento* per quel ramo della struttura ad albero degli argomenti. Inoltre, i gestori code senza sottoscrizioni o publisher non hanno bisogno di connettersi ai gestori code dell'host argomento e i gestori code con sottoscrizioni non hanno bisogno di connettersi ai gestori code che non ospitano un argomento. Questa configurazione può ridurre in modo significativo il numero di connessioni tra gestori code nel cluster e la quantità di informazioni trasmesse tra gestori code. Ciò è particolarmente vero nei cluster di grandi dimensioni in cui solo un sottoinsieme di gestori code sta eseguendo attività di pubblicazione / sottoscrizione. Questa configurazione fornisce anche un certo controllo sul carico sui singoli gestori code nel cluster, per cui (ad esempio) è possibile scegliere di ospitare argomenti molto attivi su sistemi più potenti e resilienti. Per alcune configurazioni, in particolare per i cluster più grandi, di solito si tratta di una topologia più appropriata rispetto all' *instradamento diretto*.

Tuttavia, l'instradamento all'host argomento impone anche alcuni vincoli sul sistema:

- La configurazione e manutenzione del sistema richiedono una maggiore pianificazione rispetto all'instradamento diretto. È necessario decidere quali punti raggruppare nella struttura ad albero degli argomenti e la posizione delle definizioni di argomento nel cluster.
- Così come per gli argomenti con instradamento diretto, quando si definisce un nuovo argomento instradato all'host argomento, le informazioni vengono inviate ai gestori code del repository completo e da lì indirizzate a tutti i membri del cluster. Questo evento fa sì che i canali vengano avviati in ciascun membro del cluster da tutti i repository (se non già avviati).
- Le pubblicazioni vengono sempre inviate al gestore code host da un gestore code non host, anche se non sono presenti sottoscrizioni nel cluster. Pertanto, occorre utilizzare gli argomenti instradati quando è prevista l'esistenza di sottoscrizioni o quando il sovraccarico di connettività globale e conoscenza è maggiore del rischio di traffico di pubblicazione supplementare.

  Nota: Come descritto in precedenza, rendere i publisher locali per un host argomento può ridurre questo rischio.
- I messaggi che vengono pubblicati sui gestori code non host non vengono indirizzati direttamente al gestore code che ospita la sottoscrizione, ma vengono instradati sempre attraverso un gestore code dell'host argomento. Questo approccio può aumentare il sovraccarico totale nel cluster, nonché aumentare la latenza dei messaggi e ridurre le prestazioni.

  Nota: Come descritto in precedenza, rendere le sottoscrizioni o i publisher locali per un host argomento può ridurre questo rischio.
- L'utilizzo di un unico gestore code dell'host argomento introduce un singolo punto di errore per tutti i messaggi che vengono pubblicati in un argomento. È possibile rimuovere questo singolo punto di errore definendo più host argomento. Tuttavia, la presenza di più host influisce sull'ordine dei messaggi pubblicati man mano che vengono ricevuti dalle sottoscrizioni.
- Il carico di messaggi supplementare è sostenuto dai gestori code dell'host argomento, in quanto questi dovranno elaborare il traffico di pubblicazione da più gestori code. Questo carico può essere ridotto: utilizzare più host argomento per un singolo argomento (nel qual caso l'ordine dei messaggi non viene mantenuto) o utilizzare gestori code differenti per ospitare gli argomenti instradati per i diversi rami di una struttura ad albero degli argomenti.

Prima di utilizzare l'instradamento dell'host argomento, esplorare gli approcci alternativi descritti in “Instradamento diretto nei cluster di pubblicazione / sottoscrizione” a pagina 78e “Instradamento nelle gerarchie di pubblicazione / sottoscrizione” a pagina 108.

Clustering di pubblicazione / sottoscrizione: procedure ottimali

L'utilizzo di argomenti raggruppati rende semplice l'estensione del dominio di pubblicazione / sottoscrizione tra gestori code, ma può portare a problemi se i meccanismi e le implicazioni non sono completamente compresi. Esistono due modelli per la condivisione delle informazioni e l'instradamento delle pubblicazioni. Implementare il modello che meglio soddisfa le singole esigenze di business e si comporta al meglio sul cluster scelto.

Le informazioni sulle migliori pratiche riportate nelle seguenti sezioni non forniscono una soluzione unica per tutte le soluzioni, ma condividono piuttosto approcci comuni per risolvere problemi comuni. Si presume che si abbia una conoscenza di base dei cluster IBM MQ e della messaggistica di pubblicazione / sottoscrizione e che si abbia familiarità con le informazioni nelle reti di pubblicazione / sottoscrizione distribuite e “Progettazione di cluster di pubblicazione / sottoscrizione” a pagina 76.

Quando si utilizza un cluster per la messaggistica point - to - point, ogni gestore code nel cluster funziona in base alla necessità di sapere. In altre parole, rileva solo altre risorse del cluster, ad esempio altri gestori code nel cluster e code cluster, quando le applicazioni che si collegano ad essi richiedono di utilizzarle. Quando si aggiunge la messaggistica di pubblicazione / sottoscrizione a un cluster, viene introdotto un livello maggiore di condivisione delle informazioni e di connettività tra i gestori code del cluster. Per poter seguire le procedure ottimali per i cluster di pubblicazione / sottoscrizione, è necessario comprendere appieno le implicazioni di questa modifica del comportamento.

Per consentirti di creare l'architettura migliore, in base alle tue precise esigenze, ci sono due modelli per la condivisione delle informazioni e l'instradamento della pubblicazione nei cluster di pubblicazione / sottoscrizione: *instradamento diretto* e *instradamento dell'host argomento*. Per fare la giusta scelta, è necessario comprendere entrambi i modelli e i diversi requisiti che ogni modello soddisfa. Questi requisiti sono discussi nelle sezioni seguenti, insieme a “Pianificazione della rete di pubblicazione / sottoscrizione distribuita” a pagina 73:

- “Motivi per limitare il numero di gestori code del cluster coinvolti nell'attività di pubblicazione / sottoscrizione” a pagina 93
- “Come decidere quali argomenti raggruppare” a pagina 94
- “Come dimensionare il sistema” a pagina 94
- “Ubicazione di pubblicazione e sottoscrizione” a pagina 95
- “Traffico di pubblicazione” a pagina 96
- “Modifica della sottoscrizione e stringhe di argomenti dinamici” a pagina 96

Motivi per limitare il numero di gestori code del cluster coinvolti nell'attività di pubblicazione / sottoscrizione

Esistono considerazioni sulla capacità e sulle prestazioni quando si utilizza la messaggistica di pubblicazione / sottoscrizione in un cluster. Di conseguenza, è consigliabile considerare attentamente la necessità di attività di pubblicazione / sottoscrizione tra i gestori code e limitarla solo al numero di gestori code che lo richiedono. Una volta identificata la serie minima di gestori code che devono pubblicare e sottoscrivere gli argomenti, è possibile renderli membri di un cluster che contiene solo loro e nessun altro gestore code.

Questo approccio è particolarmente utile se si dispone di un cluster stabilito che funziona già bene per la messaggistica point - to - point. Quando si trasforma un cluster di grandi dimensioni esistente in un cluster di pubblicazione / sottoscrizione, si consiglia di creare inizialmente un cluster separato per il lavoro di pubblicazione / sottoscrizione in cui è possibile provare le applicazioni, piuttosto che utilizzare il cluster corrente. È possibile utilizzare un sottoinsieme di gestori code esistenti che si trovano già in uno o più cluster point - to - point e rendere questo sottoinsieme membro del nuovo cluster di pubblicazione / sottoscrizione. Tuttavia, i gestori code del repository completo per il nuovo cluster non devono essere membri di nessun altro cluster; ciò isola il carico aggiuntivo dai repository completi del cluster esistenti.

Se non è possibile creare un nuovo cluster e si deve trasformare un cluster di grandi dimensioni esistente in un cluster di pubblicazione / sottoscrizione, non utilizzare un modello instradato direttamente. Il modello di host argomento instradato di solito funziona meglio in cluster più grandi, perché in genere

limita la condivisione delle informazioni di pubblicazione / sottoscrizione e la connettività alla serie di gestori code che stanno eseguendo attivamente il lavoro di pubblicazione / sottoscrizione, concentrandosi sui gestori code che ospitano gli argomenti. L'eccezione è rappresentata dal fatto che un aggiornamento manuale delle informazioni di sottoscrizione viene richiamato su un gestore code che ospita una definizione di argomento, a quel punto il gestore code dell'host argomento si connetterà a ogni gestore code nel cluster. Consultare Risincronizzazione delle sottoscrizioni proxy.

Se si stabilisce che un cluster non può essere utilizzato per la pubblicazione / sottoscrizione a causa della sua dimensione o del carico corrente, si consiglia di evitare che questo cluster venga inaspettatamente trasformato in un cluster di pubblicazione / sottoscrizione. Utilizzare la proprietà del gestore code **PSCLUS** per arrestare gli utenti che aggiungono un argomento in cluster su qualsiasi gestore code nel cluster. Consultare “Blocco della pubblicazione / sottoscrizione in cluster” a pagina 103.

Come decidere quali argomenti raggruppare

È importante scegliere attentamente quali argomenti vengono aggiunti al cluster: più in alto nella struttura ad albero degli argomenti si trovano questi argomenti, più diventa diffuso il loro utilizzo. Ciò può causare la propagazione di un numero maggiore di informazioni di sottoscrizione e di pubblicazioni rispetto al necessario. Se ci sono più rami distinti della struttura ad albero degli argomenti, dove alcuni devono essere raggruppati in cluster e altri no, creare oggetti argomento gestiti alla radice di ogni ramo che necessita di cluster e aggiungerli al cluster. Ad esempio, se i rami `/A`, `/B` e `/C` necessitano di cluster, definire un oggetto argomento cluster separato per ogni ramo.

Nota: Il sistema impedisce di nidificare definizioni di argomenti in cluster nella struttura ad albero degli argomenti. È possibile raggruppare gli argomenti solo in un punto della struttura ad albero degli argomenti per ogni ramo secondario. Ad esempio, non è possibile definire oggetti argomento in cluster per `/A` e per `/A/B`. La nidificazione degli argomenti del cluster può creare confusione su quale oggetto del cluster si applica a quale sottoscrizione, specialmente quando le sottoscrizioni utilizzano caratteri jolly. Ciò è ancora più importante quando si utilizza l'instradamento dell'host argomento, dove le decisioni di instradamento sono definite in modo preciso dall'assegnazione degli host argomento.

Se gli argomenti in cluster devono essere aggiunti in alto nella struttura ad albero degli argomenti, ma alcuni rami della struttura ad albero al di sotto del punto in cluster non richiedono il funzionamento in cluster, è possibile utilizzare gli attributi dell'ambito della sottoscrizione e della pubblicazione per ridurre il livello di condivisione della sottoscrizione e della pubblicazione per ulteriori argomenti.

Non inserire il nodo root dell'argomento nel cluster senza considerare il comportamento visualizzato. Rendere gli argomenti globali ovvi laddove possibile, ad esempio utilizzando un qualificatore di alto livello nella stringa di argomenti: `/global` o `/cluster`.

Vi è un ulteriore motivo per non voler creare il nodo dell'argomento root in cluster. Ciò è dovuto al fatto che ogni gestore code dispone di una definizione locale per il nodo root, l'oggetto argomento `SYSTEM.BASE.TOPIC` . Quando questo oggetto viene raggruppato in cluster su un gestore code nel cluster, tutti gli altri gestori code ne vengono informati. Tuttavia, quando esiste una definizione locale dello stesso oggetto, le relative proprietà sovrascrivono l'oggetto cluster. Ciò si traduce in quei gestori code che agiscono come se l'argomento non fosse raggruppato in cluster. Per risolvere questo problema, è necessario raggruppare ogni definizione di `SYSTEM.BASE.TOPIC`. È possibile eseguire questa operazione per le definizioni di instradamento diretto, ma non per le definizioni di instradamento dell'host argomento, poiché ogni gestore code diventa un host argomento.

Come dimensionare il sistema

I cluster di pubblicazione / sottoscrizione generalmente risultano in un modello diverso di canali cluster per la messaggistica point - to - point in un cluster. Il modello point - to - point è un modello 'opt in', ma i cluster di pubblicazione / sottoscrizione hanno una natura più indiscriminata con fan - out di sottoscrizione, specialmente quando si utilizzano argomenti instradati direttamente. Pertanto, è importante identificare quali gestori code in un cluster di pubblicazione / sottoscrizione utilizzeranno i canali cluster per connettersi ad altri gestori code e in quali circostanze.

La seguente tabella elenca la serie tipica di canali mittente e ricevente del cluster prevista per ogni gestore code in un cluster di pubblicazione / sottoscrizione in esecuzione normale, in base al ruolo del gestore code nel cluster di pubblicazione / sottoscrizione.

Tabella 5. Canali mittente e destinatario cluster per ogni metodo di instradamento.

Ruolo gestore code	Ricevitori cluster diretti	Mittenti cluster diretti	Ricevitori cluster argomento	Mittenti cluster argomento
Repository completo	AllQmgrs	AllQmgrs	AllQmgrs	AllQMgrs
Host della definizione argomento	n/a	n/a	AllSubs+AllPubs (1)	AllSubs (1)
Sottoscrizioni create	AllPubs (1)	AllQMgrs	AllHosts	AllHosts
Publisher connessi	AllSubs (1)	AllSubs (1)	AllHosts	AllHosts
Nessun publisher o sottoscrittore	AllSubs (1)	Nessuno (1)	Nessuno (2)	Nessuno (2)

Chiave:

AllQmgrs
Un canale da e verso ogni gestore code nel cluster.

AllSubs
Un canale da e verso ogni gestore code in cui è stata creata una sottoscrizione.

AllPubs
Un canale da e verso ogni gestore code a cui è stata connessa un'applicazione di pubblicazione.

AllHosts
Un canale da e verso ogni gestore code in cui è stata configurata una definizione dell'oggetto argomento con cluster.

Nessuna
Nessun canale verso o da altri gestori code nel cluster per il solo scopo della messaggistica di pubblicazione / sottoscrizione.

Note:

1. Se un aggiornamento del gestore code delle sottoscrizioni proxy viene effettuato da questo gestore code, un canale da e verso tutti gli altri gestori code nel cluster potrebbe essere creato automaticamente.
2. Se un aggiornamento del gestore code delle sottoscrizioni proxy viene effettuato da questo gestore code, un canale verso e da qualsiasi altro gestore code nel cluster che ospita una definizione di un argomento del cluster potrebbe essere creato automaticamente.

La tabella precedente mostra che l'instradamento host argomento in genere utilizza meno canali mittente e ricevente del cluster rispetto all'instradamento diretto. Se la connettività del canale è un problema per alcuni gestori code in un cluster, per motivi di capacità o capacità di stabilire determinati canali (ad esempio, tramite i firewall), l'instradamento dell'host argomento è pertanto una soluzione preferita.

Ubicazione di pubblicazione e sottoscrizione

La pubblicazione / sottoscrizione in cluster consente ai messaggi pubblicati su un gestore code di essere consegnati alle sottoscrizioni su qualsiasi altro gestore code nel cluster. Per quanto riguarda la messaggistica point - to - point, il costo di trasmissione dei messaggi tra gestori code può essere dannoso per le prestazioni. Pertanto, è necessario considerare la possibilità di creare sottoscrizioni agli argomenti sugli stessi gestori code in cui vengono pubblicati i messaggi.

Quando si utilizza l'instradamento dell'host argomento in un cluster, è importante considerare anche l'ubicazione delle sottoscrizioni e dei publisher rispetto ai gestori code che ospitano l'argomento. Quando

il publisher non è connesso a un gestore code che è un host dell'argomento cluster, i messaggi pubblicati vengono sempre inviati a un gestore code che ospita l'argomento. Allo stesso modo, quando una sottoscrizione viene creata su un gestore code che non è un host argomento per un argomento cluster, i messaggi pubblicati da altri gestori code nel cluster vengono sempre inviati prima a un gestore code che ospita un argomento. In modo più specifico, se la sottoscrizione si trova su un gestore code che ospita l'argomento, ma sono presenti uno o più altri gestori code che ospitano lo stesso argomento, una proporzione di pubblicazioni provenienti da altri gestori code viene instradata attraverso gli altri gestori code che ospitano l'argomento. Per ulteriori informazioni sulla progettazione di un cluster di pubblicazione / sottoscrizione instradato dell'host argomento per ridurre la distanza tra i publisher e le sottoscrizioni, consultare Instradamento dell'host argomento utilizzando i publisher o i sottoscrittori centralizzati .

Traffico di pubblicazione

I messaggi pubblicati da un'applicazione connessa a un gestore code in un cluster vengono trasmessi alle sottoscrizioni su altri gestori code utilizzando i canali mittente del cluster.

Quando si utilizza l'instradamento diretto, i messaggi pubblicati utilizzano il percorso più breve tra i gestori code. In altre parole, passano direttamente dal gestore code di pubblicazione a ciascuno dei gestori code con sottoscrizioni. I messaggi non vengono trasmessi ai gestori code che non hanno sottoscrizioni per l'argomento. Consultare Sottoscrizioni proxy in una rete di pubblicazione / sottoscrizione.

Quando la frequenza dei messaggi di pubblicazione tra un gestore code e un altro nel cluster è elevata, l'infrastruttura del canale cluster tra questi due punti deve essere in grado di mantenere la frequenza. Ciò potrebbe implicare l'ottimizzazione dei canali e della coda di trasmissione utilizzati.

Quando si utilizza l'instradamento dell'host argomento, ogni messaggio pubblicato su un gestore code che non è un host argomento viene trasmesso a un gestore code dell'host argomento. Ciò è indipendente dal fatto che una o più sottoscrizioni siano presenti in qualsiasi altro punto del cluster. Ciò introduce ulteriori fattori da considerare nella pianificazione:

- La latenza aggiuntiva dell'invio di ciascuna pubblicazione a un gestore code dell'host argomento è accettabile?
- Ciascun gestore code dell'host argomento può sostenere la frequenza di pubblicazione in entrata e in uscita? Considerare un sistema con publisher su molti gestori code differenti. Se tutti inviano i messaggi a una serie molto piccola di gestori code che ospitano argomenti, tali host argomento potrebbero diventare un collo di bottiglia nell'elaborazione di tali messaggi e nell'indirizzarli ai gestori code di sottoscrizione.
- Si prevede che una percentuale significativa dei messaggi pubblicati non avrà un sottoscrittore corrispondente? In tal caso, e la frequenza di pubblicazione di tali messaggi è elevata, potrebbe essere preferibile rendere il gestore code del publisher un host argomento. In questa situazione, qualsiasi messaggio pubblicato in cui non esistono sottoscrizioni nel cluster non verrà trasmesso ad altri gestori code.

Questi problemi potrebbero anche essere risolti introducendo più host di argomenti, per distribuire il carico di pubblicazione su di essi:

- In presenza di più argomenti distinti, ciascuno con una parte del traffico di pubblicazione, considerare la possibilità di ospitarli su gestori code differenti.
- Se gli argomenti non possono essere separati su host di argomenti differenti, considerare la possibilità di definire lo stesso oggetto argomento su più gestori code. Ciò si traduce in un bilanciamento del carico di lavoro delle pubblicazioni per l'instradamento. Tuttavia, ciò è appropriato solo quando non è richiesto l'ordinamento dei messaggi di pubblicazione.

Modifica della sottoscrizione e stringhe di argomenti dinamici

Un'altra considerazione è l'effetto sulle prestazioni del sistema per la propagazione delle sottoscrizioni proxy. In genere, un gestore code invia un messaggio di sottoscrizione proxy ad alcuni altri gestori code nel cluster quando viene creata la prima sottoscrizione per una specifica stringa di argomenti in cluster

(non solo un oggetto argomento configurato) su tale gestore code. Allo stesso modo, un messaggio di eliminazione della sottoscrizione proxy viene inviato quando viene eliminata l'ultima sottoscrizione per una specifica stringa di argomenti in cluster.

Per l'instradamento diretto, ogni gestore code con sottoscrizioni invia tali sottoscrizioni proxy a ogni altro gestore code nel cluster. Per l'instradamento dell'host argomento, ogni gestore code con sottoscrizioni invia solo le sottoscrizioni proxy a ciascun gestore code che ospita una definizione per tale argomento del cluster. Pertanto, con l'instradamento diretto, maggiore è il numero di gestori code presenti nel cluster, maggiore è il sovraccarico di gestione delle sottoscrizioni proxy. Mentre, con l'instradamento dell'host argomento, il numero di gestori code nel cluster non è un fattore.

In entrambi i modelli di instradamento, se una soluzione di pubblicazione / sottoscrizione è composta da molte stringhe di argomenti univoche sottoscritte, o gli argomenti su un gestore code nel cluster sono frequentemente sottoscritti e annullati, verrà visualizzato un sovraccarico significativo su tale gestore code, causato dalla costante generazione di messaggi che distribuiscono ed eliminano le sottoscrizioni proxy. Con l'instradamento diretto, a ciò si aggiunge la necessità di inviare questi messaggi a ogni gestore code nel cluster.

Se la frequenza di modifica delle sottoscrizioni è troppo elevata per essere adattata, anche all'interno di un sistema instradato dell'host argomento, consultare Prestazioni della sottoscrizione nelle reti di pubblicazione / sottoscrizione per informazioni sui modi per ridurre il sovraccarico della sottoscrizione proxy.

Definizione degli argomenti del cluster

sono argomenti di amministrazione con l'attributo **cluster** definito. Le informazioni sugli argomenti cluster vengono inoltrate a tutti i membri di un cluster e combinate con argomenti locali per creare parti di uno spazio argomento che si estende su più gestori code. Ciò fa sì che i messaggi pubblicati su un argomento in un gestore code vengano consegnati alle sottoscrizioni di altri gestori code nel cluster.

Quando si definisce un argomento cluster su un gestore code, la definizione dell'argomento cluster viene inviata ai gestori code del repository completo. I repository completi propagano quindi la definizione dell'argomento cluster a tutti i gestori code all'interno del cluster, rendendo disponibile lo stesso argomento cluster ai publisher e sottoscrittori di qualsiasi gestore code del cluster. Il gestore code su cui si crea un argomento cluster è noto come host dell'argomento cluster. L'argomento cluster può essere utilizzato da qualsiasi gestore code nel cluster, ma le modifiche a un cluster devono essere effettuate sul gestore code dove è definito tale argomento (l'host) nel punto in cui la modifica viene propagata a tutti i membri del cluster attraverso i repository completi.

Quando si utilizza l'instradamento diretto, l'ubicazione della definizione dell'argomento in cluster non influenza direttamente il comportamento del sistema, poiché tutti i gestori code nel cluster utilizzano la definizione dell'argomento nello stesso modo. Pertanto, è necessario definire l'argomento su qualsiasi gestore code che sarà membro del cluster per tutto il tempo necessario e che si trova su un sistema sufficientemente affidabile da essere regolarmente in contatto con i gestori code del repository completo.

Quando si utilizza l'instradamento dell'host argomento, l'ubicazione della definizione dell'argomento in cluster è molto importante, poiché altri gestori code nel cluster creano canali a questo gestore code e inviano ad esso informazioni di sottoscrizione e pubblicazioni. Per scegliere il gestore code migliore per ospitare la definizione dell'argomento, è necessario comprendere l'instradamento dell'host dell'argomento. Consultare “Instradamento host argomento nei cluster di pubblicazione / sottoscrizione” a pagina 83.

Se si dispone di un argomento in cluster e di un oggetto argomento locale, l'argomento locale ha la precedenza. Consultare “Più definizioni di argomenti cluster con lo stesso nome” a pagina 100.

Per informazioni sui comandi da utilizzare per visualizzare gli argomenti cluster, consultare le informazioni correlate.

Eredità argomenti raggruppati

Generalmente, le applicazioni di pubblicazione e sottoscrizione in una topologia di pubblicazione / sottoscrizione in cluster si aspettano di funzionare allo stesso modo, indipendentemente dal gestore

code nel cluster a cui sono connesse. Questo è il motivo per cui gli oggetti argomento gestiti in cluster vengono propagati a ogni gestore code nel cluster.

Un oggetto argomento gestito eredita il suo comportamento da altri oggetti argomento gestiti più in alto nella struttura ad albero degli argomenti. Questa eredità si verifica quando non è stato impostato un valore esplicito per un parametro dell'argomento.

Nel caso di pubblicazione / sottoscrizione in cluster, è importante considerare tale eredità perché introduce la possibilità che i publisher e i sottoscrittori si comportino in modo diverso a seconda del gestore code a cui si connettono. Se un oggetto argomento in cluster lascia dei parametri per ereditare da oggetti argomento superiori, l'argomento potrebbe comportarsi in modo diverso su gestori code differenti nel cluster. Allo stesso modo, gli oggetti argomento definiti localmente definiti al di sotto di un oggetto argomento in cluster nella struttura ad albero degli argomenti indicano che tali argomenti inferiori sono ancora in cluster, ma l'oggetto locale potrebbe modificarne il funzionamento in modo diverso rispetto ad altri gestori code nel cluster.

Sottoscrizioni jolly

Le sottoscrizioni proxy vengono create quando le sottoscrizioni locali vengono effettuate a una stringa di argomenti che si risolve in un oggetto argomento del cluster o al di sotto di esso. Se una sottoscrizione con caratteri jolly viene effettuata più in alto nella gerarchia di argomenti rispetto a qualsiasi argomento cluster, non dispone di sottoscrizioni proxy inviate intorno al cluster per l'argomento cluster corrispondente e pertanto non riceve alcuna pubblicazione da altri membri del cluster. Tuttavia, riceve pubblicazioni dal gestore code locale.

Tuttavia, se un'altra applicazione effettua la sottoscrizione a una stringa di argomenti che si risolve in o al di sotto dell'argomento del cluster, le sottoscrizioni proxy vengono generate e le pubblicazioni vengono propagate a questo gestore code. All'arrivo, la sottoscrizione di un carattere jolly originale e superiore è considerata un destinatario legittimo di tali pubblicazioni e riceve una copia. Se questo comportamento non è richiesto, impostare **`WILDCARD(BLOCK)`** sull'argomento del cluster. Ciò rende il carattere jolly originale non considerato una sottoscrizione legittima e arresta la ricezione di qualsiasi pubblicazione (locale o da un altro punto del cluster) sull'argomento del cluster o sui relativi argomenti secondari.

Concetti correlati

Utilizzo degli argomenti di gestione

Utilizzo delle sottoscrizioni

Riferimenti correlati

VISUALIZZAZIONEARGOMENTO

STATOVISUALIZZAZIONEP

VISUALIZZAZIONESUB

Attributi argomento cluster

Quando un oggetto argomento ha l'attributo del nome cluster impostato, la definizione dell'argomento viene propagata a tutti i gestori code nel cluster. Ogni gestore code utilizza gli attributi dell'argomento propagato per controllare il comportamento delle applicazioni di pubblicazione / sottoscrizione.

Un oggetto argomento ha diversi attributi che si applicano ai cluster di pubblicazione / sottoscrizione. Alcuni controllano il comportamento generale delle applicazioni di pubblicazione e sottoscrizione e altri il modo in cui l'argomento viene utilizzato nel cluster.

Una definizione di oggetto argomento con cluster deve essere configurata in modo che tutti i gestori code nel cluster possano utilizzarla correttamente.

Ad esempio, se le code modello da utilizzare per le sottoscrizioni gestite (`MDURMDL` e `MNDURMDL`) sono impostati su un nome coda non predefinito, tale coda modello denominata deve essere definita su tutti i gestori code in cui verranno create le sottoscrizioni gestite.

Allo stesso modo, se un attributo è impostato su ASPARENT, il funzionamento dell'argomento dipenderà dai nodi più elevati nella struttura ad albero degli argomenti (consultare Oggetti argomento di gestione) su ogni singolo gestore code nel cluster. Ciò potrebbe determinare un comportamento diverso durante la pubblicazione o la sottoscrizione da gestori code differenti.

Gli attributi principali direttamente correlati al comportamento di pubblicazione / sottoscrizione nel cluster sono i seguenti:

CLROUTE
Questo parametro controlla l'instradamento dei messaggi tra i gestori code in cui sono connessi i publisher e i gestori code in cui esistono sottoscrizioni corrispondenti.

- L'instradamento viene configurato in modo che sia diretto tra questi gestori code o tramite un gestore code su cui è presente una definizione dell'argomento cluster. Consultare Cluster di pubblicazione / sottoscrizione per ulteriori dettagli.
- Non è possibile modificare **CLROUTE** mentre è impostato il parametro **CLUSTER** . Per modificare **CLROUTE**, impostare prima la proprietà **CLUSTER** su un valore vuoto. Ciò impedisce alle applicazioni che utilizzano l'argomento di comportarsi in modo cluster. Ciò a sua volta determina un'interruzione delle pubblicazioni consegnate alle sottoscrizioni, pertanto è necessario disattivare anche la messaggistica di pubblicazione / sottoscrizione durante l'esecuzione della modifica.

PROXYSUB
Questo parametro controlla quando vengono effettuate le sottoscrizioni proxy.

- FIRSTUSE è il valore predefinito e fa sì che le sottoscrizioni proxy vengano inviate in risposta alle sottoscrizioni locali su un gestore code in una topologia di pubblicazione / sottoscrizione distribuita e annullate quando non più richieste. Per i dettagli sul motivo per cui si potrebbe voler modificare questo attributo dal valore predefinito di FIRSTUSE, consultare Inoltro sottoscrizione proxy individuale e *pubblicazione ovunque* .
- Per abilitare la *pubblicazione ovunque*, impostare il parametro **PROXYSUB** su FORCE per un oggetto argomento di alto livello. Ne risulta una singola sottoscrizione proxy con caratteri jolly che corrisponde a tutti gli argomenti al di sotto di questo oggetto argomento nella struttura ad albero degli argomenti.

Nota: L'impostazione dell'attributo **PROXYSUB(FORCE)** in un cluster di pubblicazione / sottoscrizione di grandi dimensioni o occupato può causare un carico eccessivo sulle risorse di sistema. L'attributo **PROXYSUB(FORCE)** viene propagato a ogni gestore code, non solo al gestore code su cui è stato definito l'argomento. Ciò fa sì che ogni gestore code nel cluster crei una sottoscrizione proxy con caratteri jolly.

Una copia di un messaggio per questo argomento, pubblicato su qualsiasi gestore code del cluster, viene inviata a ogni gestore code del cluster, direttamente o tramite un gestore code dell'host argomento, a seconda dell'impostazione **CLROUTE** .

Quando l'argomento viene instradato direttamente, ogni gestore code crea canali mittente del cluster a ogni altro gestore code. Quando l'argomento è un host argomento instradato, i canali per ciascun gestore code dell'host argomento vengono creati da ogni gestore code del cluster.

Per ulteriori informazioni sul parametro **PROXYSUB** quando utilizzato nei cluster, vedi Direct routed publish / subscribe performance.

PUBSCOBE e SUBSCOPE
Questi parametri determinano se questo gestore code propaga le pubblicazioni ai gestori code nella topologia (cluster di pubblicazione / sottoscrizione o gerarchia) o limita l'ambito al solo gestore code locale. È possibile eseguire il lavoro equivalente in modo programmatico utilizzando MQPMO_SCOPE_QMGR e MQSO_SCOPE_QMGR.

PUBSCOPE
Se un oggetto argomento del cluster è definito con **PUBSCOPE(QMGR)**, la definizione viene condivisa con il cluster, ma l'ambito delle pubblicazioni basate su tale argomento è solo locale e non vengono inviate ad altri gestori code nel cluster.

SUBSCOPE
Se un oggetto argomento del cluster è definito con **SUBSCOPE(QMGR)**, la definizione viene condivisa con il cluster, ma l'ambito delle sottoscrizioni che si basano su tale argomento è solo locale, quindi nessuna sottoscrizione proxy viene inviata ad altri gestori code nel cluster.

Questi due attributi vengono comunemente utilizzati insieme per isolare un gestore code dall'interazione con altri membri del cluster su argomenti particolari. Il gestore code non pubblica o riceve pubblicazioni su tali argomenti da e verso altri membri del cluster. Questa situazione non impedisce la pubblicazione o la sottoscrizione se gli oggetti argomento sono definiti su argomenti secondari.

L'impostazione di **SUBSCOPE** su QMGR su una definizione locale di un argomento non impedisce ad altri gestori code nel cluster di propagare le relative sottoscrizioni proxy al gestore code se utilizzano una versione cluster dell'argomento, con **SUBSCOPE(ALL)**. Tuttavia, se la definizione locale imposta anche **PUBSCOPE** su QMGR , le sottoscrizioni proxy non vengono inviate alle pubblicazioni da questo gestore code.

Concetti correlati

Ambito della pubblicazione

Ambito della sottoscrizione

Più definizioni di argomenti cluster con lo stesso nome

È possibile definire lo stesso oggetto argomento cluster denominato su più di un gestore code nel cluster e in determinati scenari ciò abilita un comportamento specifico. Quando esistono più definizioni di argomenti cluster con lo stesso nome, la maggior parte delle proprietà deve corrispondere. In caso contrario, vengono riportati errori o avvertenze in base alla significatività della mancata corrispondenza.

In generale, se si verifica una mancata corrispondenza nelle proprietà di più definizioni di argomenti cluster, vengono emesse delle avvertenze e una delle definizioni di oggetti argomento viene utilizzata da ciascun gestore code nel cluster. La definizione utilizzata da ciascun gestore code non è deterministica o congruente tra i gestori code nel cluster. Tali disallineamenti dovrebbero essere risolti il più rapidamente possibile.

Durante l'impostazione o la manutenzione del cluster, a volte è necessario creare più definizioni di argomenti del cluster che non sono identiche. Tuttavia, ciò è sempre utile solo come misura temporanea, e viene quindi trattato come una potenziale condizione di errore.

Quando vengono rilevate delle mancate corrispondenze, i seguenti messaggi di avviso vengono scritti nel log degli errori di ciascun gestore code:

- Multi Su Multipiattaforma, AMQ9465 e AMQ9466.
- z/OS Su z/OS, CSQX465I e CSQX466I.

Le proprietà scelte per qualsiasi stringa di argomenti su ciascun gestore code possono essere determinate visualizzando lo stato dell'argomento piuttosto che le definizioni degli oggetti argomento, ad esempio utilizzando **DISPLAY TPSTATUS**.

In alcune situazioni, un conflitto nelle proprietà di configurazione è abbastanza grave da interrompere la creazione dell'oggetto argomento o da far sì che gli oggetti non corrispondenti vengano contrassegnati come non validi e non propagati nel cluster (consultare **CLSTATE** in DISPLAY TOPIC). Queste situazioni si verificano quando si verifica un conflitto nella proprietà di instradamento cluster (**CLROUTE**) delle definizioni argomento. Inoltre, a causa dell'importanza della coerenza tra le definizioni instradate dell'host argomento, ulteriori incongruenze vengono respinte come descritto in dettaglio nelle sezioni successive di questo articolo.

Se il conflitto viene rilevato al momento della definizione dell'oggetto, la modifica della configurazione viene rifiutata. Se successivamente vengono rilevati dai gestori code del repository completo, i seguenti messaggi di avvertenza vengono scritti nei log degli errori dei gestori code:

- Multi Su Multipiattaforma: AMQ9879
- z/OS Su z/OS CSQX879E.

Quando più definizioni dello stesso oggetto argomento sono definite nel cluster, una definizione definita localmente ha la precedenza su qualsiasi definizione definita in remoto. Pertanto, se esistono differenze nelle definizioni, i gestori code che ospitano le definizioni multiple si comportano in modo diverso.

L'effetto della definizione di un argomento non cluster con lo stesso nome di un argomento cluster da un altro gestore code

È possibile definire un oggetto argomento gestito che non è in cluster su un gestore code che si trova in un cluster e definire simultaneamente lo stesso oggetto argomento denominato come definizione di argomento in cluster su un gestore code differente. In tal modo, l'oggetto argomento definito localmente ha la precedenza su tutte le definizioni remote dello stesso nome.

Ciò ha l'effetto di impedire il funzionamento del cluster dell'argomento quando viene utilizzato da questo gestore code. In altre parole, le sottoscrizioni potrebbero non ricevere pubblicazioni dai publisher remoti e i messaggi dai publisher potrebbero non essere propagati alle sottoscrizioni remote nel cluster.

Prima di configurare un sistema di questo tipo, è necessario prestare particolare attenzione, poiché ciò può creare confusione.

Nota: Se un singolo gestore code deve impedire che le pubblicazioni e le sottoscrizioni si propaghino intorno al cluster, anche quando l'argomento è stato raggruppato altrove, un approccio alternativo consiste nell'impostare gli ambiti di pubblicazione e sottoscrizione solo sul gestore code locale. Consultare “Attributi argomento cluster” a pagina 98.

Più definizioni dell'argomento cluster in un cluster con instradamento diretto

Per l'instradamento diretto, di solito non si definisce lo stesso argomento cluster su più di un gestore code cluster. Questo perché l'instradamento diretto rende l'argomento disponibile in tutti i gestori code nel cluster, indipendentemente dal gestore code su cui è stato definito. Inoltre, l'aggiunta di più definizioni di argomenti cluster aumenta in modo significativo l'attività del sistema e la complessità amministrativa, e con l'aumento della complessità si ha una maggiore probabilità di errore umano:

- Ciascuna definizione risulta in un oggetto argomento cluster aggiuntivo che viene inviato agli altri gestori code nel cluster, inclusi gli altri gestori code dell'host argomento cluster.
- Tutte le definizioni per un determinato argomento in un cluster devono essere identiche, altrimenti è difficile stabilire quale definizione argomento viene utilizzata da un gestore code.

Non è inoltre essenziale che il solo gestore code host sia continuamente disponibile per il corretto funzionamento dell'argomento nel cluster, poiché la definizione dell'argomento del cluster viene memorizzata nella cache dai gestori code del repository completo e da tutti gli altri gestori code nei repository del cluster parziali. Per ulteriori informazioni, consultare Disponibilità dei gestori code dell'host argomento che utilizzano l'instradamento diretto.

Per una situazione in cui potrebbe essere necessario definire temporaneamente un argomento del cluster su un secondo gestore code, ad esempio quando l'host esistente dell'argomento deve essere rimosso dal cluster, fare riferimento a Spostamento di una definizione dell'argomento del cluster in un gestore code differente.

Se occorre modificare una definizione dell'argomento cluster, effettuare la modifica nello stesso gestore code in cui era stata definita. Il tentativo di modificarla da un altro gestore code potrebbe accidentalmente creare una seconda definizione dell'argomento con attributi dell'argomento in conflitto.

Più definizioni dell'argomento cluster in un cluster instradato all'host argomento

Quando un argomento cluster viene definito con un instradamento cluster di *host argomento*, l'argomento viene propagato su tutti i gestori code nel cluster proprio come per gli argomenti instradati *diretti* . Inoltre, tutta la messaggistica di pubblicazione / sottoscrizione per tale argomento viene instradata attraverso i gestori code in cui è definito tale argomento. Pertanto, l'ubicazione e il numero di definizioni dell'argomento nel cluster diventano importanti (consultare “Instradamento host argomento nei cluster di pubblicazione / sottoscrizione” a pagina 83).

Per garantire una disponibilità e una scalabilità adeguate, è utile, se possibile, disporre di più definizioni di argomenti. Consultare Disponibilità dei gestori code dell'host argomento che utilizzano l'instradamento dell'host argomento.

Quando si aggiungono o si rimuovono ulteriori definizioni di un argomento instradato *host argomento* in un cluster, è necessario considerare il flusso di messaggi al momento della modifica della configurazione. Se i messaggi vengono pubblicati nel cluster nell'argomento al momento della modifica, è richiesto un processo a fasi per aggiungere o rimuovere una definizione di argomento. Fare riferimento a Spostamento di una definizione di argomento del cluster in un gestore code differente e a Aggiunta di ulteriori host argomento a un cluster instradato dell'host argomento.

Come precedentemente spiegato, le proprietà delle definizioni multiple devono corrispondere, con la possibile eccezione del parametro **PUB** , come descritto nella sezione successiva. Quando le pubblicazioni vengono instradate tramite i gestori code dell'host argomento, è ancora più importante che più definizioni siano congruenti. Pertanto, un'incongruenza rilevata nella stringa di argomenti o nel nome cluster viene rifiutata se una o più definizioni di argomenti sono state configurate per l'instradamento del cluster di host di argomenti.

Nota: Le definizioni di argomenti del cluster vengono rifiutate anche se viene effettuato un tentativo di configurarle sopra o sotto un altro argomento nella struttura ad albero degli argomenti, dove la definizione di argomenti del cluster esistente è configurata per l'instradamento dell'host dell'argomento. Ciò evita ambiguità nell'instradamento delle pubblicazioni rispetto alle sottoscrizioni con caratteri jolly.

Gestione speciale per il parametro PUB

Il parametro di **PUB** viene utilizzato per controllare quando le applicazioni possono pubblicare un argomento. Nel caso dell'instradamento dell'host argomento in un cluster, può anche controllare quali gestori code dell'host argomento vengono utilizzati per instradare pubblicazioni. Per questo motivo è consentito avere più definizioni dello stesso oggetto argomento nel cluster, con impostazioni diverse per il parametro PUB .

Se più definizioni cluster remote di un argomento hanno impostazioni differenti per questo parametro, l'argomento consente l'invio e la consegna delle pubblicazioni alle sottoscrizioni se vengono soddisfatte le condizioni riportate di seguito:

- Non c'è un oggetto argomento corrispondente definito sul gestore code a cui è connesso il publisher impostato su `PUB(DISABLED)`.
- Una o più definizioni di argomenti multipli nel cluster sono impostate su `PUB(ENABLED)`, oppure una o più definizioni di argomenti multipli sono impostate su `PUB(ASPARENT)` e i gestori code locali in cui il publisher è connesso e la sottoscrizione definita sono impostati su `PUB(ENABLED)` in un punto più alto nella struttura ad albero degli argomenti.

Per l'instradamento dell'host argomento, quando i messaggi vengono pubblicati dalle applicazioni connesse ai gestori code che non sono host argomento, i messaggi vengono instradati solo ai gestori code che ospitano l'argomento in cui il parametro **PUB** non è stato esplicitamente impostato su `DISABLED`. È quindi possibile utilizzare l'impostazione `PUB(DISABLED)` per disattivare il traffico di messaggi attraverso determinati host argomento. È possibile eseguire questa operazione per preparare la manutenzione o la rimozione di un gestore code o per i motivi descritti in Aggiunta di ulteriori host argomento a un cluster instradato di host argomento.

Disponibilità dei gestori code dell'host argomento del cluster
Progettare il cluster di pubblicazione / sottoscrizione per ridurre al minimo il rischio che, se un gestore code dell'host argomento diventa non disponibile, il cluster non sarà più in grado di elaborare il traffico per l'argomento. L'effetto di un gestore code dell'host argomento che diventa non disponibile dipende dal fatto che il cluster stia utilizzando l'instradamento dell'host argomento o l'instradamento diretto.

Disponibilità dei gestori code dell'host argomento che utilizzano l'instradamento diretto

Per l'instradamento diretto, di solito non si definisce lo stesso argomento cluster su più di un gestore code cluster. Questo perché l'instradamento diretto rende l'argomento disponibile in tutti i gestori code nel cluster, indipendentemente dal gestore code su cui è stato definito.Consultare Definizioni di più argomenti cluster in un cluster instradato direttamente.

In un cluster, ogni volta che l'host di un oggetto in cluster (ad esempio una coda in cluster o un argomento in cluster) diventa non disponibile per un periodo di tempo prolungato, gli altri membri del cluster alla fine annulleranno la conoscenza di tali oggetti. Nel caso di un argomento con cluster, se il gestore code dell'host dell'argomento del cluster diventa non disponibile, gli altri gestori code continuano a elaborare le richieste di pubblicazione / sottoscrizione per l'argomento in un cluster diretto (ovvero, inviando pubblicazioni a sottoscrizioni su gestori code remoti) per almeno 60 giorni dall'ultima volta che il gestore code che ospita l'argomento è stato in comunicazione con i gestori code del repository completo. Se il gestore code su cui è stato definito l'oggetto argomento cluster non viene mai più reso disponibile, alla fine gli oggetti argomento memorizzati nella cache sugli altri gestori code vengono eliminati e l'argomento ritorna a un argomento locale, nel qual caso le sottoscrizioni cessano di ricevere le pubblicazioni dalle applicazioni connesse ai gestori code remoti.

Con un periodo di 60 giorni per ripristinare il gestore code su cui si definisce un oggetto argomento del cluster, non è necessario adottare misure speciali per garantire che l'host argomento del cluster rimanga disponibile (notare, tuttavia, che le sottoscrizioni definite sull'host argomento del cluster non disponibile non rimangono disponibili). Il periodo di 60 giorni è sufficiente per far fronte a problemi tecnici ed è probabile che venga superato solo a causa di errori amministrativi. Per attenuare questa possibilità, se l'host dell'argomento del cluster non è disponibile, tutti i membri del cluster scrivono ogni ora i messaggi di log degli errori, indicando che il relativo oggetto dell'argomento del cluster memorizzato nella cache non è stato aggiornato. Rispondere a questi messaggi verificando che il gestore code su cui è definito l'oggetto argomento cluster sia in esecuzione. Se non è possibile rendere nuovamente disponibile il gestore code dell'host argomento del cluster, definire la stessa definizione di argomento del cluster, con esattamente gli stessi attributi, su un altro gestore code del cluster.

Disponibilità dei gestori code dell'host argomento che utilizzano l'instradamento dell'host argomento

Per l'instradamento dell'host dell'argomento, tutta la messaggistica di pubblicazione / sottoscrizione per un argomento viene instradata attraverso i gestori code in cui è definito tale argomento. Per questo motivo, è molto importante considerare la disponibilità continua di questi gestori code nel cluster.
Se un host dell'argomento diventa non disponibile e non esiste alcun altro host per l'argomento, il traffico dai publisher ai sottoscrittori su gestori code differenti nel cluster si arresta immediatamente per l'argomento. Se sono disponibili ulteriori host argomento, i gestori code del cluster instradano il nuovo traffico di pubblicazione attraverso questi host argomento, fornendo la disponibilità continua delle rotte dei messaggi.

Per quanto riguarda gli argomenti diretti, dopo 60 giorni, se il primo host argomento non è ancora disponibile, la conoscenza dell'argomento di tale host argomento viene rimossa dal cluster. Se questa è l'ultima definizione rimanente per questo argomento nel cluster, tutti gli altri gestori code cessano di inoltrare le pubblicazioni a qualsiasi host argomento per l'instradamento.

Per garantire una disponibilità e una scalabilità adeguate, è quindi utile, se possibile, definire ogni argomento su almeno due gestori code cluster. Ciò fornisce una protezione contro qualsiasi gestore code dell'host argomento specificato che diventa non disponibile. Consultare anche Più definizioni di argomenti del cluster in un cluster instradato dell'host argomento.

Se non è possibile configurare più host di argomenti (ad esempio, perché è necessario conservare l'ordine dei messaggi) e non è possibile configurare solo un host di argomenti (poiché la disponibilità di un singolo gestore code non deve influenzare il flusso di pubblicazioni per le sottoscrizioni in tutti i gestori code nel cluster), considerare la configurazione dell'argomento come un argomento instradato direttamente. In questo modo si evita di fare affidamento su un singolo gestore code per l'intero cluster, ma è comunque necessario che ogni singolo gestore code sia disponibile per elaborare le sottoscrizioni e i publisher ospitati localmente.

Blocco della pubblicazione / sottoscrizione in cluster

L'introduzione del primo argomento del cluster instradato direttamente in un cluster forza ogni gestore code nel cluster a rendersi conto di ogni altro gestore code e potenzialmente fa sì che creino canali l'uno per l'altro. Se ciò non è opportuno, è necessario configurare la pubblicazione / sottoscrizione instradata dell'host argomento. Se l'esistenza di un argomento cluster instradato direttamente potrebbe

compromettere la stabilità del cluster, a causa dei problemi di ridimensionamento di ciascun gestore code, è possibile disabilitare completamente la funzionalità di pubblicazione / sottoscrizione del cluster impostando **PSCLUS** su DISABLED su ogni gestore code del cluster.

Come descritto in"Instradamento diretto nei cluster di pubblicazione / sottoscrizione" a pagina 78, quando si introduce un argomento con cluster instradato direttamente in un cluster, tutti i repository parziali vengono automaticamente informati di tutti gli altri membri del cluster. L'argomento con cluster può anche creare sottoscrizioni su tutti gli altri nodi (ad esempio, dove **PROXYSUB(FORCE)** è specificato) e causare l'avvio di un numero elevato di canali da un gestore code, anche quando non sono presenti sottoscrizioni locali. Ciò inserisce un carico aggiuntivo immediato su ciascun gestore code nel cluster. Per un cluster che contiene molti gestori code, ciò può causare una riduzione significativa delle prestazioni. Pertanto, l'introduzione della pubblicazione / sottoscrizione diretta instradata a un cluster deve essere pianificata attentamente.

Quando si sa che un cluster non può contenere i costi generali della pubblicazione / sottoscrizione instradata diretta, è possibile utilizzare invece la pubblicazione / sottoscrizione instradata dell'host argomento. Per una panoramica delle differenze, consultare "Progettazione di cluster di pubblicazione / sottoscrizione" a pagina 76.

Se si preferisce disabilitare completamente la funzionalità di pubblicazione / sottoscrizione per il cluster, è possibile farlo impostando l'attributo del gestore code **PSCLUS** su DISABLED su ogni gestore code nel cluster. Questa impostazione disabilita la pubblicazione / sottoscrizione instradata diretta e l'host argomento instradato nel cluster, modificando tre aspetti della funzionalità del gestore code:

- Un amministratore di questo gestore code non è più in grado di definire un oggetto Topic come cluster.
- Le definizioni di argomenti in entrata o le sottoscrizioni proxy da altri gestori code vengono rifiutate e viene registrato un messaggio di avvertenza per informare l'amministratore della configurazione non corretta.
- I repository completi non condividono più automaticamente le informazioni su ogni gestore code con tutti gli altri repository parziali quando ricevono una definizione di argomento.

Anche se **PSCLUS** è un parametro di ogni singolo gestore code in un cluster, non è destinato a disabilitare in modo selettivo la pubblicazione / sottoscrizione in un sottoinsieme di gestori code nel cluster. Se si disabilita in modo selettivo in questo modo, verranno visualizzati messaggi di errore frequenti. Ciò è dovuto al fatto che le sottoscrizioni proxy e le definizioni degli argomenti vengono costantemente visualizzate e rifiutate se un argomento è raggruppato in un gestore code in cui **PSCLUS** è abilitato.

Si consiglia pertanto di impostare **PSCLUS** su DISABLED su ogni gestore code nel cluster. Tuttavia, in pratica questo stato può essere difficile da raggiungere e gestire, ad esempio i gestori code possono unirsi e lasciare il cluster in qualsiasi momento. È necessario almeno assicurarsi che **PSCLUS** sia impostato su DISABLED su tutti i gestori code del repository completo. Se si esegue questa operazione, e un argomento in cluster viene successivamente definito su un gestore code ABILITATO nel cluster, ciò non fa in modo che i repository completi informino ogni gestore code di ogni altro gestore code, pertanto il cluster è protetto da potenziali problemi di scalabilità in tutti i gestori code. In questo scenario, l'origine dell'argomento del cluster viene riportata nei log degli errori dei gestori code del repository completo.

Se un gestore code partecipa a uno o più cluster di pubblicazione / sottoscrizione e anche a uno o più cluster point - to - point, è necessario impostare **PSCLUS** su ABILITATO su tale gestore code. Per questo motivo, quando si sovrappone un cluster point-to-point con un cluster di pubblicazione - sottoscrizione, è necessario utilizzare una serie separata di repository completi in ogni cluster. Questo approccio consente alle definizioni degli argomenti e alle informazioni su ogni gestore code di fluire solo nel cluster di pubblicazione / sottoscrizione.

Per evitare configurazioni incongruenti quando si passa da **PSCLUS** da ENABLED a DISABLED, non possono esistere oggetti argomento in cluster in alcun cluster di cui questo gestore code è membro. Tali argomenti, anche quelli definiti in remoto, devono essere eliminati prima di modificare **PSCLUS** in DISABLED.

Per ulteriori informazioni su **PSCLUS**, consultare ALTER QMGR (PSCLUS).

Concetti correlati

Prestazioni cluster di pubblicazione / sottoscrizione instradate dirette

Pubblica / sottoscrivi e più cluster

Un singolo gestore code può essere membro di più di un cluster. Questa disposizione è talvolta nota come *cluster di sovrapposizione*. Tramite tale sovrapposizione, le code cluster possono essere rese accessibili da più cluster e il traffico di messaggi point-to-point può essere instradato dai gestori code di un cluster ai gestori code di un altro cluster. Gli argomenti raggruppati nei cluster di pubblicazione / sottoscrizione non forniscono la stessa funzionalità. Pertanto, il loro comportamento deve essere chiaramente compreso quando si utilizzano più cluster.

A differenza di una coda, non è possibile associare una definizione di argomento a più di un cluster. L'ambito di un argomento con cluster è limitato ai gestori code nello stesso cluster per cui è definito l'argomento. Ciò consente la propagazione delle pubblicazioni alle sottoscrizioni solo sui gestori code nello stesso cluster.

Una struttura ad albero degli argomenti del gestore code

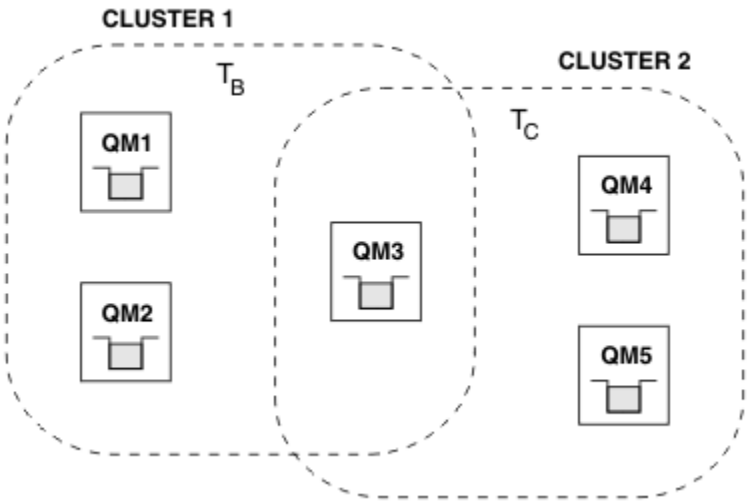


Figura 28. Sovrapposizione di cluster: due cluster ciascuno che effettua la sottoscrizione a argomenti differenti

Quando un gestore code è membro di più cluster, viene informato di tutti gli argomenti del cluster definiti in ognuno di questi cluster. Ad esempio, nella figura precedente, QM3 è consapevole sia degli oggetti argomento del cluster gestiti T_B che T_C, mentre QM1 è consapevole solo di T_B. QM3 applica entrambe le definizioni di argomento al relativo argomento locale e, pertanto, ha un comportamento diverso rispetto a QM1 per alcuni argomenti. Per questo motivo è importante che gli argomenti raggruppati da cluster differenti non interferiscano tra loro. L'interferenza può verificarsi quando un argomento cluster viene definito sopra o sotto un altro argomento cluster in un cluster differente (ad esempio, hanno stringhe di argomenti di `/Sport` e `/Sport/Football`) o anche per la stessa stringa di argomenti in entrambi. Un'altra forma di interferenza è quando gli oggetti argomento con cluster gestiti sono definiti con lo stesso nome oggetto in cluster differenti, ma per stringhe argomento differenti.

Se viene effettuata tale configurazione, la consegna delle pubblicazioni alle sottoscrizioni corrispondenti diventa molto dipendente dalle ubicazioni relative dei publisher e dei sottoscrittori rispetto al cluster. Per questo motivo, non è possibile fare affidamento su una configurazione di questo tipo ed è necessario modificarla per rimuovere gli argomenti che interferiscono.

Quando si pianifica una topologia cluster sovrapposta con la messaggistica di pubblicazione / sottoscrizione, è possibile evitare qualsiasi interferenza trattando la struttura ad albero degli argomenti e i nomi degli oggetti argomento raggruppati come se si estendessero a tutti i cluster sovrapposti nella topologia.

Integrazione di più cluster di pubblicazione / sottoscrizione

Se esiste un requisito per la messaggistica di pubblicazione / sottoscrizione per estendere i gestori code in cluster differenti, sono disponibili due opzioni:

- Collegare i cluster tramite l'utilizzo di una configurazione della gerarchia di pubblicazione / sottoscrizione. Consultare Combinazione di spazi argomento di più cluster.
- Creare un cluster aggiuntivo che si sovrapponga ai cluster esistenti e includa tutti i gestori code che devono pubblicare o sottoscrivere un particolare argomento.

Con quest' ultima opzione, è necessario considerare attentamente la dimensione del cluster e il meccanismo di instradamento del cluster più efficace. Consultare“Progettazione di cluster di pubblicazione / sottoscrizione” a pagina 76.

Considerazioni di progettazione per le pubblicazioni conservate nei cluster di pubblicazione / sottoscrizione

Ci sono alcune limitazioni da considerare quando si progetta un cluster di pubblicazione / sottoscrizione per lavorare con le pubblicazioni conservate.

Considerazioni

Considerazione 1 I gestori code del seguente cluster memorizzano sempre l'ultima versione di una pubblicazione conservata:

- Il gestore code del publisher
- In un cluster instradato di host argomento, l'host argomento (fornito con un solo host argomento per l'argomento, come spiegato nella prossima sezione di questo articolo)
- Tutti i gestori code con sottoscrizioni corrispondenti alla stringa di argomenti della pubblicazione conservata

Considerazione 2: i gestori code non ricevono le pubblicazioni conservate aggiornate quando non dispongono di sottoscrizioni. Di conseguenza, qualsiasi pubblicazione conservata memorizzata su un gestore code che non fa più sottoscrizione all'argomento diventerà obsoleta.

Considerazione 3: quando si crea una sottoscrizione, se è presente una copia locale di una pubblicazione conservata per la stringa di argomenti, la copia locale viene consegnata alla sottoscrizione. Se si è il primo sottoscrittore per una determinata stringa di argomenti, anche una pubblicazione conservata corrispondente viene consegnata da uno dei seguenti membri del cluster:

- In un cluster instradato direttamente, il gestore code del publisher
- In un cluster di host argomento instradati, gli host argomento per l'argomento fornito

La consegna di una pubblicazione conservata da un host argomento o da un gestore code di pubblicazione al gestore code di sottoscrizione è asincrona alle chiamate MQSUB . Pertanto, se si utilizza la chiamata MQSUBRQ , la pubblicazione conservata più recente potrebbe essere persa fino a una successiva chiamata a MQSUBRQ.

Implicazioni

Per qualsiasi cluster di pubblicazione / sottoscrizione, quando viene effettuata una prima sottoscrizione, il gestore code locale potrebbe archiviare una copia obsoleta di una pubblicazione conservata e questa è la copia consegnata alla nuova sottoscrizione. L'esistenza di una sottoscrizione sul gestore code locale significa che questa verrà risolta al successivo aggiornamento della pubblicazione conservata.

Per un cluster di pubblicazione / sottoscrizione instradato dell'host argomento, se si configura più di un host argomento per un determinato argomento, i nuovi sottoscrittori potrebbero ricevere la pubblicazione conservata più recente da un host argomento oppure potrebbero ricevere una pubblicazione conservata obsoleta da un altro host argomento (con l'ultima perdita). Per l'instradamento dell'host argomento, è consuetudine configurare più host argomento per un determinato argomento. Tuttavia, se si prevede che

le applicazioni utilizzino le pubblicazioni conservate, è necessario configurare solo un host argomento per ciascun argomento.

Per qualsiasi stringa di argomenti fornita, è necessario utilizzare solo un singolo publisher e assicurarsi che il publisher utilizzi sempre lo stesso gestore code. Se non si esegue questa operazione, diverse pubblicazioni conservate potrebbero essere attive su gestori code differenti per lo stesso argomento, causando un comportamento imprevisto. Poiché vengono distribuite più sottoscrizioni proxy, è possibile che vengano ricevute più pubblicazioni conservate.

Se si è ancora preoccupati per i sottoscrittori che utilizzano pubblicazioni obsolete, considerare l'impostazione di una scadenza del messaggio quando si crea ogni pubblicazione conservata.

È possibile utilizzare il comando **CLEAR TOPICSTR** per rimuovere una pubblicazione conservata da un cluster di pubblicazione / sottoscrizione. In determinate circostanze, potrebbe essere necessario immettere il comando su più membri del cluster di pubblicazione / sottoscrizione, come descritto in **CLEAR TOPICSTR**.

Sottoscrizioni jolly e pubblicazioni conservate

Se si utilizzano sottoscrizioni con caratteri jolly, le sottoscrizioni proxy corrispondenti consegnate ad altri membri del cluster di pubblicazione / sottoscrizione vengono fornite con caratteri jolly dal separatore di argomenti immediatamente prima del primo carattere jolly. Consultare Caratteri jolly e argomenti cluster.

Pertanto, il carattere jolly utilizzato potrebbe corrispondere a un numero maggiore di stringhe di argomenti e di pubblicazioni conservate, rispetto all'applicazione di sottoscrizione.

Ciò aumenta la capacità di memoria necessaria per le pubblicazioni conservate ed è pertanto necessario assicurarsi che i gestori code host dispongano di capacità di memoria sufficiente.

Concetti correlati

Pubblicazioni conservate

Inoltro e pubblicazione di singole sottoscrizioni proxy ovunque

REFRESH CLUSTER considerazioni per i cluster di pubblicazione / sottoscrizione

Immettendo il comando **REFRESH CLUSTER** il gestore code elimina temporaneamente le informazioni conservate localmente su un cluster, inclusi gli argomenti del cluster e le relative sottoscrizioni proxy associate.

Il tempo impiegato dall'immissione del comando **REFRESH CLUSTER** al punto che il gestore code riacquista una conoscenza completa delle informazioni necessarie per la pubblicazione / sottoscrizione in cluster dipende dalla dimensione del cluster, dalla disponibilità e dalla reattività dei gestori code del repository completo.

Durante il processo di aggiornamento, si verifica un'interruzione del traffico di pubblicazione / sottoscrizione in un cluster di pubblicazione / sottoscrizione. Per i cluster di grandi dimensioni, l'utilizzo del comando **REFRESH CLUSTER** può interrompere il cluster mentre è in corso e di nuovo a intervalli di 27 giorni quando gli oggetti cluster inviano automaticamente gli aggiornamenti di stato a tutti i gestori code interessati. Consultare Refreshing in a large cluster can affect performance and availability of the cluster. Per questi motivi, il comando **REFRESH CLUSTER** deve essere utilizzato in un cluster di pubblicazione / sottoscrizione solo se sotto la guida del centro di assistenza IBM .

L'interruzione del cluster può apparire esternamente come i sintomi seguenti:

- Le sottoscrizioni agli argomenti del cluster su questo gestore code non ricevono pubblicazioni dai publisher connessi ad altri gestori code nel cluster.
- I messaggi pubblicati negli argomenti del cluster su questo gestore code non vengono propagati alle sottoscrizioni su altri gestori code.
- Le sottoscrizioni agli argomenti del cluster su questo gestore code create durante questo periodo non inviano in modo congruente sottoscrizioni proxy ad altri membri del cluster.
- Le sottoscrizioni agli argomenti del cluster su questo gestore code eliminati durante questo periodo non rimuovono in modo congruente le sottoscrizioni proxy da altri membri del cluster.

- Pause di 10 secondi, o più lunghe, nella consegna dei messaggi.
- Errori di **MQPUT** , ad esempio MQRC_PUBLICATION_FAILURE.
- Pubblicazioni collocate nella coda di messaggi non instradabili con motivo MQRC_UNKNOWN_REMOTE_Q_MGR

Per questi motivi le applicazioni di pubblicazione / sottoscrizione devono essere disattivate prima di immettere il comando **REFRESH CLUSTER** .

Dopo che un comando **REFRESH CLUSTER** è stato immesso su un gestore code in un cluster di pubblicazione / sottoscrizione, attendere che tutti i gestori code del cluster e gli argomenti del cluster siano stati aggiornati correttamente, quindi risincronizzare le sottoscrizioni proxy come descritto in Risincronizzazione delle sottoscrizioni proxy. Quando tutte le sottoscrizioni proxy sono state correttamente risincronizzate, riavviare le applicazioni di pubblicazione / sottoscrizione.

Se un comando **REFRESH CLUSTER** sta impiegando molto tempo per essere completato, monitorarlo osservando CURDEPTH di SYSTEM.CLUSTER.COMMAND.QUEUE.

Concetti correlati

“Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER” a pagina 70
Utilizzare il comando **REFRESH CLUSTER** per eliminare tutte le informazioni contenute localmente su un cluster e ricreare tali informazioni dai repository completi nel cluster. Non è necessario utilizzare questo comando, tranne in circostanze eccezionali. Se hai bisogno di usarlo, ci sono considerazioni speciali su come usarlo. Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

Riferimenti correlati

Problemi dell'applicazione durante l'esecuzione di REFRESH CLUSTER

Riferimento comandi MQSC: REFRESH CLUSTER

Instradamento nelle gerarchie di pubblicazione / sottoscrizione

Se la topologia del gestore code distribuito è una gerarchia di pubblicazione / sottoscrizione e viene effettuata una sottoscrizione su un gestore code, per impostazione predefinita viene creata una sottoscrizione proxy su ogni gestore code nella gerarchia. Le pubblicazioni ricevute su qualsiasi gestore code vengono quindi instradate attraverso la gerarchia a ciascun gestore code su cui è presente una sottoscrizione corrispondente.

Per un'introduzione al modo in cui i messaggi vengono instradati tra i gestori code nelle gerarchie di pubblicazione / sottoscrizione e nei cluster, consultare Reti di pubblicazione / sottoscrizione distribuite.

Quando viene effettuata una sottoscrizione a un argomento su un gestore code in una gerarchia di pubblicazione / sottoscrizione distribuita, il gestore code gestisce il processo mediante il quale la sottoscrizione viene propagata ai gestori code connessi. Le *sottoscrizioni proxy* passano a tutti i gestori code nella rete. Una sottoscrizione proxy fornisce a un gestore code le informazioni necessarie per inoltrare una pubblicazione ai gestori code che ospitano le sottoscrizioni per tale argomento. Ogni gestore code in una gerarchia di pubblicazione / sottoscrizione è consapevole solo delle sue relazioni dirette. Le pubblicazioni immesse in un gestore code vengono inviate, tramite le relazioni dirette, a tali gestori code con sottoscrizioni. Questo è illustrato nella seguente figura, in cui *Sottoscrittore 1* registra una sottoscrizione per un particolare argomento sul gestore code *Asia* (1). Le sottoscrizioni proxy per questa sottoscrizione sul gestore code *Asia* vengono inoltrati a tutti gli altri gestori code nella rete (2,3, 4).

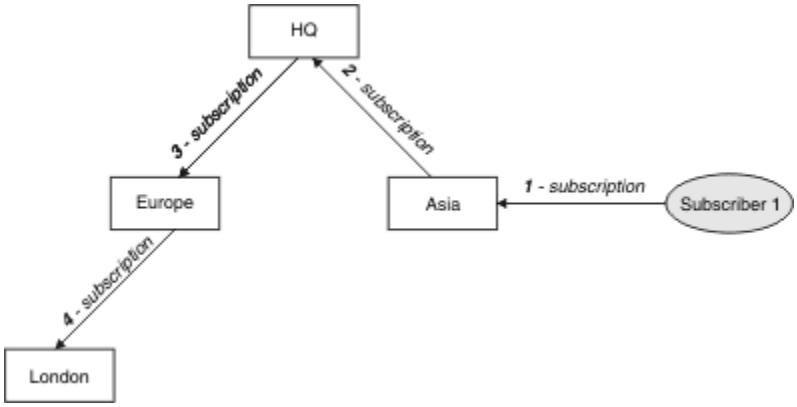


Figura 29. Propagazione delle sottoscrizioni attraverso una rete di gestori code

Un gestore code consolida tutte le sottoscrizioni create su di esso, sia da applicazioni locali che da gestori code remoti. Crea sottoscrizioni proxy per gli argomenti delle sottoscrizioni con i relativi vicini, a meno che non esista già una sottoscrizione proxy. Questo è illustrato nella seguente figura, in cui il *Sottoscrittore 2* registra una sottoscrizione, allo stesso argomento di Figura 29 a pagina 109, sul gestore code *HQ* (5). La sottoscrizione per questo argomento viene inoltrata al gestore code *Asia* , in modo che sia consapevole che le sottoscrizioni esistono altrove sulla rete (6). La sottoscrizione non viene inoltrata al gestore code *Europa* , perché è già stata registrata una sottoscrizione per questo argomento; consultare il passo 3 in Figura 29 a pagina 109.

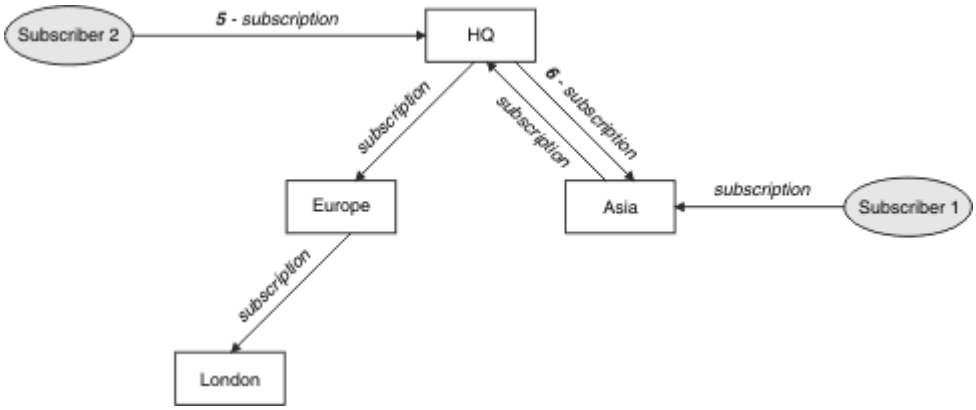


Figura 30. Sottoscrizioni multiple

Quando un'applicazione pubblica informazioni su un argomento, per impostazione predefinita il gestore code di ricezione le inoltra a tutti i gestori code che hanno sottoscrizioni valide per l'argomento. Potrebbe inoltrarlo tramite uno o più gestori code intermedi. Questo è illustrato nella seguente figura, in cui un publisher invia una pubblicazione, sullo stesso argomento di Figura 30 a pagina 109, al gestore code *Europa* (7). Una sottoscrizione per questo argomento esiste da *HQ* a *Europe*, quindi la pubblicazione viene inoltrata al gestore code *HQ* (8). Tuttavia, non esiste alcuna sottoscrizione da *Londra* a *Europa* (solo da *Europa* a *Londra*), quindi la pubblicazione non viene inoltrata al gestore code *Londra* . Il gestore code *HQ* invia la pubblicazione direttamente al *Sottoscrittore 2* e al gestore code *Asia* (9). La pubblicazione viene inoltrata al *Sottoscrittore 1* da *Asia* (10).

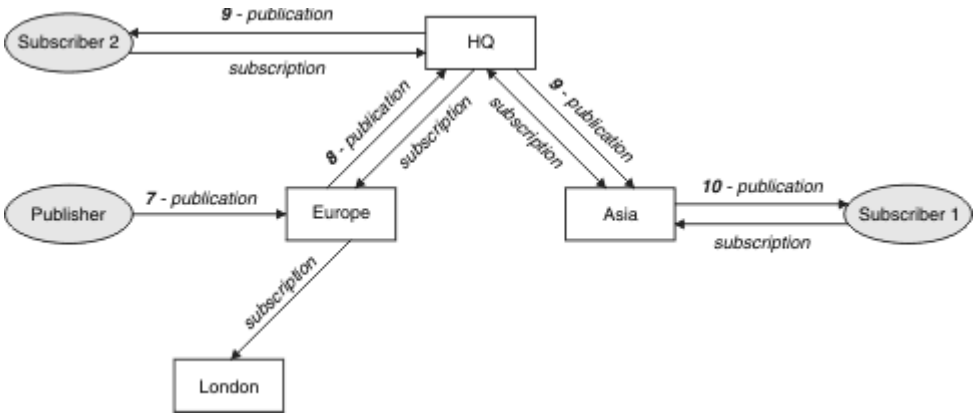


Figura 31. Propagazione delle pubblicazioni tramite una rete di gestori code

Quando un gestore code invia pubblicazioni o sottoscrizioni a un altro gestore code, imposta il proprio ID utente nel messaggio. Se si sta utilizzando una gerarchia di pubblicazione / sottoscrizione e se il canale in entrata è configurato per inserire i messaggi con l'autorizzazione dell'ID utente nel messaggio, è necessario autorizzare l'ID utente del gestore code di invio. Consultare Utilizzo degli ID utente predefiniti con una gerarchia di gestori code.

Nota: Se si utilizzano invece i cluster di pubblicazione / sottoscrizione, l'autorizzazione viene gestita dal cluster.

Sintesi e considerazioni aggiuntive

Una gerarchia di pubblicazione / sottoscrizione fornisce un controllo preciso sulla relazione tra i gestori code. Dopo che è stato creato, ha bisogno di un piccolo intervento manuale da amministrare. Tuttavia, impone anche alcuni vincoli al sistema:

- I nodi superiori nella gerarchia, in particolare il nodo root, devono essere ospitati su apparecchiature robuste, altamente disponibili e performanti. Ciò è dovuto al fatto che si prevede che un maggiore traffico di pubblicazione scorrerà attraverso questi nodi.
- La disponibilità di ogni gestore code non foglia nella gerarchia influenza la capacità della rete di trasmettere i messaggi dai publisher ai sottoscrittori su altri gestori code.
- Per impostazione predefinita, tutte le stringhe argomento sottoscritte vengono propagate in tutta la gerarchia e le pubblicazioni vengono propagate solo ai gestori code remoti che hanno una sottoscrizione all'argomento associato. Pertanto, le rapide modifiche all'insieme delle sottoscrizioni possono diventare un fattore limitante. È possibile modificare questo comportamento predefinito e fare in modo che tutte le pubblicazioni vengano propagate a tutti i gestori code, il che elimina la necessità di sottoscrizioni proxy. Vedere Prestazioni della sottoscrizione nelle reti di pubblicazione / sottoscrizione.

  Nota: Una restrizione simile si applica anche ai cluster instradati direttamente.
- A causa della natura interconnessa dei gestori code di pubblicazione / sottoscrizione, la propagazione delle sottoscrizioni proxy su tutti i nodi nella rete richiede tempo. Le pubblicazioni remote non iniziano necessariamente ad essere sottoscritte immediatamente, quindi le pubblicazioni iniziali potrebbero non essere inviate in seguito ad una sottoscrizione ad una nuova stringa di argomenti. È possibile rimuovere i problemi causati dal ritardo della sottoscrizione facendo in modo che tutte le pubblicazioni vengano propagate a tutti i gestori code, eliminando la necessità di sottoscrizioni proxy. Consultare Prestazioni della sottoscrizione nelle reti di pubblicazione / sottoscrizione.

  Nota: Questa limitazione si applica anche ai cluster instradati direttamente.
- Per una gerarchia di pubblicazione / sottoscrizione, l'aggiunta o la rimozione di gestori code richiede la configurazione manuale della gerarchia, con un'attenta considerazione dell'ubicazione di tali gestori code e della loro dipendenza da altri gestori code. A meno che non si stiano aggiungendo o rimuovendo

gestori code che si trovano nella parte inferiore della gerarchia e pertanto non vi siano ulteriori rami al di sotto di essi, sarà necessario configurare anche altri gestori code nella gerarchia.

Prima di utilizzare una gerarchia di pubblicazione / sottoscrizione come meccanismo di instradamento, esplorare gli approcci alternativi descritti in "Instradamento diretto nei cluster di pubblicazione / sottoscrizione" a pagina 78 e "Instradamento host argomento nei cluster di pubblicazione / sottoscrizione" a pagina 83.

Code di sistema di pubblicazione / sottoscrizione distribuite

Quattro code di sistema vengono utilizzate dai gestori code per la messaggistica di pubblicazione / sottoscrizione. È necessario essere consapevoli della loro esistenza solo per scopi di determinazione dei problemi e di pianificazione della capacità.

Consultare Bilanciamento di produttori e consumatori nelle reti di pubblicazione / sottoscrizione per istruzioni su come monitorare queste code.

Tabella 6. Code di sistema di pubblicazione / sottoscrizione su Multiplatforms

Coda di sistema	**Finalità**
SYSTEM.INTER.QMGR.CONTROL	Coda di controllo di pubblicazione / sottoscrizione distribuita IBM MQ
SYSTEM.INTER.QMGR.FANREQ	Coda di input del processo fan - out della sottoscrizione proxy interno di pubblicazione / sottoscrizione distribuita IBM MQ
SYSTEM.INTER.QMGR.PUBS	Pubblicazioni di pubblicazione / sottoscrizione distribuite IBM MQ
SYSTEM.HIERARCHY.STATE	IBM MQ stato della relazione della gerarchia di pubblicazione / sottoscrizione distribuita

z/OS Su z/OS, si impostano gli oggetti di sistema necessari quando si crea il gestore code, includendo gli esempi CSQ4INSX, CSQ4INSR e CSQ4INSG nel dataset di input di inizializzazione CSQINP2 . Per ulteriori informazioni, consultare Attività 13: personalizzazione dei dataset di input di inizializzazione.

Gli attributi delle code di sistema di pubblicazione / sottoscrizione sono mostrati in Tabella 7 a pagina 111.

Tabella 7. Attributi delle code di sistema di pubblicazione / sottoscrizione

Attributo	**Valore predefinito**
DEFPSIST	Sì
DEFSOPT	CONDIVISO
MAXMSGL	Multi Su Multipiattaforma: il valore del parametro MAXMSGL del comando ALTER QMGR z/OS Su z/OS: 4194304 (ovvero, 4 MB)
MAXDEPTH	999999999
SHARE	N/A
z/OS z/OS STGCLASS	Questo attributo viene utilizzato solo su piattaforme z/OS

Nota: L'unica coda che contiene i messaggi immessi dalle applicazioni è SYSTEM.INTER.QMGR.PUBS. **MAXDEPTH** è impostato sul relativo valore massimo per questa coda per consentire la creazione temporanea di messaggi pubblicati durante le interruzioni o i tempi di carico eccessivo. Se il gestore code è in esecuzione su un sistema in cui non è stato possibile contenere tale profondità di coda, è necessario modificarla.

Attività correlate

Risoluzione dei problemi di pubblicazione / sottoscrizione distribuiti

Errori della coda di sistema di pubblicazione / sottoscrizione distribuita

Gli errori possono verificarsi quando le code del gestore code di pubblicazione / sottoscrizione distribuite non sono disponibili. Ciò influisce sulla diffusione della conoscenza della sottoscrizione nella rete di pubblicazione / sottoscrizione e sulla pubblicazione delle sottoscrizioni sui gestori code remoti.

Se la coda di richieste di fan - out SYSTEM.INTER.QMGR.FANREQ non è disponibile, la creazione di una sottoscrizione potrebbe generare un errore e i messaggi di errore verranno scritti nel log di errori del gestore code quando le sottoscrizioni proxy devono essere consegnate ai gestori code connessi direttamente.

Se la coda di stato della relazione della gerarchia SYSTEM.HIERARCHY.STATE non è disponibile, viene scritto un messaggio di errore nel log degli errori del gestore code e il motore di pubblicazione / sottoscrizione viene messo in modalità COMPAT . Per visualizzare la modalità di pubblicazione / sottoscrizione, utilizzare il comando DISPLAY QMGR PSMODE.

Se altre code SYSTEM.INTER.QMGR non sono disponibili, viene scritto un messaggio di errore nel log degli errori del gestore code e, sebbene la funzione non sia disabilitata, è probabile che i messaggi di pubblicazione / sottoscrizione si accumulino sulle code su questo o su gestori code remoti.

Se la coda del sistema di pubblicazione / sottoscrizione o la coda di trasmissione richiesta a un gestore code del cluster principale, secondario o di pubblicazione / sottoscrizione non è disponibile, si verificano i seguenti risultati:

- Le pubblicazioni non vengono consegnate e un'applicazione di pubblicazione potrebbe ricevere un errore. Per informazioni dettagliate su quando l'applicazione di pubblicazione riceve un errore, consultare i seguenti parametri del comando **DEFINE TOPIC** : **PMSGDLV** , **NPMSGDLV** e **USEDLQ** .
- Le pubblicazioni tra gestori code ricevute vengono sottoposte a backout nella coda di input e successivamente ritentate. Se viene raggiunta la soglia di backout, le pubblicazioni non consegnate vengono inserite nella coda dei messaggi non recapitabili. Il log degli errori del gestore code conterrà i dettagli del problema.
- Viene eseguito il backout di una sottoscrizione proxy non consegnata nella coda di richiesta fanout e successivamente un nuovo tentativo. Se viene raggiunta la soglia di backout, la sottoscrizione proxy non consegnata non viene consegnata ad alcun gestore code connesso e viene collocata nella coda di messaggi non recapitabili. Il log degli errori del gestore code conterrà i dettagli del problema, inclusi i dettagli di qualsiasi azione di gestione correttiva necessaria richiesta.
- I messaggi del protocollo di relazione della gerarchia hanno esito negativo e lo stato della connessione è contrassegnato come ERROR. Per visualizzare lo stato della connessione, utilizzare il comando **DISPLAY PUBSUB**.

Attività correlate

Risoluzione dei problemi di pubblicazione / sottoscrizione distribuiti

Multi Pianificazione dei requisiti di storage e prestazioni su Multiplatforms

È necessario impostare un archivio realistico e raggiungibile e obiettivi di prestazioni per il proprio sistema IBM MQ . Utilizzare i link per informazioni sui fattori che influenzano l'archiviazione e le prestazioni sulla piattaforma.

I requisiti variano in base ai sistemi su cui si utilizza IBM MQ e ai componenti che si desidera utilizzare.

Per le informazioni più recenti sugli ambienti hardware e software supportati, consultare Requisiti di sistema perIBM MQ.

IBM MQ memorizza i dati del gestore code nel filesystem. Utilizzare i seguenti collegamenti per informazioni sulla pianificazione e la configurazione delle strutture di directory da utilizzare con IBM MQ:

- "Pianificazione del supporto del file system su Multiplatforms" a pagina 117
- "Requisiti per i file system condivisi su Multiplatforms" a pagina 118
- "Condivisione di file IBM MQ su Multiplatforms" a pagina 127
- Linux AIX "Struttura di directory su sistemi AIX and Linux ." a pagina 129
- Windows "Struttura di directory su sistemi Windows ." a pagina 137
- IBM i "Struttura di directory su IBM i" a pagina 141

Utilizzare i collegamenti seguenti per informazioni relative alle risorse di sistema, alla memoria condivisa e alla priorità del processo su AIX and Linux:

- Linux AIX "Risorse IPC IBM MQ e UNIX System V" a pagina 145
- AIX "Memoria condivisa su AIX" a pagina 144
- Linux AIX "Priorità processo IBM MQ e UNIX" a pagina 145

Utilizzare i seguenti collegamenti per informazioni sui file di log:

- "Scelta della registrazione circolare o lineare su Multiplatforms" a pagina 144
- Calcolo della dimensione del log

Concetti correlati

"Pianificazione dell'ambiente IBM MQ su z/OS" a pagina 146
Quando si pianifica l'ambiente IBM MQ , è necessario considerare i requisiti delle risorse per i dataset, i set di pagine, Db2, le CF (Coupling Facility) e la necessità di funzioni di registrazione e backup. Utilizzare questo argomento per pianificare l'ambiente in cui viene eseguito IBM MQ .

Attività correlate

"Pianificazione di un'architettura IBM MQ" a pagina 5
Quando si pianifica l'ambiente IBM MQ , considerare il supporto fornito da IBM MQ per le architetture di gestori code singoli e multipli e per gli stili di messaggistica point-to-point e di pubblicazione / sottoscrizione. Inoltre, pianificare i requisiti delle risorse e l'utilizzo delle funzioni di registrazione e backup.

Riferimenti correlati

Requisiti hardware e software su AIX and Linux
Requisiti hardware e software su Windows

Multi Requisiti di spazio su disco su Multiplatforms

I requisiti di memoria per IBM MQ dipendono dai componenti che si installano e dallo spazio di lavoro necessario.

L'archiviazione su disco è richiesta per i componenti facoltativi che si sceglie di installare, inclusi i componenti prerequisiti richiesti. Il requisito di memoria totale dipende anche dal numero di code utilizzate, dal numero e dalla dimensione dei messaggi nelle code e se i messaggi sono persistenti. È inoltre necessaria la capacità di archiviazione su disco, nastro o altri supporti, nonché lo spazio per i propri programmi applicativi.

Le seguenti tabelle mostrano lo spazio su disco approssimativo richiesto quando si installano varie combinazioni del prodotto su piattaforme differenti. (I valori vengono arrotondati per eccesso ai 5 MB più vicini, dove un MB è 1.048.576 byte.)

- LTS “Requisiti di spazio su disco per Long Term Support” a pagina 114
- CD “Requisiti di spazio su disco per Continuous Delivery” a pagina 115

Requisiti di spazio su disco per Long Term Support

V 9.3.0 LTS

Tabella 8. IBM MQ requisiti di spazio su disco per Multiplatforms for Long Term Support			
Piattaforma	**Installazione client** “1” a pagina 114	**Installazione server** “2” a pagina 114	**Installazione completa** “3” a pagina 114
AIX AIX	335 MB	375 MB	1810 MB
IBM i IBM i (consultare Note aggiuntive per IBM i)	485 MB	845 MB	1965 MB
Linux Linux for x86-64	270 MB	295 MB	2010 MB
Linux Linux on Power Systems - Little Endian	170 MB	190 MB	1400 MB
Linux Linux for IBM Z	255 MB	290 MB	1485 MB
Windows Windows (installazione a 64 bit) “4” a pagina 114	295 MB	415 MB	2310 MB

Note:

1. Un'installazione client include i seguenti componenti:
   - Runtime
   - Client
2. Un'installazione server include i componenti seguenti:
   - Runtime
   - Server
3. Un'installazione completa include tutti i componenti disponibili.
4. Windows Non tutti i componenti qui elencati sono funzioni installabili su sistemi Windows ; la loro funzionalità è talvolta inclusa in altre funzioni. Vedere IBM MQ funzioni per i sistemi Windows.

Ulteriori note per IBM i: IBM i

1. Su IBM i non è possibile separare il client nativo dal server. La figura del server nella tabella è per 5724H72*BASE senza Java, insieme al caricamento in lingua inglese (2924). Ci sono 22 possibili carichi di lingua univoci.
2. La figura nella tabella è per il client nativo 5725A49 *BASE senza Java.
3. Le classi Java e JMS possono essere aggiunte sia ai bind server che client. Se si desidera includere queste funzioni aggiungere 110 MB.
4. L'aggiunta dell'origine degli esempi al client o al server aggiunge altri 10 MB.

5. L'aggiunta di esempi alle classi Java e JMS aggiunge ulteriori 5 MB.

Requisiti di spazio su disco per Continuous Delivery

V 9.3.0 CD

Tabella 9. IBM MQ requisiti di spazio su disco per Multiplatforms for Continuous Delivery

Release Platform/CD	Installazione client "1" a pagina 117	Installazione server "2" a pagina 117	Installazione completa "3" a pagina 117
AIX **AIX**			
V 9.3.0 IBM MQ 9.3.0	330 MB	375 MB	1760 MB
V 9.3.1 IBM MQ 9.3.1	340 MB	375 MB	1815 MB
V 9.3.2 IBM MQ 9.3.2	355 MB	390 MB	1440 MB
V 9.3.3 IBM MQ 9.3.3	355 MB	390 MB	1440 MB
V 9.3.4 IBM MQ 9.3.4	355 MB	390 MB	1440 MB
V 9.3.5 IBM MQ 9.3.5	355 MB	390 MB	1440 MB
Linux **Linux per x86-64 (64 bit)**			
V 9.3.0 IBM MQ 9.3.0	265 MB	295 MB	2010 MB
V 9.3.1 IBM MQ 9.3.1	275 MB	295 MB	2010 MB
V 9.3.2 IBM MQ 9.3.2	280 MB	295 MB	1195 MB
V 9.3.3 IBM MQ 9.3.3	280 MB	295 MB	1195 MB
V 9.3.4 IBM MQ 9.3.4	280 MB	295 MB	1195 MB
V 9.3.5 IBM MQ 9.3.5	280 MB	295 MB	1195 MB
Linux **Linux on Power Systems - Little Endian**			
V 9.3.0 IBM MQ 9.3.0	170 MB	190 MB	1350 MB
V 9.3.1 IBM MQ 9.3.1	170 MB	195 MB	1400 MB

Tabella 9. IBM MQ requisiti di spazio su disco per Multiplatforms for Continuous Delivery (Continua)			
Release Platform/CD	**Installazione client** "1" a pagina 117	**Installazione server** "2" a pagina 117	**Installazione completa** "3" a pagina 117
V 9.3.2 IBM MQ 9.3.2	170 MB	195 MB	1075 MB
V 9.3.3 IBM MQ 9.3.3	170 MB	195 MB	1075 MB
V 9.3.4 IBM MQ 9.3.4	170 MB	195 MB	1075 MB
V 9.3.5 IBM MQ 9.3.5	170 MB	195 MB	1075 MB
Linux **Linux per IBM Z**			
V 9.3.0 IBM MQ 9.3.0	255 MB	290 MB	1435 MB
V 9.3.1 IBM MQ 9.3.1	255 MB	290 MB	1485 MB
V 9.3.2 IBM MQ 9.3.2	260 MB	290 MB	1160 MB
V 9.3.3 IBM MQ 9.3.3	260 MB	290 MB	1160 MB
V 9.3.4 IBM MQ 9.3.4	260 MB	290 MB	1160 MB
V 9.3.5 IBM MQ 9.3.5	260 MB	290 MB	1160 MB
Windows **Windows (installazione a 64 bit)** "4" a pagina 117			
V 9.3.0 IBM MQ 9.3.0	290 MB	410 MB	2095 MB
V 9.3.1 IBM MQ 9.3.1	295 MB	415 MB	2310 MB
V 9.3.2 IBM MQ 9.3.2	300 MB	415 MB	1785 MB
V 9.3.3 IBM MQ 9.3.3	300 MB	415 MB	1785 MB
V 9.3.4 IBM MQ 9.3.4	300 MB	415 MB	1785 MB
V 9.3.5 IBM MQ 9.3.5	300 MB	415 MB	1785 MB

Note:

1. Un'installazione client include i seguenti componenti:
   - Runtime
   - Client
2. Un'installazione server include i componenti seguenti:
   - Runtime
   - Server
3. Un'installazione completa include tutti i componenti disponibili.
4. Windows Non tutti i componenti qui elencati sono funzioni installabili su sistemi Windows ; la loro funzionalità è talvolta inclusa in altre funzioni. Vedere IBM MQ funzioni per i sistemi Windows.

Concetti correlati

Componenti e funzioni di IBM MQ

Multi Pianificazione del supporto del file system su Multiplatforms

I dati del gestore code vengono memorizzati nel file system. Un gestore code utilizza il blocco del file system per impedire che più istanze di un gestore code a più istanze siano attive contemporaneamente.

File system condivisi

I file system condivisi consentono a più sistemi di accedere simultaneamente alla stessa periferica di archiviazione fisica. Si verificherebbe un danneggiamento se più sistemi accedessero direttamente allo stesso dispositivo di archiviazione fisico senza alcun mezzo per applicare il blocco e il controllo della simultaneità. I sistemi operativi forniscono i file system locali con il controllo del blocco e della simultaneità per i processi locali; i file system di rete forniscono il controllo del blocco e della simultaneità per i sistemi distribuiti.

Storicamente, i file system di rete non sono stati eseguiti abbastanza velocemente, o hanno fornito un sufficiente controllo di blocco e simultaneità, per soddisfare i requisiti per la registrazione dei messaggi. Oggi, i file system in rete possono fornire buone prestazioni e implementazioni di protocolli di file system di rete affidabili come *RFC 3530, Network File System (NFS) version 4 protocol*, soddisfano i requisiti per la registrazione dei messaggi in modo affidabile.

File system condivisi e IBM MQ

I dati del gestore code per un gestore code a più istanze sono memorizzati in un file system di rete condiviso. Sui sistemi AIX, Linux, and Windows , i file di dati e i file di log del gestore code devono essere collocati nel file system di rete condiviso. IBM i Su IBM i, i journal vengono utilizzati al posto dei file di log e i journal non possono essere condivisi. I gestori code a più istanze su IBM i utilizzano la replica del journal o journal commutabili, per rendere i journal disponibili tra diverse istanze del gestore code.

IBM MQ utilizza il blocco per impedire che più istanze dello stesso gestore code a più istanze siano attive contemporaneamente. Lo stesso blocco garantisce inoltre che due gestori code separati non possano inavvertitamente utilizzare la stessa serie di file di dati del gestore code. Solo un'istanza di un gestore code può avere il blocco alla volta. Di conseguenza, IBM MQ supporta i dati del gestore code memorizzati nella memoria di rete a cui si accede come un file system condiviso.

Poiché non tutti i protocolli di blocco dei file system di rete sono solidi e poiché un file system potrebbe essere configurato per le prestazioni piuttosto che per l'integrità dei dati, è necessario eseguire il comando **amqmfsck** per verificare se un file system di rete controllerà correttamente l'accesso ai dati e ai log del gestore code. Questo comando si applica solo ai sistemi UNIX, Linux e IBM i . Su Windows, esiste un solo file system di rete supportato e il comando **amqmfsck** non è obbligatorio.

Attività correlate

“Verifica del funzionamento del file system condiviso su Multiplatforms” a pagina 119

Eseguire **amqmfsck** per controllare se un file system condiviso su AIX, Linux o IBM i soddisfa i requisiti per la memorizzazione dei dati del gestore code di un gestore code a più istanze. (L'unico requisito per una configurazione Windows è che utilizzi SMB 3 per il provisioning di memoria condivisa.)

Multi Requisiti per i file system condivisi su Multiplatforms

I file system condivisi devono fornire l'integrità di scrittura dei dati, garantire l'accesso esclusivo ai file e rilasciare i blocchi in caso di errore per lavorare in modo affidabile con IBM MQ.

Requisiti che un file system condiviso deve soddisfare

Ci sono tre requisiti fondamentali che un file system condiviso deve soddisfare per funzionare in modo affidabile con IBM MQ:

1. Integrità di scrittura dei dati

   L'integrità di scrittura dei dati è a volte denominata *Write through to disk on flush*. Il gestore code deve essere in grado di sincronizzarsi con i dati di cui è stato eseguito correttamente il commit sul dispositivo fisico. In un sistema transazionale, è necessario essere certi che alcune scritture siano state sottoposte a commit in modo sicuro prima di continuare con altre elaborazioni.

   Più specificamente, le piattaforme IBM MQ for AIX or Linux utilizzano l'opzione di apertura *O_SYNC* e la chiamata di sistema `fsync()` per forzare esplicitamente le scritture sul supporto ripristinabile e l'operazione di scrittura dipende dal corretto funzionamento di queste opzioni.

   Attenzione: Linux È necessario montare il filesystem con l'opzione `async` , che supporta ancora l'opzione di scritture sincrone e fornisce prestazioni migliori rispetto all'opzione `sync` .

   Tenere presente, tuttavia, che se il file system è stato esportato da Linux, è comunque necessario esportare il file system utilizzando l'opzione `sync` .

2. Accesso esclusivo garantito ai file

   Per sincronizzare più gestori code, è necessario che un gestore code ottenga un blocco esclusivo su un file.

3. Rilascia i blocchi in caso di errore

   Se un gestore code ha esito negativo o se si verifica un errore di comunicazione con il file system, i file bloccati dal gestore code devono essere sbloccati e resi disponibili ad altri processi senza attendere che il gestore code venga riconnesso al file system.

Un file system condiviso deve soddisfare questi requisiti affinché IBM MQ possa funzionare in modo affidabile. In caso contrario, i log e i dati del gestore code vengono danneggiati quando si utilizza il file system condiviso in una configurazione del gestore code a più istanze.

Per i gestori code a più istanze su Microsoft Windows, la memoria di rete deve essere acceduta dal protocollo SMB (Server Message Block) utilizzato dalle reti Microsoft Windows . Il client SMB (Server Message Block) non soddisfa i requisiti IBM MQ per bloccare la semantica su piattaforme diverse da Microsoft Windows, quindi i gestori code a più istanze in esecuzione su piattaforme diverse da Microsoft Windows non devono utilizzare SMB (Server Message Block) come file system condiviso.

Per i gestori code a più istanze su altre piattaforme supportate, l'archiviazione deve essere acceduta da un protocollo del file system di rete compatibile con Posix e che supporta il blocco basato sul lease. Network File System 4 soddisfa questo requisito. I file system più vecchi, come Network File System Versione 3, che non dispongono di un meccanismo affidabile per rilasciare i blocchi dopo un malfunzionamento, non devono essere utilizzati con i gestori code a più istanze.

Verifica se il file system condiviso soddisfa i requisiti

È necessario verificare se il file system condiviso che si intende utilizzare soddisfa questi requisiti. È inoltre necessario verificare se il filesystem è configurato correttamente per l'affidabilità. I file

system condivisi a volte forniscono opzioni di configurazione per migliorare le prestazioni a scapito dell'affidabilità.

Per ulteriori informazioni, consultare Verifica dell'istruzione per i file system del gestore code a più istanze IBM MQ.

In circostanze normali, IBM MQ funziona correttamente con la memorizzazione nella cache dell'attributo e non è necessario disabilitare la memorizzazione nella cache, ad esempio impostando NOAC su un montaggio NFS . La memorizzazione nella cache degli attributi può causare problemi quando più client del file system si contendono l'accesso in scrittura allo stesso file sul server del file system, in quanto gli attributi memorizzati nella cache utilizzati da ciascun client potrebbero non essere gli stessi degli attributi sul server. Un esempio di file a cui si accede in questo modo sono i log degli errori del gestore code per un gestore code a più istanze. I log degli errori del gestore code potrebbero essere scritti sia da un'istanza del gestore code attiva che da un'istanza del gestore code in standby e gli attributi dei file memorizzati nella cache potrebbero causare una crescita dei log degli errori superiore a quella prevista, prima che si verifichi il rollover dei file.

Per un ausilio nel controllo del file system, eseguire l'attività Verifica del funzionamento del file system condiviso. Questa attività controlla se il file system condiviso soddisfa i requisiti 2 e 3. È necessario verificare il requisito 1 nella documentazione del file system condiviso o sperimentando la registrazione dei dati sul disco.

Gli errori del disco possono causare errori durante la scrittura su disco, che IBM MQ riporta come errori FFDC (First Failure Data Capture). È possibile eseguire il programma di controllo del file system per il proprio sistema operativo per controllare il file system condiviso per eventuali errori del disco. Ad esempio:

- Linux AIX Su AIX and Linux il programma di controllo del file system è denominato fsck.
- Windows Su piattaforme Windows , il programma di controllo del file system è denominato CHKDSK o SCANDISK.

Sicurezza server NFS

Note:

- Non è possibile utilizzare le opzioni **nosuid** o **noexec** per un punto di montaggio utilizzato per contenere la directory di installazione di IBM MQ . Ciò è dovuto al fatto che IBM MQ include programmi eseguibili setuid / setgid e a questi non deve essere impedita la corretta esecuzione.
- Quando si inseriscono i dati del gestore code solo su un server NFS (Network File System) (NFS), è possibile utilizzare le seguenti tre opzioni con il comando mount per rendere il sistema sicuro, senza alcun impatto dannoso sull'esecuzione del gestore code:

  noexec
  Utilizzando questa opzione, si impedisce l'esecuzione dei file binari su NFS, il che impedisce a un utente remoto di eseguire codice indesiderato sul sistema.

  nosuid
  Utilizzando questa opzione, si impedisce l'utilizzo dei bit set - user - identifier e set - group - identifier, che impediscono a un utente remoto di ottenere privilegi più elevati.

  nessun dev
  Utilizzando questa opzione, si arrestano i caratteri e si bloccano i dispositivi speciali da utilizzare o definire, il che impedisce a un utente remoto di uscire da una prigione chroot.

IBM i Linux AIX *Verifica del funzionamento del file system condiviso su Multiplatforms*

Eseguire **amqmfsck** per controllare se un file system condiviso su AIX, Linux o IBM i soddisfa i requisiti per la memorizzazione dei dati del gestore code di un gestore code a più istanze. (L'unico requisito per una configurazione Windows è che utilizzi SMB 3 per il provisioning di memoria condivisa.)

Prima di iniziare

È necessario un server con memoria di rete e altri due server connessi ad esso che hanno IBM MQ installato. È necessario disporre dell'autorizzazione di amministratore (root) per la configurazione del file system ed essere un IBM MQ amministratore per eseguire **amqmfsck**.

Informazioni su questa attività

"Requisiti per i file system condivisi su Multiplatforms" a pagina 118 descrive i requisiti del filesystem per l'utilizzo di un filesystem condiviso con gestori code a più istanze. La IBM MQ nota tecnica Istruzione di test per i file system del gestore code a più istanze IBM MQ elenca i file system condivisi con cui IBM ha già eseguito il test. La procedura in questa attività descrive come eseguire il test di un file system per valutare se un file system non elencato conserva l'integrità dei dati.

Il failover di un gestore code a più istanze può essere attivato da errori hardware o software, inclusi problemi di rete che impediscono al gestore code di scrivere nei propri dati o file di log. Principalmente, si è interessati a causare errori sul server di file. Ma è anche necessario far sì che i server IBM MQ abbiano esito negativo, per verificare che tutti i blocchi siano stati rilasciati correttamente. Per essere sicuri in un file system condiviso, verificare tutti i seguenti errori e tutti gli altri errori specifici del proprio ambiente:

1. Chiusura del sistema operativo sul file server inclusa la sincronizzazione dei dischi.
2. Arresto del sistema operativo sul file server senza sincronizzazione dei dischi.
3. Premendo il pulsante di reimpostazione su ciascuno dei server.
4. Estrarre il cavo di rete da ciascuno dei server.
5. Estrarre il cavo di alimentazione da ciascun server.
6. Disattivare ciascuno dei server.

Creare la directory sulla memoria di rete che si intende utilizzare per condividere i dati e i log del gestore code. Il proprietario della directory deve essere un Amministratore IBM MQ o, in altre parole, un membro del gruppo `mqm` su AIX and Linux. L'utente che esegue i test deve disporre dell'autorizzazione di amministratore IBM MQ .

Utilizzare l'esempio di esportazione e montaggio di un filesystem in Creazione di un gestore code a più istanze su Linux o Creazione di un gestore code a più istanze utilizzando il mirroring del journal e NetServer su IBM i per facilitare la configurazione del filesystem. File system diversi richiedono diversi passi di configurazione. Leggere la documentazione del file system.

Nota: Eseguire il IBM MQ MQI client programma di esempio **amqsfhac** in parallelo con **amqmfsck** per dimostrare che un gestore code conserva l'integrità del messaggio durante un malfunzionamento.

Procedura

In ogni controllo, causare tutti gli errori nell'elenco precedente mentre il programma di controllo del file system è in esecuzione. Se si intende eseguire **amqsfhac** contemporaneamente a **amqmfsck**, eseguire l'attività "Esecuzione di amqsfhac per verificare l'integrità del messaggio" a pagina 125 in parallelo con questa attività.

1. Montare la directory esportata sui due server IBM MQ .

   Sul server di file system creare una directory condivisa `share`de una sottodirectory per salvare i dati per i gestori code a più istanze, `qmdata`. Per un esempio di impostazione di una directory condivisa per i gestori code a più istanze su Linux, consultare Creazione di un gestore code a più istanze su Linux
2. Controllare il funzionamento del file system di base.

   Su un server IBM MQ , eseguire il programma di controllo del file system senza parametri.

   Sul server IBM MQ 1:

   ```
   amqmfsck /shared/qmdata
   ```
3. Controllare la scrittura simultanea nella stessa directory da entrambi i server IBM MQ .

Su due server IBM MQ , eseguire il programma di controllo del file system contemporaneamente con l'opzione `-c` .

Sul server IBM MQ 1:

```
amqmfsck -c /shared/qmdata
```

Sul server IBM MQ 2:

```
amqmfsck -c /shared/qmdata
```

4. Verificare di attendere e rilasciare i blocchi su entrambi i server IBM MQ .

   Su entrambi i server IBM MQ eseguire il programma di controllo del filesystem contemporaneamente con l'opzione `-w` .

   Sul server IBM MQ 1:

   ```
   amqmfsck -w /shared/qmdata
   ```

   Sul server IBM MQ 2:

   ```
   amqmfsck -w /shared/qmdata
   ```

5. Verificare l'integrità dei dati.

   a) Formattare il file di test.

   Creare un file di grandi dimensioni nella directory che si sta verificando. Il file viene formattato in modo che le fasi successive possano essere completate correttamente. Il file deve essere abbastanza grande da avere tempo sufficiente per interrompere la seconda fase per simulare il failover. Provare il valore predefinito di 262144 pagine (1 GB). Il programma riduce automaticamente questo valore predefinito sui filesystem lenti in modo che la formattazione venga completata in circa 60 secondi

   Sul server IBM MQ 1:

   ```
   amqmfsck -f /shared/qmdata
   ```

   Il server risponde con i seguenti messaggi:

   ```
   Formatting test file for data integrity test.

   Test file formatted with 262144 pages of data.
   ```

   b) Scrivere i dati nel file di test utilizzando il programma di controllo del file system durante la causa di un errore.

   Eseguire il programma di test su due server contemporaneamente. Avviare il programma di test sul server su cui si verificherà l'errore, quindi avviare il programma di test sul server che sopravviverà all'errore. Causa dell'errore che si sta analizzando.

   Il primo programma di test viene arrestato con un messaggio di errore. Il secondo programma di test ottiene il blocco sul file di test e scrive i dati nel file di test a partire dal punto in cui il primo programma di test si è spento. Consentire il completamento del secondo programma di test.

Tabella 10. Esecuzione del controllo di integrità dei dati su due server contemporaneamente

IBM MQ Server 1	**IBM MQ Server 2**
`amqmfsck -a /shared/qmdata`	

Tabella 10. Esecuzione del controllo di integrità dei dati su due server contemporaneamente (Continua)

IBM MQ Server 1	IBM MQ Server 2

`Please start this program on a second machine`
`with the same parameters.`
 	
`File lock acquired.`
 	
`Start a second copy of this program with the same parameters on another server.`
 	
`Writing data into test file.`
 	
`To increase the effectiveness of the test, interrupt the writing by ending the process,`
`temporarily breaking the network connection`
`to the networked storage,`
`rebooting the server or turning off the power.`
	`amqmfsck -a /shared/qmdata`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`

Turn the power off here.	

	`File lock acquired.`
	
	`Reading test file`
	
	`Checking the integrity of the data read.`
	
	`Appending data into the test file after data already found.`
	
	`The test file is full of data. It is ready to be inspected for data integrity.`

La tempistica del test dipende dal comportamento del file system. Ad esempio, generalmente impiega 30-90 secondi perché un file system rilasci i blocchi di file ottenuti dal primo programma dopo un'interruzione di corrente. Se si ha poco tempo per introdurre l'errore prima che il primo programma di test abbia riempito il file, utilizzare l'opzione `-x` di **amqmfsck** per eliminare il file di test. Provare il test dall'inizio con un file di test più grande.

c) Verificare l'integrità dei dati nel file di test.

Sul server IBM MQ 2:

```
amqmfsck -i /shared/qmdata
```

Il server risponde con i seguenti messaggi:

```
File lock acquired

Reading test file checking the integrity of the data read.

The data read was consistent.
```

```
The tests on the directory completed successfully.
```

6. Eliminare i file di test.

   Sul server IBM MQ 2:

   ```
   amqmfsck -x /shared/qmdata

   Test files deleted.
   ```

   Il server risponde con il messaggio:

   ```
   Test files deleted.
   ```

Risultati

Il programma restituisce un codice di uscita di zero se i test vengono completati correttamente, altrimenti un codice diverso da zero.

Esempi

La prima serie di tre esempi mostra il comando che produce un output minimo.

Test riuscito del blocco file di base su un server

```
> amqmfsck /shared/qmdata
The tests on the directory completed successfully.
```

Test non riuscito del blocco del file di base su un server

```
> amqmfsck /shared/qmdata
AMQ6245: Error Calling 'write()[2]' on file '/shared/qmdata/amqmfsck.lck' error '2'.
```

Test di blocco riuscito su due server

Tabella 11. Blocco riuscito su due server

IBM MQ Server 1	IBM MQ Server 2

`> amqmfsck -w /shared/qmdata`
`Please start this program on a second`
`machine with the same parameters.`
`Lock acquired.`
`Press Return`
`or terminate the program to release the lock.`	

	`> amqmfsck -w /shared/qmdata` `Waiting for lock...`
`[ Return pressed ]` `Lock released.`	

	`Lock acquired.`
	`The tests on the directory completed`
	`successfully`

La seconda serie di tre esempi mostra gli stessi comandi utilizzando la modalità dettagliata.

Test riuscito del blocco file di base su un server

```
> amqmfsck -v /shared/qmdata
System call: stat("/shared/qmdata")'
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
```

```
System call: fchmod(fd, 0666)
System call: fstat(fd)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: write(fd)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: close(fd)
System call: fd1 = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd1, F_SETLK, F_RDLCK)
System call: fd2 = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd2, F_SETLK, F_RDLCK)
System call: close(fd2)
System call: write(fd1)
System call: close(fd1)
The tests on the directory completed successfully.
```

Test non riuscito del blocco del file di base su un server

```
> amqmfsck -v /shared/qmdata
System call: stat("/shared/qmdata")
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fchmod(fd, 0666)
System call: fstat(fd)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: write(fd)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_RDLCK)
System call: fdSameFile = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fdSameFile, F_SETLK, F_RDLCK)
System call: close(fdSameFile)
System call: write(fd)
AMQxxxx: Error calling 'write()[2]' on file '/shared/qmdata/amqmfsck.lck', errno 2
(Permission denied).
```

Test di blocco riuscito su due server

Tabella 12. Blocco riuscito su due server - modalità dettagliata

IBM MQ Server 1	IBM MQ Server 2

`> amqmfsck -wv /shared/qmdata`
`Calling 'stat("/shared/qmdata")'`
`Calling 'fd = open("/shared/qmdata/`
`amqmfsck.lkw",`
`O_EXCL | O_CREAT | O_RDWR, 0666)'`
`Calling 'fchmod(fd, 0666)'`
`Calling 'fstat(fd)'`
`Please start this program on a second`
`machine with the same parameters.`
`Calling 'fcntl(fd, F_SETLK, F_WRLCK)'`
`Lock acquired.`
`Press Return`
`or terminate the program to release the lock.`	

	`> amqmfsck -wv /shared/qmdata`
	`Calling 'stat("/shared/qmdata")'`
	`Calling 'fd = open("/shared/qmdata/`
	`amqmfsck.lkw",`
	`O_EXCL | O_CREAT | O_RDWR,0666)'`
	`Calling 'fd = open("/shared/qmdata/amqmfsck.lkw,`
	`O_RDWR, 0666)'`
	`Calling 'fcntl(fd, F_SETLK, F_WRLCK)`
	`'Waiting for lock...`

`[ Return pressed ]`
`Calling 'close(fd)'`
`Lock released.`	

Tabella 12. Blocco riuscito su due server - modalità dettagliata (Continua)	
IBM MQ Server 1	**IBM MQ Server 2**

	`Calling 'fcntl(fd, F_SETLK, F_WRLCK)'`
	`Lock acquired.`
	`The tests on the directory completed successfully`

Riferimenti correlati

Programmi di esempio HA (High Availability)

Multi

Esecuzione di amqsfhac per verificare l'integrità del messaggio

Eseguire il IBM MQ MQI client programma di esempio **amqsfhac** in parallelo con **amqmfsck** per dimostrare che un gestore code conserva l'integrità del messaggio durante un errore.

Prima di iniziare

Sono necessari quattro server per questo test. Due server per il gestore code a più istanze, uno per il file system e uno per l'esecuzione di **amqsfhac** come applicazione IBM MQ MQI client .

Seguire il passo “1” a pagina 120 in “Verifica del funzionamento del file system condiviso su Multiplatforms” a pagina 119 per configurare il file system per un gestore code a più istanze.

Informazioni su questa attività

Il IBM MQ MQI client programma di esempio **amqsfhac** controlla che un gestore code che utilizza la memoria di rete mantenga l'integrità dei dati in seguito a un errore. Eseguire **amqsfhac** in parallelo con **amqmfsck** per dimostrare che un gestore code conserva l'integrità del messaggio durante un errore.

Procedura

1. Creare un gestore code a più istanze su un altro server, QM1, utilizzando il file system creato al passo “1” a pagina 120 nella Procedura.

   Consultare Crea un gestore code a più istanze.
2. Avviare il gestore code su entrambi i server rendendolo altamente disponibile.

   Sul server 1:

   ```
   strmqm -x QM1
   ```

   Sul server 2:

   ```
   strmqm -x QM1
   ```
3. Impostare la connessione client per eseguire **amqsfhac**.
   a) Utilizzare la procedura contenuta in *Verifica di un'installazione di IBM MQ* per la piattaforma o le piattaforme che l'azienda utilizza per configurare una connessione client o gli script di esempio in Esempi di client riconnettibili.
   b) Modificare il canale del client in modo che abbia due indirizzi IP, corrispondenti ai due server su cui è in esecuzione QM1.

      Nello script di esempio, modificare:

      ```
      DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
      CONNAME('LOCALHOST(2345)') QMNAME(QM1) REPLACE
      ```

      A:

```
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
CONNAME('server1(2345),server2(2345)') QMNAME(QM1) REPLACE
```

dove `server1` e `server2` sono i nomi host dei due server e 2345 è la porta su cui è in ascolto il listener del canale. Di solito, il valore predefinito è 1414. È possibile utilizzare 1414 con la configurazione listener predefinita.

4. Creare due code locali su `QM1` per la verifica.
   Eseguire lo script MQSC riportato di seguito:

```
DEFINE QLOCAL(TARGETQ) REPLACE
DEFINE QLOCAL(SIDEQ) REPLACE
```

5. Verifica la configurazione con **amqsfhac**

```
amqsfhac QM1 TARGETQ SIDEQ 2 2 2
```

6. Verificare l'integrit ... del messaggio durante la verifica dell'integrit ... del file system.

   Eseguire **amqsfhac** durante il passo “5” a pagina 121 di “Verifica del funzionamento del file system condiviso su Multiplatforms” a pagina 119.

```
amqsfhac QM1 TARGETQ SIDEQ 10 20 0
```

   Se si arresta l'istanza del gestore code attivo, **amqsfhac** si riconnette all'altra istanza del gestore code una volta che è diventata attiva. Riavviare di nuovo l'istanza del gestore code arrestata, in modo da poter invertire l'errore nella verifica successiva. Sarà probabilmente necessario aumentare il numero di iterazioni in base alla sperimentazione con il proprio ambiente in modo che il programma di test venga eseguito per un tempo sufficiente affinché si verifichi il failover.

Risultati

Un esempio di esecuzione di **amqsfhac** nel passo “6” a pagina 126 viene mostrato nel seguente esempio. In questo esempio, il test ha esito positivo.

```
Sample AMQSFHAC start
qmname = QM1
qname = TARGETQ
sidename = SIDEQ
transize = 10
iterations = 20
verbose = 0
Iteration 0
Iteration 1
Iteration 2
Iteration 3
Iteration 4
Iteration 5
Iteration 6
Resolving MQRC_CALL_INTERRUPTED
MQGET browse side tranid=14 pSideinfo->tranid=14
Resolving to committed
Iteration 7
Iteration 8
Iteration 9
Iteration 10
Iteration 11
Iteration 12
Iteration 13
Iteration 14
Iteration 15
Iteration 16
Iteration 17
Iteration 18
Iteration 19
Sample AMQSFHAC end
```

Se il test ha rilevato un problema, l'output riporta l'errore. In alcune esecuzioni di test, `MQRC_CALL_INTERRUPTED` potrebbe riportare "`Resolving to backed out`". Non fa alcuna differenza

per il risultato. Il risultato dipende dal fatto che la scrittura su disco sia stata sottoposta a commit dall'archivio file di rete prima o dopo che si è verificato l'errore.

Riferimenti correlati

amqmfsck (controllo file system)

Programmi di esempio HA (High Availability)

Multi Condivisione di file IBM MQ su Multiplatforms

Ad alcuni file IBM MQ si accede esclusivamente da un gestore code attivo, mentre altri file sono condivisi.

I file IBM MQ sono suddivisi in file di programma e file di dati. I file di programma sono generalmente installati localmente su ciascun server che esegue IBM MQ. I gestori code condividono l'accesso ai file di dati e alle directory nella directory di dati predefinita. Richiedono l'accesso esclusivo alle proprie strutture di directory del gestore code contenute in ciascuna delle directory `qmgrs` e `log` mostrate in Figura 32 a pagina 127.

Figura 32 a pagina 127 è una vista di alto livello della struttura di directory IBM MQ . Mostra le directory che possono essere condivise tra gestori code e rese remote. I dettagli variano per piattaforma. Le linee tratteggiate indicano percorsi configurabili.

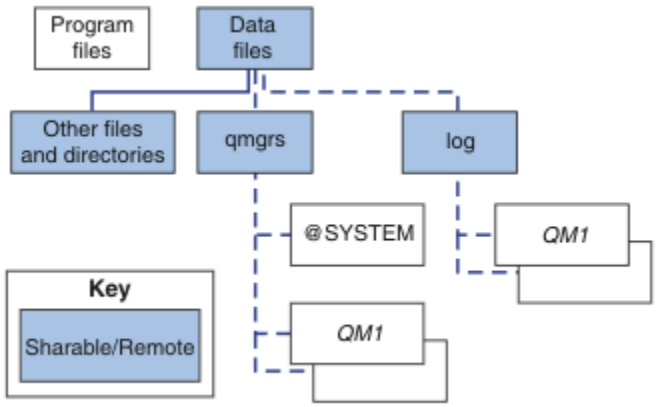


Figura 32. Vista generale della struttura di directory IBM MQ

File di programma

La directory dei file di programma viene generalmente lasciata nell'ubicazione predefinita, è locale e condivisa da tutti i gestori code sul server.

File di dati

La directory dei file di dati è in genere locale nell'ubicazione predefinita, `/var/mqm` sui sistemi AIX and Linux e configurabile sull'installazione su Windows. È condiviso tra gestori code. È possibile rendere remota l'ubicazione predefinita, ma non condividerla tra diverse installazioni di IBM MQ. L'attributo `DefaultPrefix` nella configurazione IBM MQ punta a questo percorso.

`qmgrs`

Esistono due modi alternativi per specificare l'ubicazione dei dati del gestore code.

Utilizzo dell'attributo `Prefix`

L'attributo **`Prefix`** specifica l'ubicazione della directory `qmgrs` . IBM MQ crea il nome della directory del gestore code dal nome del gestore code e lo crea come sottodirectory della directory `qmgrs` .

L'attributo **`Prefix`** si trova nella stanza QueueManager del file `mqs.ini` ed è ereditato dal valore nell'attributo **`DefaultPrefix`** della stanza Tutti i gestori code. Per impostazione predefinita, per semplicità amministrativa, i gestori code generalmente condividono la stessa directory `qmgrs` .

Se si modifica l'ubicazione della directory `qmgrs` per qualsiasi gestore code, è necessario modificare il valore del suo attributo **Prefix** .

L'attributo **Prefix** per la directory `QM1` in Figura 32 a pagina 127 per una piattaforma AIX and Linux è:

```
Prefix=/var/mqm
```

Utilizzo dell'attributo DataPath

L'attributo **DataPath** specifica l'ubicazione della directory di dati del gestore code.

L'attributo **DataPath** specifica il percorso completo, incluso il nome della directory di dati del gestore code. L'attributo **DataPath** è diverso dall'attributo **Prefix** , che specifica un percorso incompleto alla directory dei dati del gestore code.

L'attributo **DataPath** , se specificato, si trova nella stanza stanzaQueueManager del file `mqs.ini` . Se è stato specificato, ha la precedenza su qualsiasi valore nell'attributo **Prefix** .

Se si modifica l'ubicazione della directory dei dati del gestore code per qualsiasi gestore code, è necessario modificare il valore dell'attributo `DataPath` .

L'attributo `DataPath` per la directory `QM1` in Figura 32 a pagina 127, per una piattaforma Linux o AIX , è il seguente:

```
DataPath=/var/mqm/qmgrs/QM1
```

log

La directory di log viene specificata separatamente per ogni gestore code nella sezione Log nella configurazione del gestore code. La configurazione del gestore code è in `qm.ini`.

Sottodirectory *DataPath*/*QmgrName*/@IPCC

Le sottodirectory *DataPath*/*QmgrName*/`@IPCC` si trovano nel percorso della directory condivisa. Vengono utilizzati per creare il percorso indirizzario per gli oggetti file system IPC. È necessario distinguere lo spazio dei nomi di un gestore code quando un gestore code è condiviso tra sistemi.

Gli oggetti del file system IPC devono essere distinti dal sistema. Una sottodirectory, per ogni sistema su cui viene eseguito il gestore code, viene aggiunta al percorso della directory, consultare Figura 33 a pagina 128.

```
DataPath/QmgrName/@IPCC/esem/myHostName/
```

Figura 33. Sottodirectory IPC di esempio

myHostName contiene fino a 20 caratteri del nome host restituito dal sistema operativo. Su alcuni sistemi, il nome host potrebbe avere una lunghezza massima di 64 caratteri prima del troncamento. Il valore generato di *myHostName* potrebbe causare un problema per due motivi:

1. I primi 20 caratteri non sono univoci.
2. Il nome host viene generato da un algoritmo DHCP che non sempre assegna lo stesso nome host a un sistema.

In questi casi, impostare *myHostName* utilizzando la variabile di ambiente **MQS_IPC_HOST**; consultare Figura 34 a pagina 128.

```
export MQS_IPC_HOST= myHostName
```

*Figura 34. Esempio: impostazione **MQS_IPC_HOST***

Altri file e directory

Altri file e directory, come la directory che contiene i file di traccia e il log degli errori comune, vengono normalmente condivisi e conservati sul file system locale.

Con il sostegno dei file system condivisi, IBM MQ gestisce l'accesso esclusivo a questi file utilizzando i blocchi del file system. Un blocco del file system consente di attivare una sola istanza di un particolare gestore code alla volta.

Quando si avvia la prima istanza di uno specifico gestore code, questo assume la proprietà della relativa directory del gestore code. Se si avvia una seconda istanza, questa può assumere la proprietà solo se la prima istanza è stata arrestata. Se il primo gestore code è ancora in esecuzione, la seconda istanza non riesce ad avviarsi e riporta che il gestore code è in esecuzione altrove. Se il primo gestore code è stato arrestato, il secondo gestore code assume la proprietà dei file del gestore code e diventa il gestore code in esecuzione.

È possibile automatizzare la procedura del secondo gestore code che prende il posto del primo gestore code. Avviare il primo gestore code con l'opzione `strmqm -x` che consente a un altro gestore code di eseguire il comando. Il secondo gestore code attende che i file del gestore code vengano sbloccati prima di tentare di acquisire la proprietà dei file del gestore code e di avviarli.

Linux AIX Struttura di directory su sistemi AIX and Linux .

La struttura di directory IBM MQ sui sistemi AIX and Linux può essere associata a diversi file system per una gestione più semplice, migliori prestazioni e una maggiore affidabilità.

Utilizzare la struttura di directory flessibile di IBM MQ per sfruttare i filesystem condivisi per l'esecuzione di gestori code a più istanze.

Utilizzare il comando **crtmqm** *QM1* per creare la struttura di directory mostrata in Figura 35 a pagina 129 dove R è la release del prodotto. Si tratta di una tipica struttura di directory per un gestore code creato su un sistema IBM MQ . Alcune impostazioni di directory, file e attributi .ini vengono omesse per chiarezza e un altro nome gestore code potrebbe essere modificato da un gestore code. I nomi dei file system variano a seconda dei sistemi.

In un'installazione tipica, ogni gestore code creato fa riferimento a directory comuni `log` e `qmgrs` sul file system locale. In una configurazione a più istanze, le indirizzari `log` e `qmgrs` si trovano su un filesystem di rete condiviso con un'altra installazione di IBM MQ.

Figura 35 a pagina 129 mostra la configurazione predefinita per IBM MQ v7.R su AIX , dove R è la release del prodotto. Per esempi di configurazioni alternative a più istanze, vedere“Configurazioni di directory di esempio su sistemi AIX and Linux” a pagina 134.

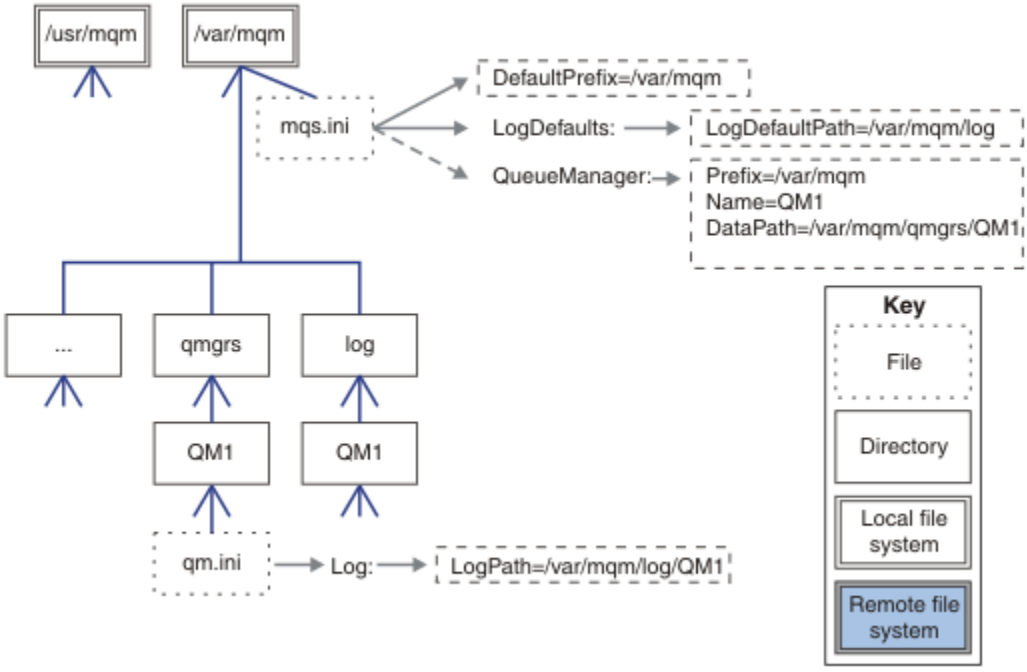


Figura 35. Struttura di directory IBM MQ predefinita di esempio per sistemi AIX and Linux

I file eseguibili del prodotto sono installati di default in `/usr/mqm` su AIX e in `/opt/mqm` sugli altri sistemi. Le directory di lavoro vengono create sotto la directory `/var/mqm` .

Nota: Se è stato creato il file system `/var/mqm` prima di installare IBM MQ , assicurarsi che l'utente mqm disponga delle autorizzazioni di directory complete, ad esempio, la modalità file 755.

Nota: La directory `/var/mqm/errors` deve essere un filesystem separato per impedire che FFDC prodotti dal gestore code riempiscano il filesystem che contiene `/var/mqm`.

Per ulteriori informazioni, consultare Creazione di file system su sistemi AIX and Linux .

Le directory 'log e 'qmgrs sono mostrate nelle loro posizioni predefinite, definite dai valori predefiniti degli attributi LogDefaultPath e DefaultPrefix nel file 'mqs.ini. Quando viene creato un gestore code, per default la directory dei dati del gestore code viene creata in *DefaultPrefix*/qmgrse la directory del file di log in *LogDefaultPath*/log. LogDefaultPath e DefaultPrefix hanno effetto solo sul luogo in cui i gestori di code e i file di registro vengono creati per impostazione predefinita. L'ubicazione effettiva di una directory del gestore code viene salvata nel file `mqs.ini` e l'ubicazione della directory del file di log viene salvata nel file `qm.ini` .

La directory del file di log per un gestore code è definita nel file `qm.ini` nell'attributo LogPath . Utilizzare l'opzione `-ld` nel comando **crtmqm** per impostare l'attributo LogPath per un gestore code; ad esempio **crtmqm** `-ld` *LogPath* `QM1` . Se si omette il parametro ld, viene utilizzato il valore di LogDefaultPath.

La directory dei dati del gestore code è definita nell'attributo DataPath della stanza QueueManager del file `mqs.ini` . Utilizzare l'opzione `-md` sul comando **crtmqm** per impostare DataPath per un gestore code; ad esempio, **crtmqm** `- md` *DataPath* `QM1` . Se si omette il parametro md , viene utilizzato il valore dell'attributo DefaultPrefix o Prefix . Prefisso ha la precedenza su DefaultPrefix.

In genere, creare QM1 specificando le directory di log e di dati in un singolo comando.

```
 crtmqm
-md DataPath -ld
LogPath QM1
```

È possibile modificare l'ubicazione di un log del gestore code e le directory dei dati di un gestore code esistente modificando gli attributi DataPath e LogPath nel file `qm.ini` quando il gestore code viene arrestato.

Il percorso della directory `errors` , come i percorsi di tutte le directory in `/var/mqm`, non è modificabile. Tuttavia, le directory possono essere montate su file system differenti o collegate simbolicamente a directory differenti.

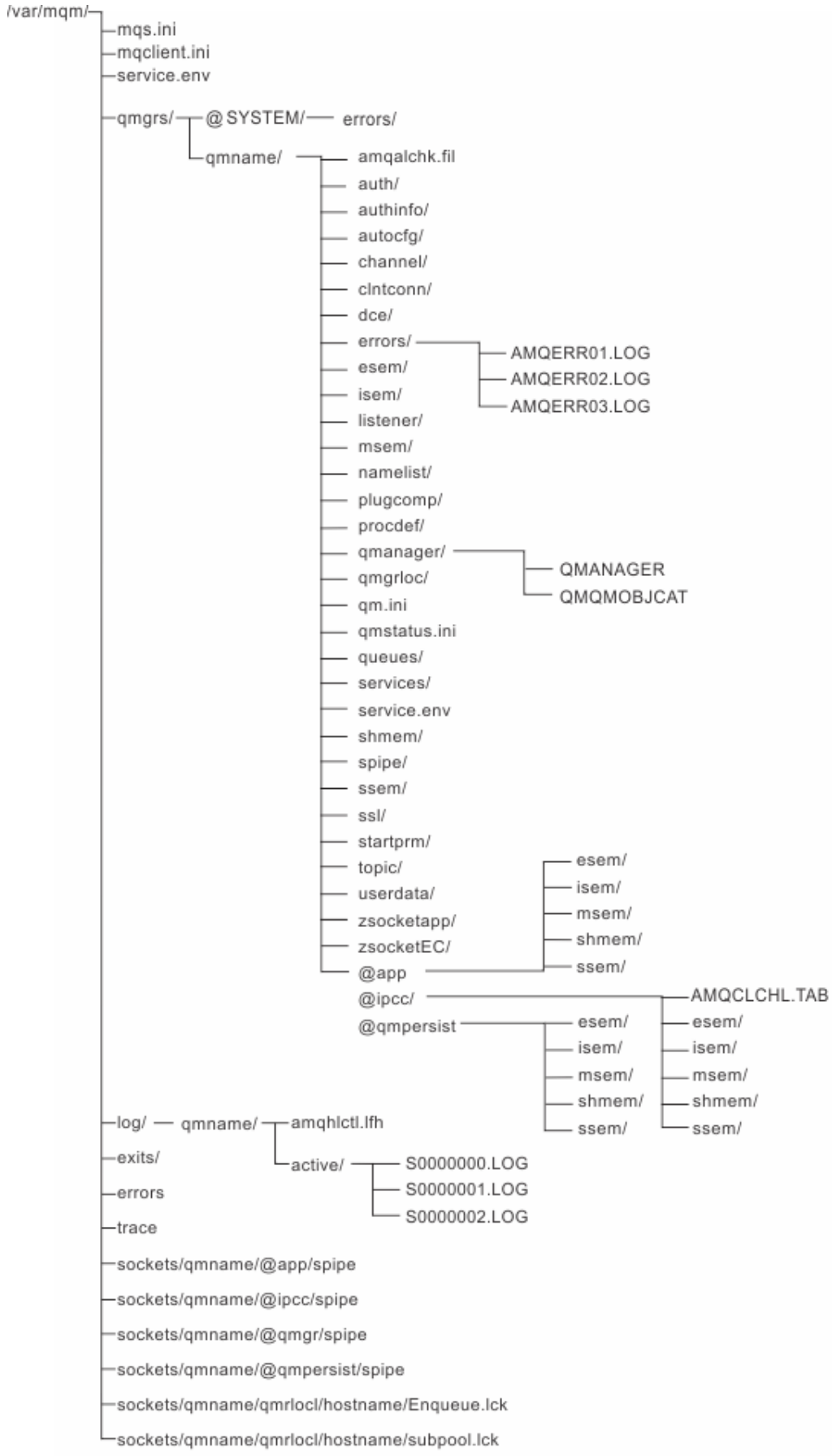
Linux AIX *Contenuto della directory su sistemi AIX and Linux*

Contenuto delle directory associate a un gestore code.

Per informazioni sul percorso dei file del prodotto, consultare Scelta di un percorso di installazione

Per informazioni sulle configurazioni di directory alternative, consultare “Pianificazione del supporto del file system su Multiplatforms” a pagina 117.

La seguente struttura di directory è rappresentativa di IBM MQ dopo che un gestore code è stato in uso per qualche tempo. La struttura effettiva dipende dalle operazioni che si sono verificate sul gestore code.


/var/mqm/
mqs.ini
mqclient.ini
service.env
qmgrs/
@SYSTEM/
errors/
qmname/
amqalchk.fil
auth/
authinfo/
autocfg/
channel/
clntconn/
dce/
errors/
AMQERR01.LOG
AMQERR02.LOG
AMQERR03.LOG
esem/
isem/
listener/
msem/
namelist/
plugcomp/
procdef/
qmanager/
QMANAGER
QMQMOBJCAT
qmgrloc/
qm.ini
qmstatus.ini
queues/
services/
service.env
shmem/
spipe/
ssem/
ssl/
startprm/
topic/
userdata/
zsocketapp/
zsocketEC/
@app
esem/
isem/
msem/
shmem/
ssem/
@ipcc/
AMQCLCHL.TAB
@qmpersist
esem/
isem/
msem/
shmem/
ssem/
esem/
isem/
msem/
shmem/
ssem/
log/
qmname/
amqhlctl.lfh
active/
S0000000.LOG
S0000001.LOG
S0000002.LOG
exits/
errors
trace
sockets/qmname/@app/spipe
sockets/qmname/@ipcc/spipe
sockets/qmname/@qmgr/spipe
sockets/qmname/@qmpersist/spipe
sockets/qmname/qmrlocl/hostname/Enqueue.lck
sockets/qmname/qmrlocl/hostname/subpool.lck

/var/mqm/

La directory /var/mqm contiene i file di configurazione e le directory di output che si applicano a un'installazione di IBM MQ nel suo complesso e non a un singolo gestore code.

Tabella 13. Contenuto documentato della directory /var/mqm su AIX and Linux	
Nome file o directory	**Indice**
mqs.ini	File di configurazione dell'installazione di IBM MQ , letto all'avvio di un gestore code. Percorso file modificabile utilizzando la variabile di ambiente **AMQ_MQS_INI_LOCATION** . Verificare che sia impostato ed esportato nella shell in cui viene eseguito il comando **strmqm** .
mqclient.ini	File di configurazione client predefinito letto dai programmi IBM MQ MQI client . Percorso file modificabile utilizzando la variabile di ambiente **MQCLNTCF** .
service.env	Contiene le variabili di ambiente dell'ambito macchina per un processo di servizio. Percorso file fisso.
errori /	Log degli errori dell'ambito macchina e file FFST . Percorso directory fisso. Consultare anche FFST: IBM MQ for UNIX e Linux systems.
socket /	Contiene informazioni per ogni gestore code solo per il sistema.
traccia /	File di traccia. Percorso directory fisso.
web /	Directory server mqweb.
uscite /	Directory predefinita contenente i programmi di uscita del canale utente. Ubicazione modificabile nelle stanze ApiExit nel file mqs.ini .
exits64/	

/var/mqm/qmgrs/*qmname*/

/var/mqm/qmgrs/*qmname*/ contiene directory e file per un gestore code. La directory è bloccata per l'accesso esclusivo dall'istanza del gestore code attivo. Il percorso della directory è direttamente modificabile nel file mqs.ini oppure utilizzando l'opzione **md** del comando **crtmqm** .

Tabella 14. Contenuto documentato della directory /var/mqm/qmgrs/qmname su AIX and Linux	
Nome file o directory	**Indice**
qm.ini	File di configurazione del gestore code, letto all'avvio del gestore code.
errori /	Log degli errori dell'ambito gestore code. *qmname* = @system contiene i messaggi relativi al canale per un gestore code sconosciuto o non disponibile.

Tabella 14. Contenuto documentato della directory /var/mqm/qmgrs/qmname su AIX and Linux (Continua)	
Nome file o directory	**Indice**
@ipcc/ AMQCLCHL.TAB	Tabella di controllo del canale client predefinita, creata dal server IBM MQ e letta dai programmi IBM MQ MQI client . Percorso file modificabile utilizzando le variabili di ambiente **MQCHLLIB** e **MQCHLTAB** .
QMANAGER	File oggetto gestore code: QMANAGER Catalogo oggetti gestore code: QMQMOBJCAT
authinfo /	Ogni oggetto definito nel gestore code è associato a un file in queste directory. Il nome del file corrisponde approssimativamente al nome della definizione; consultare Descrizione dei nomi file IBM MQ.
canale /	
clntconn /	
listener /	
elenco nomi /	
procdef /	
code /	
servizi /	
argomenti /	
...	Altre directory utilizzate da IBM MQ, come @ipcc, che devono essere modificate solo da IBM MQ.
dati utente /	Può essere utilizzato per memorizzare lo stato persistente delle applicazioni (può essere utilizzato da RDQM quando si spostano i gestori code su nodi diversi - consultare Memorizzazione dello stato dell'applicazione persistente.)
DataPath**autocfg	Utilizzato per la configurazione automatica

/var/mqm/log/*qmname*/

/var/mqm/log/*qmname*/ contiene i file di log del gestore code. La directory è bloccata per l'accesso esclusivo dall'istanza del gestore code attivo. Il percorso della directory è modificabile nel file qm.ini o utilizzando l'opzione **ld** del comando **crtmqm** .

Tabella 15. Contenuto documentato della directory /var/mqm/log/qmname su AIX and Linux	
Nome file o directory	**Indice**
amqhlctl.lfh	File di controllo log.
attivo /	Questa directory contiene i file di log con numero S0000000.LOG, S0000001.LOG, S0000002.LOGe così via.

/opt/mqm

/opt/mqm è, per impostazione predefinita, la directory di installazione sulla maggior parte delle piattaforme. Consultare “Requisiti di spazio su disco su Multiplatforms” a pagina 113 per ulteriori

informazioni sulla quantità di spazio necessario per la directory di installazione sulla piattaforma o sulle piattaforme utilizzate dall'azienda.

Linux AIX *Configurazioni di directory di esempio su sistemi AIX and Linux*

Esempi di configurazioni di file system alternativi su sistemi AIX and Linux .

È possibile personalizzare la struttura di directory IBM MQ in vari modi per raggiungere diversi obiettivi.

- Inserire le directory `qmgrs` e `log` sui file system condivisi remoti per configurare un gestore code a più istanze.
- Utilizzare file system separati per le directory di dati e di log e assegnare le directory a dischi differenti, per migliorare le prestazioni riducendo il conflitto I/O.
- Utilizzare le unità di memoria più veloci per le directory che hanno un effetto maggiore sulle prestazioni. La latenza del dispositivo fisico è spesso un fattore più importante nelle prestazioni della messaggistica persistente rispetto al fatto che un dispositivo sia montato localmente o in remoto. Il seguente elenco mostra quali directory sono più e meno sensibili alle prestazioni.
  1. `log`
  2. `qmgrs`
  3. Altre directory, incluso `/usr/mqm`
- Creare le indirizzari `qmgrs` e `log` sui file system assegnati all'archiviazione con una buona resilienza, ad esempio un disk array ridondante.
- È meglio memorizzare i log degli errori comuni in `var/mqm/errors`, localmente, piuttosto che su un file system di rete, in modo che sia possibile registrare gli errori relativi al file system di rete.

Figura 36 a pagina 134 è un modello da cui derivano strutture di directory IBM MQ alternative. Nel modello, le linee tratteggiate rappresentano percorsi configurabili. Negli esempi, le linee tratteggiate vengono sostituite da linee continue che corrispondono alle informazioni di configurazione memorizzate nella variabile di ambiente AMQ_MQS_INI_LOCATION e nei file `mqs.ini` e `qm.ini` .

Nota: Le informazioni sul percorso vengono mostrate come appaiono nei file `mqs.ini` o `qm.ini` . Se si forniscono parametri di percorso nel comando **`crtmqm`** , omettere il nome della directory del gestore code: il nome del gestore code viene aggiunto al percorso da IBM MQ.

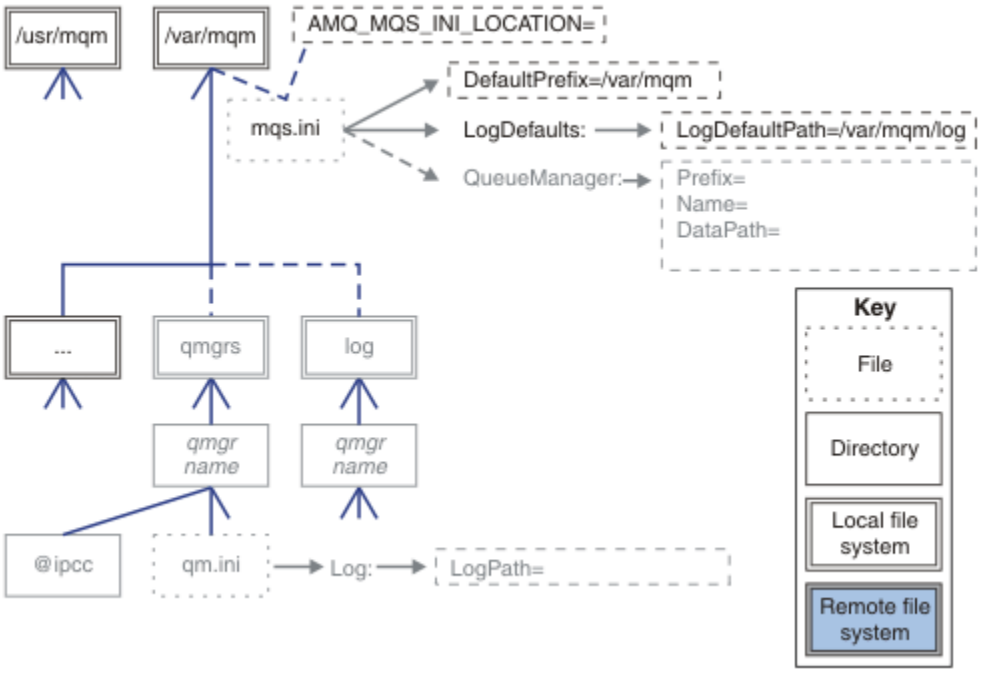


Figura 36. Modello di modello struttura di directory

Struttura di directory tipica per IBM MQ

Figura 37 a pagina 135 è la struttura di directory predefinita creata in IBM MQ con il comando **crtmqm** *QM1*.

Il file `mqs.ini` ha una stanza per il gestore code QM1 , creato facendo riferimento al valore di `DefaultPrefix`. La stanza `Log` nel file `qm.ini` ha un valore per `LogPath`, impostato mediante riferimento a `LogDefaultPath` in `mqs.ini`.

Utilizzare i parametri facoltativi di **crtmqm** per sovrascrivere i valori predefiniti di `DataPath` e `LogPath`.

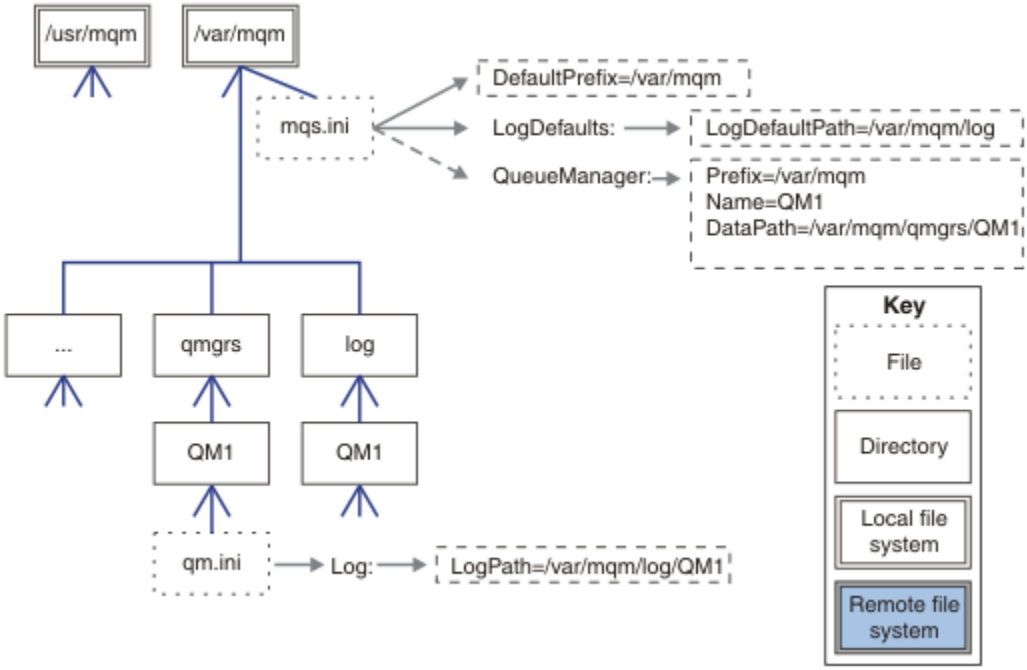


Figura 37. Struttura di directory IBM MQ predefinita di esempio per sistemi AIX and Linux

Condividi directory `qmgrs` e `log` predefinite

Un'alternativa a “Condividi tutto” a pagina 137è quella di condividere separatamente le directory `qmgrs` e `log` (Figura 38 a pagina 136). In questa configurazione, non è necessario impostare `AMQ_MQS_INI_LOCATION` poiché il file mqs.ini predefinito è memorizzato nel file system `/var/mqm` locale. I file e le directory, come `mqclient.ini` e `mqserver.ini` , non vengono condivisi.

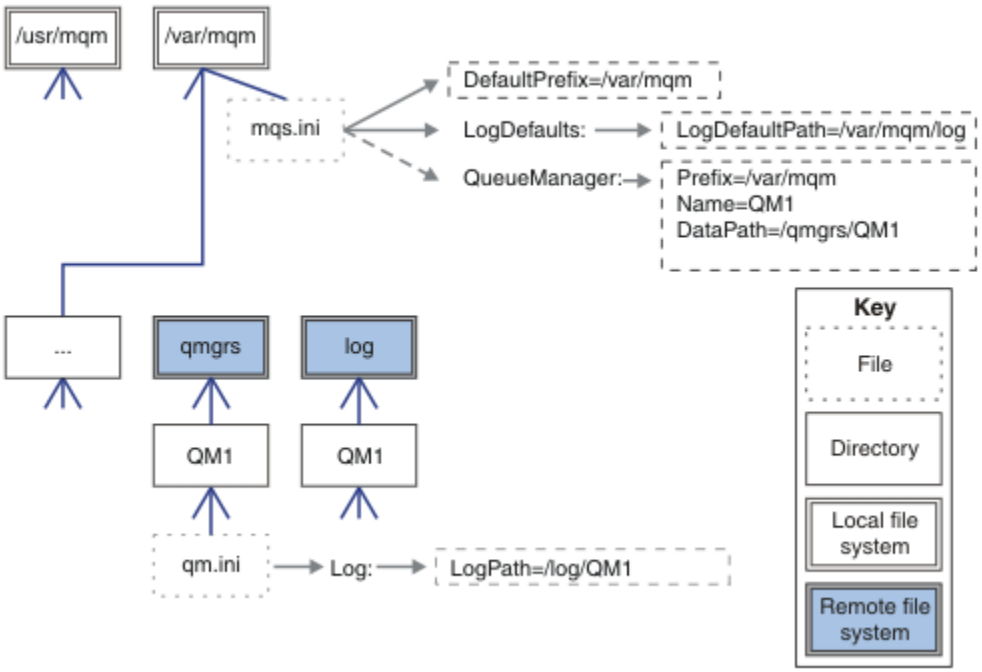


Figura 38. Condividi directory qmgrs e log

Condividere le directory denominate qmgrs e log

La configurazione in Figura 39 a pagina 136 colloca `log` e `qmgrs` in un file system condiviso remoto denominato `/ha`. La stessa configurazione fisica può essere creata in due modi diversi.

1. Impostare `LogDefaultPath=/ha` ed eseguire il comando **crtmqm** - md */ha/qmgrs* QM1. Il risultato è esattamente come illustrato in Figura 39 a pagina 136.
2. Lasciare invariati i percorsi predefiniti ed eseguire il comando, **crtmqm** - ld */ha/log* - md */ha/qmgrs* QM1.

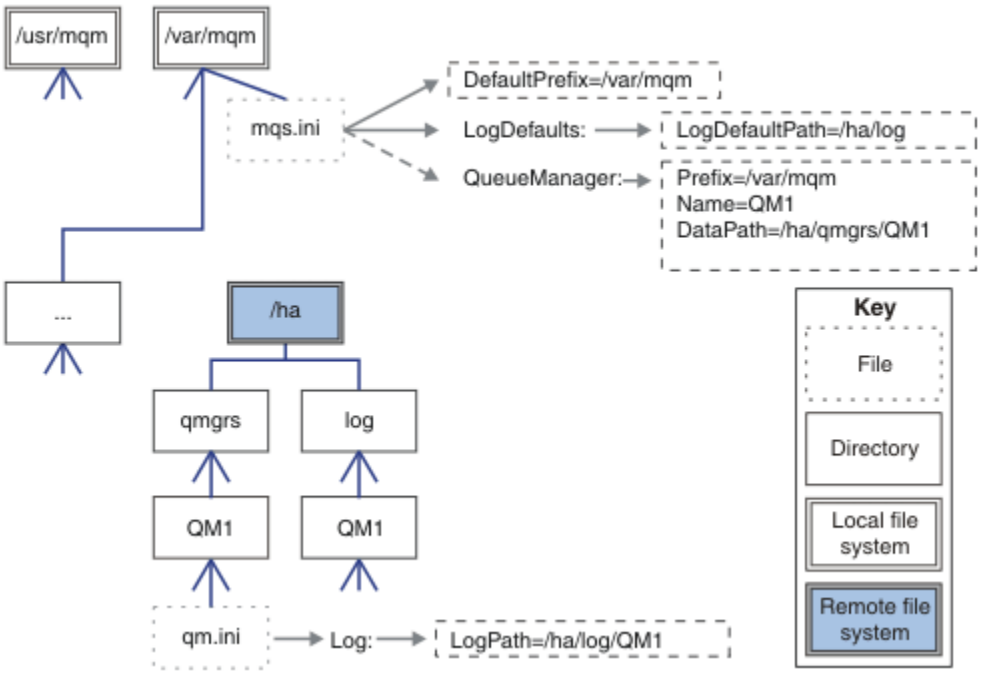


Figura 39. Condividere le directory denominate qmgrs e log

Condividi tutto

Figura 40 a pagina 137 è una configurazione semplice per il sistema con archiviazione file di rete veloce.

Montare `/var/mqm` come file system condiviso remoto. Per impostazione predefinita, quando si avvia QM1, cerca `/var/mqm`, lo trova sul file system condiviso e legge il file `mqs.ini` in `/var/mqm`. Invece di utilizzare il file `/var/mqm/mqs.ini` singolo per i gestori code su tutti i server, è possibile impostare la variabile di ambiente `AMQ_MQS_INI_LOCATION` su ciascun server in modo che punti a file `mqs.ini` diversi.

Nota: Il contenuto del file di errori generico in `/var/mqm/errors/` viene condiviso tra gestori code su server differenti.

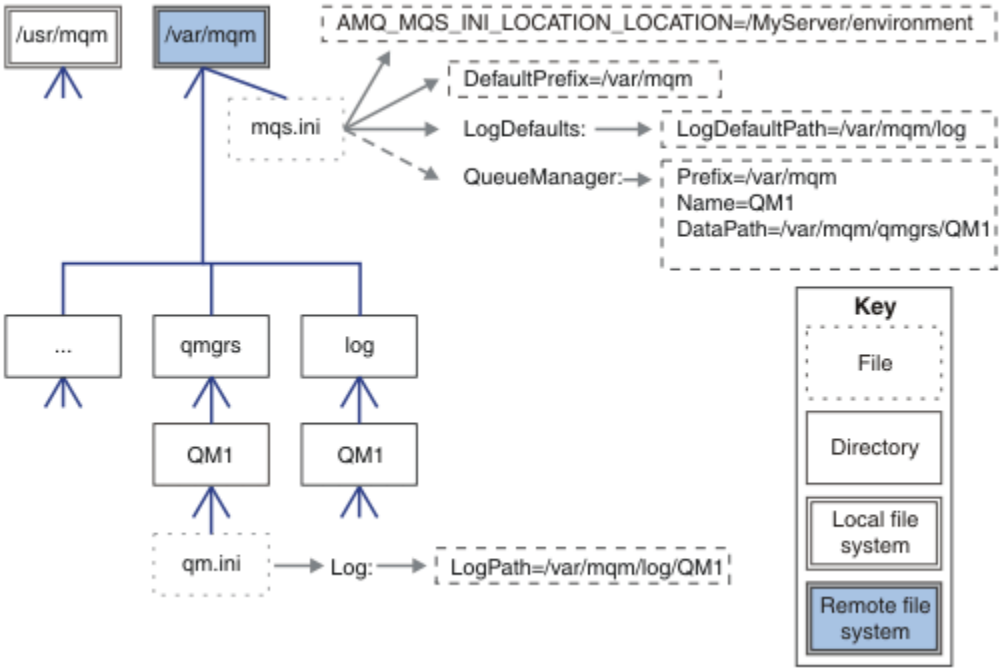


Figura 40. Condividi tutto

Notare che non è possibile utilizzarlo per i gestori code a più istanze. Il motivo è che è necessario che ogni host in un gestore code a più istanze disponga di una propria copia locale di `/var/mqm` per tenere traccia dei dati locali, come i semafori e la memoria condivisa. Queste entità non possono essere condivise tra host.

Windows Struttura di directory su sistemi Windows .

Come trovare le informazioni di configurazione del gestore code e le directory su Windows.

Le directory predefinite per l'installazione di IBM MQ for Windows sono:

Directory programma

```
C:\Program Files\IBM\MQ
```

Directory di dati

```
C:\Programmi\ IBM \ MQ
```

Importante: Windows Per le installazioni Windows, le directory sono come indicate, a meno che non vi sia un'installazione precedente del prodotto che contiene ancora delle voci di registro e/o gestori code. In questa situazione, la nuova installazione utilizza il vecchio percorso di directory dei dati. Per ulteriori informazioni, consultare Program and data directory locations.

Se si desidera conoscere la directory di installazione e la directory di dati utilizzata, eseguire il comando dspmqver .

la directory di installazione è elencata nel campo **InstPath** e la directory di dati è elencata nel campo **DataPath** .

L'esecuzione del comando **dspmqver** visualizza, ad esempio, le seguenti informazioni:

```
>dspmqver
Name:        IBM MQ
Version:     9.0.0.0
Level:       p900-L160512.4
BuildType:   IKAP - (Production)
Platform:    IBM MQ for Windows (x64 platform)
Mode:        64-bit
O/S:         Windows 7 Professional x64 Edition, Build 7601: SP1
InstName:    Installation1
InstDesc:
Primary:     Yes
InstPath:    C:\Program Files\IBM\MQ
DataPath:    C:\ProgramData\IBM\MQ
MaxCmdLevel: 900
LicenseType: Production
```

Gestori code a più istanze

Per configurare un gestore code a più istanze, le directory di log e di dati devono essere collocate nella memoria di rete, preferibilmente su un server diverso rispetto a uno qualsiasi dei server che eseguono le istanze del gestore code.

Due parametri vengono forniti nel comando **crtmqm** , **-md** e **-ld**, per rendere più semplice specificare l'ubicazione dei dati del gestore code e le directory di log. L'effetto della specifica del parametro **-md** è quadruplicato:

1. La stanza `mqs.ini` `QueueManager\`*`QmgrName`* contiene una nuova variabile, *DataPath*, che punta alla directory dei dati del gestore code. A differenza della variabile *Prefisso* , il percorso include il nome della directory del gestore code.
2. Le informazioni di configurazione del gestore code memorizzate nel file mqs.ini sono ridotte a *Nome*, *Prefisso*, *Directory* e *DataPath*.

Windows *Contenuto della directory*

Elenca l'ubicazione e il contenuto delle directory IBM MQ .

Una configurazione IBM MQ ha tre serie principali di file e directory:

1. Eseguibile e altri file di sola lettura che vengono aggiornati solo quando viene applicata la manutenzione. Ad esempio:
   - Il file readme
   - Il plug-in di IBM MQ Explorer e i file della guida
   - File di licenza

   Questi file sono descritti in Tabella 16 a pagina 139.
2. File e directory potenzialmente modificabili che non sono specifici di un particolare gestore code. Questi file e directory sono descritti in Tabella 17 a pagina 139.
3. File e directory specifici di ciascun gestore code su un server. Questi file e directory sono descritti in Tabella 18 a pagina 140.

File e directory di risorse

Le directory di risorse e i file contengono tutto il codice eseguibile e le risorse per eseguire un gestore code. La variabile *FilePath*, nella chiave di registro di configurazione IBM MQ specifica dell'installazione, contiene il percorso delle directory delle risorse.

Tabella 16. Directory e file nella directory FilePath	
Percorso file	**Indice**
FilePath\bin	Comandi e DLL
FilePath\bin64	Comandi e DLL (64 bit)
FilePath\conv	Tabelle conversione dati
FilePath\doc	File della guida della procedura guidata
FilePath\MQExplorer	Plug-in Eclipse della guida di Explorer ed Explorer
FilePath\gskit8	GSK (Global Security Kit)
FilePath\java	Risorse Java , incluso JRE
FilePath\licenses	Informazioni sulla licenza
FilePath\Non_IBM_License	Informazioni sulla licenza
FilePath\properties	Utilizzato internamente
FilePath\Tivoli	
FilePath\tools	Esempi e risorse di sviluppo
FilePath\web	Descritto nella struttura del file del componente di installazione IBM MQ Console e REST API per i file non modificabili.
FilePath\Uninst	Utilizzato internamente
FilePath\README.TXT	File readme

Directory non specifiche per un gestore code

Alcune directory contengono file, ad esempio file di traccia e log degli errori, che non sono specifici di un determinato gestore code. La variabile *DefaultPrefix* contiene il percorso di queste directory. *DefaultPrefix* fa parte della stanza AllQueueManagers .

Tabella 17. Directory e file nella directory DefaultPrefix	
Percorso file	**Indice**
DefaultPrefix\config	Utilizzato internamente
DefaultPrefix\conv	File di controllo conversione ccsid_part2.tbl e ccsid.tbl data , descritto in Conversione dati
DefaultPrefix\errors	Log degli errori non relativi al gestore code, AMQERR *nn*.LOG
DefaultPrefix\exits	Programmi di uscita canale
DefaultPrefix\exits64	Programmi di uscita canale (64 bit)
DefaultPrefix\ipc	Non utilizzato
DefaultPrefix\qmgrs	Descritto in Tabella 18 a pagina 140
DefaultPrefix\trace	File di traccia
DefaultPrefix\web	Descritto nella struttura del file del componente di installazione IBM MQ Console e REST API per i file modificabili dall'utente
DefaultPrefix\amqmjpse.txt	Utilizzato internamente

Directory del gestore code

Quando si crea un gestore code, viene creata una nuova serie di directory, specifiche del gestore code.

Se si crea un gestore code con il parametro **-md** *filepath* , il percorso viene memorizzato nella variabile *DataPath* nella stanza del gestore code del file mqs.ini . Se si crea un gestore code senza impostare il parametro **-md** *filepath* , le directory del gestore code vengono create nel percorso memorizzato in *DefaultPrefix*, e il percorso viene copiato nella variabile *Prefisso* nella stanza del gestore code del file mqs.ini .

Tabella 18. Directory e file nelle directory DataPath e Prefix\qmgrs\QmgrName

Percorso file	**Indice**
DataPath\@ipcc	Ubicazione predefinita per AMQCLCHL.TAB, la tabella di connessione client.
DataPath\authinfo	Utilizzato internamente.
DataPath\channel	
DataPath\clntconn	
DataPath\errors	Log degli errori, AMQERR *nn*.LOG
DataPath\listener	Utilizzato internamente.
DataPath\namelist	
DataPath\plugcomp	
DataPath\procdef	
DataPath\qmanager	
DataPath\queues	
DataPath\services	
DataPath\ssl	
DataPath\startprm	
DataPath\topic	
DataPath\active	
DataPath\active.dat	
DataPath\amqalchk.fil	
DataPath\master	
DataPath\master.dat	
DataPath\qm.ini	Configurazione del gestore code
DataPath\qmstatus.ini	Stato gestore code
DataPath\userdata	Può essere utilizzato per memorizzare lo stato persistente delle applicazioni.
Prefix\qmgrs*QmgrName*	Utilizzato internamente
Prefix\qmgrs\@SYSTEM	Non utilizzato
Prefix\qmgrs\@SYSTEM\errors	
*DataPath**autocfg*	Utilizzato per la configurazione automatica

IBM i Struttura di directory su IBM i

Viene fornita una descrizione di IFS e la struttura di directory di IBM MQ IFS viene descritta per server, client e Java.

IFS (integrated file system) è una parte di IBM i che supporta la gestione dell'input/output e della memoria del flusso simile al personal computer, ai sistemi operativi AIX and Linux , fornendo una struttura di integrazione su tutte le informazioni memorizzate nel server.

In IBM i i nomi di directory iniziano con il carattere `& (ampersand)` anziché con il carattere `@ (at)`. Ad esempio, `@system` su IBM i è `&system`.

File system root IFS per server IBM MQ

Quando si installa il server IBM MQ per IBM i, le seguenti directory vengono create nel filesystem root IFS.

ProdData:

Panoramica

```
QIBM
   '-- ProdData
      '-- mqm
      '-- doc
      '-- inc
      '-- lib
      '-- samp
      '-- licenses
      '-- LicenseDoc
      '-- 5724H72_V8R0M0
```

/QIBM/ProdData/mqm
Le sottodirectory sottostanti contengono tutti i dati del prodotto, ad esempio le classi C + +, i file di formato traccia e i file di licenza. I dati in questa directory vengono eliminati e sostituiti ogni volta che il prodotto viene installato.

/QIBM/ProdData/mqm/doc
Un riferimento al comando per i comandi CL viene fornito in formato HTML e installato qui.

/QIBM/ProdData/mqm/inc
I file di intestazione per la compilazione dei programmi C o C + +.

/QIBM/ProdData/mqm/lib
File ausiliari utilizzati da MQ.

/QIBM/ProdData/mqm/samp
Ulteriori campioni.

/QIBM/ProdData/mqm/licenses
File di licenza. I due file per ciascuna lingua sono denominati come `LA_` *xx* e `LI_` *xx* , dove *xx* è l'identificativo della lingua di 2 caratteri per ciascuna lingua fornita.

Inoltre, la seguente directory memorizza i file degli accordi di licenza:

/QIBM/ProdData/LicenseDoc/5724H72_V8R0M0
File di licenza. I file sono denominati come `5724H72_V8R0M0_` *xx* dove *xx* è l'identificativo della lingua di 2 o 5 caratteri per ogni lingua fornita.

UserData:

Panoramica

```
QIBM
   '-- UserData
      '-- mqm
```

```
        '-- errors
        '-- trace
        '-- qmgrs
        '-- &system
        '-- qmgrname1
        '-- qmgrname2
        '-- and so on
```

/QIBM/UserData/mqm
Le sottodirectory sottostanti contengono tutti i dati utente relativi ai gestori code.

Quando si installa il prodotto, viene creato un file mqs.ini nella directory /QIBM/UserData/mqm/ (a meno che non sia già presente da un'installazione precedente).

Quando si crea un gestore di code, viene creato un file qm.ini nella directory /QIBM/UserData/mqm/qmgrs/ *QMGRNAME* / (dove *QMGRNAME* è il nome del gestore di code).

I dati nelle directory vengono conservati quando il prodotto viene eliminato.

File system root IFS per IBM MQ MQI client

Quando si installa IBM MQ MQI client for IBM i, le seguenti directory vengono create nel file system root IFS:

ProdData:

Panoramica

```
QIBM
   '-- ProdData
      '-- mqm
      '-- lib
```

/QIBM/ProdData/mqm
Le sottodirectory al di sotto di questa directory contengono tutti i dati del prodotto. I dati in questa directory vengono eliminati e sostituiti ogni volta che il prodotto viene sostituito.

UserData:

Panoramica

```
QIBM
   '-- UserData
      '-- mqm
      '-- errors
      '-- trace
```

/QIBM/UserData/mqm
Le sottodirectory al di sotto di questa directory contengono tutti i dati utente.

File system root IFS per IBM MQ Java

Quando si installa IBM MQ Java su IBM i, le seguenti directory vengono create nel file system root IFS:

ProdData:

Panoramica

```
QIBM
   '-- ProdData
      '-- mqm
      '-- java
```

```
        '--samples
        '-- bin
        '-- lib
```

/QIBM/ProdData/mqm/java
Le sottodirectory sottostanti contengono tutti i dati del prodotto, incluse le classi Java . I dati in questa directory vengono eliminati e sostituiti ogni volta che il prodotto viene sostituito.

/QIBM/ProdData/mqm/java/samples
Le sottodirectory sottostanti contengono tutti i dati e le classi Java di esempio.

Librerie create dalle installazioni server e client

L'installazione del server o del client IBM MQ crea le librerie riportate di seguito:

- QMQM

  La libreria del prodotto.

- QMQMSAMP

  La libreria degli esempi (se si sceglie di installare gli esempi).

- QMxxxx

  Solo server.

  Ogni volta che si crea un gestore code, IBM MQ crea automaticamente una libreria associata, con un nome come QMxxxx dove xxxx deriva dal nome del gestore code. Questa libreria contiene oggetti specifici del gestore code, inclusi i giornali e i ricevitori associati. Per impostazione predefinita, il nome di questa libreria deriva dal nome del gestore code con prefisso QM. Ad esempio, per un gestore code denominato TEST, la libreria viene denominata QMTEST.

  Nota: Quando si crea un gestore code, è possibile specificare il nome della relativa libreria. Ad esempio:

  ```
  CRTMQM MQMNAME(TEST) MQMLIB(TESTLIB)
  ```

  È possibile utilizzare il comando WRKLIB per elencare tutte le librerie create da IBM MQ per IBM i . Rispetto alle librerie del gestore code, verrà visualizzato QMGR: QMGRNAME. Il formato del comando è:

  ```
  WRKLIB LIB(QM*)
  ```

  Queste librerie associate al gestore code vengono conservate quando il prodotto viene eliminato.

Multi Pianificazione del supporto file system per MFT su Multiplatforms

Gli agent IBM MQ Managed File Transfer MFT possono essere utilizzati per trasferire i dati da e verso i file su un filesystem. Inoltre, i monitoraggi delle risorse in esecuzione all'interno di un agent possono essere configurati per monitorare i file su un file system.

MFT richiede che questi file siano memorizzati su un filesystem che supporta il blocco. Ci sono due ragioni per questo:

- Un agent blocca un file per assicurarsi che non venga modificato una volta che ha iniziato la lettura dei dati da esso o la scrittura dei dati su di esso.
- I monitoraggi delle risorse bloccano i file per controllare che nessun altro processo li stia attualmente utilizzando.

Gli agent e i monitoraggi delle risorse utilizzano il Java metodo **`FileChannel.tryLock()`** per eseguire il blocco e il file system deve essere in grado di bloccare i file quando richiesto utilizzando questa chiamata.

Importante: I seguenti file system non sono supportati poiché non soddisfano i requisiti tecnici di MFT:

- GlusterFS
- NFS versione 3

Multi Scelta della registrazione circolare o lineare su Multiplatforms

In 'IBM MQ è possibile scegliere una registrazione circolare o lineare per i registri di ripristino. Le seguenti informazioni forniscono una panoramica di entrambi i tipi.

Vedere Registrazione: Assicurarsi che i messaggi non vadano persi per ulteriori informazioni sulla registrazione del ripristino. IBM MQ utilizza il checkpointing per limitare il volume di replay dei registri necessario dopo un ripristino da arresto anomalo. L'evento chiave che controlla se un file di log è definito attivo o meno è un " `checkpoint`. Per ulteriori informazioni sulle transazioni e sul checkpoint, vedere Uso del checkpoint per garantire un ripristino completo.

Vantaggi della registrazione circolare

I principali vantaggi della registrazione circolare sono:

- Più facile da amministrare.

  Una volta configurata correttamente la registrazione circolare per il carico di lavoro, non è necessaria alcuna ulteriore gestione. Mentre, per la registrazione lineare, le immagini dei supporti devono essere registrate e le estensioni di log che non sono più richieste devono essere archiviate o eliminate.
- Prestazioni migliori

  La registrazione circolare funziona meglio della registrazione lineare, perché la registrazione circolare è in grado di riutilizzare le estensioni di log che sono già state formattate. Mentre la registrazione lineare deve allocare nuove estensioni log e formattarle.

Per ulteriori informazioni, vedi Gestione dei log .

Vantaggi della registrazione lineare

Il vantaggio principale della registrazione lineare è che la registrazione lineare fornisce protezione contro ulteriori errori.

Né la registrazione circolare né la registrazione lineare proteggono da un log danneggiato o eliminato, o da messaggi o code che sono stati eliminati dalle applicazioni o dall'amministratore.

La registrazione lineare (ma non circolare) consente il recupero degli oggetti danneggiati. Quindi, la registrazione lineare fornisce protezione contro i file delle code danneggiati o eliminati, poiché queste code danneggiate possono essere recuperate da un log lineare. È possibile configurare l'imaging automatico dei supporti e la gestione automatica dei registri per i registri lineari per ridurre i costi di gestione. Vedere Imaging automatico dei supporti e Gestione automatica dei registri.

Protezione circolare e lineare contro la perdita di alimentazione e gli errori di comunicazione come descritto in Ripristino da perdita di alimentazione o errori di comunicazione.

Altre considerazioni

La scelta tra lineare o circolare dipende dalla ridondanza richiesta.

Vi è un costo per la scelta di una maggiore ridondanza, ossia la registrazione lineare, causato dal costo delle prestazioni e dal costo di gestione.

Per ulteriori informazioni, vedi Tipi di registrazione .

AIX Memoria condivisa su AIX

Se alcuni tipi di applicazione non riescono a connettersi a causa di una limitazione della memoria AIX , nella maggior parte dei casi questo problema può essere risolto impostando la variabile di ambiente EXTSHM=ON.

Alcuni processi a 32 bit su AIX potrebbero incontrare una limitazione del sistema operativo che influisce sulla loro capacità di connettersi ai gestori code IBM MQ . Ogni connessione standard a IBM MQ utilizza

la memoria condivisa, ma a differenza di altre piattaforme UNIX , AIX consente ai processi a 32 bit di collegare solo 11 serie di memoria condivisa.

La maggior parte dei processi a 32 bit non incontrerà questo limite, ma le applicazioni con requisiti di memoria elevati potrebbero non riuscire a collegarsi a IBM MQ con codice di errore 2102: MQRC_RESOURCE_PROBLEM. I seguenti tipi di applicazione potrebbero visualizzare questo errore:

- Programmi in esecuzione in macchine virtuali Java a 32 bit
- Programmi che utilizzano modelli di memoria grandi o molto grandi
- Programmi che si collegano a molti gestori code o database
- Programmi che si collegano a serie di memoria condivisa da soli

AIX offre una funzione di memoria condivisa estesa per i processi a 32 bit che consente loro di collegare più memoria condivisa. Per eseguire un'applicazione con questa funzione, esportare la variabile di ambiente EXTSHM=ON prima di avviare i gestori code e il programma. La funzione EXTSHM=ON previene questo errore nella maggior parte dei casi, ma è incompatibile con i programmi che utilizzano l'opzione SHM_SIZE della funzione shmctl.

Le applicazioni IBM MQ MQI client e tutti i processi a 64 - bit non sono interessati da questa limitazione. Possono connettersi ai gestori code IBM MQ indipendentemente dal fatto che EXTSHM sia stato impostato o meno.

Linux AIX Risorse IPC IBM MQ e UNIX System V

Un gestore code utilizza alcune risorse IPC. Utilizzare **ipcs -a** per individuare le risorse utilizzate.

Queste informazioni si applicano solo a sistemi IBM MQ in esecuzione su AIX and Linux

IBM MQ utilizza risorse IPC (interprocess communication) System V (*semafori* e *segmenti di memoria condivisi*) per memorizzare e trasmettere i dati tra i componenti del sistema. Queste risorse sono utilizzate dai processi del gestore code e dalle applicazioni che si connettono al gestore code. IBM MQ MQI clients non utilizzano le risorse IPC, ad eccezione del controllo di traccia IBM MQ . Utilizzare il UNIX comando **ipcs -a** per ottenere informazioni complete sul numero e la dimensione delle risorse IPC attualmente in uso sulla macchina.

Linux AIX Priorità processo IBM MQ e UNIX

Buone pratiche durante l'impostazione dei valori *nice* della priorità del processo.

Queste informazioni si applicano solo a sistemi IBM MQ in esecuzione su AIX and Linux

Se si esegue un processo in background, a tale processo può essere assegnato un valore *nice* superiore (e quindi una priorità inferiore) dalla shell di richiamo. Ciò potrebbe avere implicazioni generali sulle prestazioni di IBM MQ . In situazioni di stress elevato, se ci sono molti thread pronti per l'esecuzione con una priorità più alta e alcuni con una priorità più bassa, le caratteristiche di pianificazione del sistema operativo possono privare i thread con priorità più bassa del tempo del processore.

È buona norma che i processi avviati in modo indipendente associati ai gestori code, come ad esempio **runmqlsr**, abbiano gli stessi valori *nice* del gestore code a cui sono associati. Assicurarsi che la shell non assegni un valore *nice* superiore a questi processi in background. Ad esempio, in ksh, utilizzare l'impostazione "`set +o bgnice`" per impedire a ksh di aumentare il valore *nice* dei processi in background. È possibile verificare i valori *nice* dei processi in esecuzione esaminando la colonna *NI* di un elenco "ps -efl" .

Inoltre, avviare i processi dell'applicazione IBM MQ con lo stesso valore *nice* del gestore code. Se vengono eseguiti con valori *nice* differenti, un thread dell'applicazione potrebbe bloccare un thread del gestore code o viceversa, causando un peggioramento delle prestazioni.

z/OS Pianificazione dell'ambiente IBM MQ su z/OS

Quando si pianifica l'ambiente IBM MQ , è necessario considerare i requisiti delle risorse per i dataset, i set di pagine, Db2, le CF (Coupling Facility) e la necessità di funzioni di registrazione e backup. Utilizzare questo argomento per pianificare l'ambiente in cui viene eseguito IBM MQ .

Prima di pianificare la tua architettura IBM MQ , familiarizza con i concetti IBM MQ for z/OS di base, consulta gli argomenti in Concetti diIBM MQ for z/OS.

Quando si pianifica il gestore code, potrebbe essere necessario lavorare con persone diverse nella propria organizzazione. Di solito è una buona idea coinvolgere queste persone in anticipo, in quanto le procedure di controllo del cambiamento possono richiedere molto tempo. Potrebbero anche essere in grado di indicare quali parametri sono necessari per configurare IBM MQ for z/OS.

Ad esempio, potrebbe essere necessario utilizzare:

- Amministratore della memoria, per determinare il qualificatore di alto livello dei dataset del gestore code e per allocare spazio sufficiente per i dataset del gestore code.
- Il programmatore di sistema z/OS per definire il sottosistema IBM MQ per z/OS e l'autorizzazione APF per le librerie IBM MQ for z/OS .
- Amministratore di rete per determinare quali porte e stack TCP/IP devono essere utilizzati per IBM MQ for z/OS.
- Amministratore della sicurezza per impostare l'accesso ai data set del gestore code, ai profili di sicurezza per le risorse IBM MQ for z/OS e ai certificati TLS.
- Db2 per impostare le tabelle Db2 durante la configurazione di un gruppo di condivisione code.

Concetti correlati

IBM MQ - Sommario tecnico

Attività correlate

“Pianificazione di un'architettura IBM MQ” a pagina 5

Quando si pianifica l'ambiente IBM MQ , considerare il supporto fornito da IBM MQ per le architetture di gestori code singoli e multipli e per gli stili di messaggistica point-to-point e di pubblicazione / sottoscrizione. Inoltre, pianificare i requisiti delle risorse e l'utilizzo delle funzioni di registrazione e backup.

Configurazione di z/OS

AmministrazioneIBM MQ for z/OS

z/OS Pianificazione per il gestore code

Quando si configura un gestore code, la pianificazione deve consentire la crescita del gestore code, in modo che il gestore code soddisfi le esigenze dell'azienda.

Il modo migliore per configurare un gestore code è il seguente:

1. Configurare il gestore code di base
2. Configurare l'iniziatore di canali che esegue le comunicazioni tra il gestore code e il gestore code e le comunicazioni dell'applicazione client remota
3. Se si desidera crittografare e proteggere i messaggi, configurare Advanced Message Security
4. Se si desidera utilizzare il trasferimento file su IBM MQ, configurare Managed File Transfer per z/OS.
5. Se si desidera utilizzare il REST APIdi gestione o di messaggistica o il IBM MQ Console per gestire IBM MQ da un browser Web, configurare il server mqweb.

Alcune aziende hanno centinaia di migliaia di gestori code nel proprio ambiente. Devi considerare la tua rete IBM MQ ora e tra cinque anni.

Su z/OS, alcuni gestori code elaborano migliaia di messaggi al secondo e registrano più di 100 MB al secondo. Se si prevedono volumi molto elevati, potrebbe essere necessario considerare la possibilità di avere più di un gestore code.

Su z/OS, IBM MQ può essere eseguito come parte di un gruppo di condivisione code (QSG) in cui i messaggi sono memorizzati nella CF (Coupling Facility) e qualsiasi gestore code nel gruppo di condivisione code può accedere ai messaggi. Se si desidera eseguire in un gruppo di condivisione code, è necessario considerare quanti gestori code sono necessari. Generalmente, esiste un gestore code per ogni LPAR. È anche possibile disporre di un gestore code per eseguire regolarmente il backup delle strutture CF.

Alcune modifiche alla configurazione sono facili da eseguire, come la definizione di una nuova coda. Alcune sono più difficili, ad esempio rendere i log e le serie di pagine più grandi e alcune configurazioni non possono essere modificate, ad esempio il nome di un gestore code o il nome del gruppo di condivisione code.

Sono disponibili informazioni sulle prestazioni e sull'ottimizzazione in MP16 performance SupportPac .

Convenzioni di denominazione

È necessario disporre di una convenzione di denominazione per i dataset del gestore code.

Molte aziende utilizzano il numero di release nel nome delle librerie di caricamento e così via. Si potrebbe voler considerare di avere un alias di `MQM.SCSQAUTH` che punti alla versione attualmente in uso, come `MQM.V930.SCSQAUTH`, quindi non è necessario modificare CICS, Batch e IMS JCL quando si esegue la migrazione a una nuova versione di IBM MQ.

È possibile utilizzare un collegamento simbolico in z/OS UNIX System Services per fare riferimento alla directory di installazione per la versione di IBM MQ attualmente in uso.

I dataset utilizzati dal gestore code (log, set di pagine, librerie JCL) richiedono una convenzione di denominazione per semplificare la creazione dei profili di sicurezza e l'associazione dei dataset alle classi di memoria SMS che controllano dove i dataset vengono posizionati sul disco e gli attributi di cui dispongono.

Si noti che l'inserimento della versione di IBM MQ nel nome delle serie di pagine o dei log non è una buona idea. Un giorno è possibile migrare a una nuova versione e il dataset avrà i nomi "errati".

Applicazioni

È necessario comprendere le applicazioni aziendali e il modo migliore per configurare IBM MQ. Ad esempio, se le applicazioni hanno la logica per fornire funzionalità di ripristino e ripetizione, i messaggi non persistenti potrebbero essere sufficienti. Se si desidera che IBM MQ gestisca il ripristino, è necessario utilizzare i messaggi persistenti e inserire e richiamare i messaggi nel punto di sincronizzazione.

È necessario isolare le code da diverse transazioni aziendali. Se una coda per un'applicazione aziendale si riempie, non si desidera che influisca su altre applicazioni aziendali. Isolare le code in diverse serie di pagine e pool di buffer o strutture, se possibile.

È necessario comprendere il profilo dei messaggi. Per molte applicazioni, le code contengono solo pochi messaggi. Altre applicazioni possono avere code accumulate durante il giorno e possono essere elaborate durante la notte. Una coda che normalmente contiene solo pochi messaggi, potrebbe dover contenere più ore di messaggi se si verifica un problema e i messaggi non vengono elaborati. È necessario dimensionare le strutture CF e le serie di pagine per consentire la capacità di picco prevista.

Post - configurazione

Una volta configurato il gestore code (e i componenti), è necessario pianificare:

- Backup delle serie di pagine.
- Backup delle definizioni degli oggetti.
- Automazione del backup di qualsiasi struttura CF.
- Monitoraggio dei messaggi IBM MQ ed esecuzione di azioni quando viene rilevato un problema.
- Raccolta dei dati statistici di IBM MQ .

- Monitoraggio dell'utilizzo delle risorse, come la memoria virtuale e la quantità di dati registrati all'ora. In questo modo è possibile verificare se l'utilizzo delle risorse è in aumento e se è necessario intraprendere azioni, ad esempio l'impostazione di un nuovo gestore code

z/OS Pianificazione dei requisiti di archiviazione e delle prestazioni su z/OS

È necessario impostare un archivio realistico e raggiungibile e obiettivi di prestazioni per il proprio sistema IBM MQ . Utilizzare questo argomento per comprendere i fattori che influiscono sull'archiviazione e sulle prestazioni.

Questo argomento contiene informazioni sui requisiti di archiviazione e prestazioni per IBM MQ for z/OS. Sono disponibili le seguenti sezioni:

- z/OS opzioni di prestazioni per IBM MQ
- Determinazione z/OS dell'importanza e della velocità della gestione del carico di lavoro
- “Memoria libreria” a pagina 149
- “Utilizzo LX di sistema” a pagina 149
- “Configurazione dello spazio di archiviazione” a pagina 150
- “Storage su disco” a pagina 155

Consultare “Dove trovare ulteriori informazioni sui requisiti di archiviazione e prestazioni” a pagina 156 per ulteriori informazioni.

z/OS opzioni di prestazioni per IBM MQ

Con la gestione del carico di lavoro, è possibile definire obiettivi di prestazioni e assegnare un'importanza di business a ciascun obiettivo. L'utente definisce gli obiettivi per il lavoro in termini di business e il sistema decide la quantità di risorse, ad esempio processore e memoria, che devono essere fornite al lavoro per raggiungere il suo obiettivo. La gestione del carico di lavoro controlla la priorità di distribuzione in base agli obiettivi forniti. La gestione del carico di lavoro aumenta o riduce la priorità in base alle necessità per raggiungere l'obiettivo specificato. Pertanto, non è necessario regolare le priorità esatte di ogni lavoro nel sistema e può concentrarsi invece sugli obiettivi di business.

I tre tipi di obiettivi sono:

Tempo di risposta
Quanto velocemente si desidera che il lavoro venga elaborato

Velocità di esecuzione
La velocità con cui il lavoro deve essere eseguito quando è pronto, senza essere ritardato per processore, memoria, accesso I/O e ritardo coda

Discrezionale
Una categoria per il lavoro a bassa priorità per cui non ci sono obiettivi di prestazioni

Gli obiettivi del tempo di risposta sono appropriati per le applicazioni dell'utente finale. Ad esempio, gli utenti CICS potrebbero impostare gli obiettivi del carico di lavoro come obiettivi del tempo di risposta. Per gli spazi di indirizzo IBM MQ , gli obiettivi di velocità sono più appropriati. Una piccola quantità di lavoro eseguito nel gestore code viene conteggiata per questo obiettivo di velocità, ma questo lavoro è critico per le prestazioni. La maggior parte del lavoro eseguito dal gestore code viene contato per l'obiettivo di prestazioni dell'applicazione utente finale. La maggior parte del lavoro eseguito dallo spazio di indirizzo dell'iniziatore di canali conta per il proprio obiettivo di velocità. La ricezione e l'invio di messaggi IBM MQ , che l'iniziatore del canale realizza, è generalmente importante per le prestazioni delle applicazioni aziendali che li utilizzano.

Determinazione dell'importanza e della velocità della gestione del carico di lavoro z/OS

Per ulteriori informazioni, consultare “Determinazione dell'importanza della gestione del workload z/OS” a pagina 149.

Memoria libreria

È necessario assegnare la memoria disco per le librerie del prodotto. Le cifre esatte dipendono dalla propria configurazione e devono includere sia le librerie di destinazione e di distribuzione, sia le librerie SMP/E.

Le librerie di destinazione utilizzate da IBM MQ for z/OS utilizzano formati PDSE. Verificare che tutte le librerie di destinazione PDSE non siano condivise all'esterno di un sysplex. Per ulteriori informazioni sulle librerie richieste e sulle relative dimensioni e sul formato richiesto, consultare Program Directory. Per i link di download degli elenchi dei programmi, vedere IBM MQ for z/OS File PDF degli elenchi dei programmi.

Utilizzo LX di sistema

Ogni sottosistema IBM MQ definito riserva un indice di collegamento di sistema (LX) al momento dell'IPL e un certo numero di indici di collegamento non di sistema quando il gestore code viene avviato. L'indice di collegamento del sistema viene riutilizzato quando il gestore code viene arrestato e riavviato. Allo stesso modo, l'accodamento distribuito riserva un indice di collegamento non di sistema. Nel caso improbabile in cui il sistema z/OS abbia LX di sistema inadeguate definite, potrebbe essere necessario prendere in considerazione tali LX di sistema riservate.

Se necessario, è possibile aumentare il numero di LX di sistema impostando il parametro *NSYSLX* in SYS1.PARMLIB IEASYSxx.

z/OS *Determinazione dell'importanza della gestione del workload z/OS*

Per informazioni complete sulla gestione del carico di lavoro e sulla definizione degli obiettivi attraverso la definizione del servizio, consultare la documentazione del prodotto z/OS.

Questo argomento suggerisce come impostare l'importanza della gestione del carico di lavoro z/OS e gli obiettivi di velocità relativi ad altri lavori importanti nel sistema. Per ulteriori informazioni, consultare *z/OS MVS Planning: Workload Management* .

Lo spazio di indirizzo del gestore code deve essere definito con priorità elevata poiché fornisce i servizi del sottosistema. L'iniziatore del canale è uno spazio di indirizzo dell'applicazione, ma generalmente ha una priorità elevata per garantire che i messaggi inviati a un gestore code remoto non vengano ritardati. Advanced Message Security (AMS) fornisce anche servizi del sottosistema e deve essere definito con priorità elevata.

Utilizzare le seguenti classi di servizi:

La classe di servizi SYSSTC predefinita

- Spazi di indirizzo VTAM e TCP/IP
- Spazio di indirizzo IRLM (IRLMPROC)

Nota: Gli spazi di indirizzo VTAM, TCP/IP e IRLM devono avere una priorità di distribuzione più elevata rispetto a tutti gli spazi di indirizzo DBMS, gli spazi di indirizzo collegati e gli spazi di indirizzo subordinati. Non consentire alla gestione del carico di lavoro di ridurre la priorità di VTAM, TCP/IP o IRLM a (o inferiore) quella degli altri spazi di indirizzo DBMS

Un obiettivo ad alta velocità e importanza di 1 per una classe di servizio con un nome definito dall'utente, ad esempio PRODREGN, per quanto segue:

- Gestore code IBM MQ , iniziatore di canali e spazi di indirizzi AMS
- Db2 (tutti gli spazi di indirizzo, tranne lo spazio di indirizzo delle procedure memorizzate stabilite da Db2)

- CICS (tutti i tipi di regione)
- IMS (tutti i tipi di region tranne BMP)

Un obiettivo ad alta velocità è utile per garantire che le avvii e i riavvii vengano eseguiti il più rapidamente possibile per tutti questi spazi di indirizzo.

Gli obiettivi di velocità per le regioni CICS e IMS sono importanti solo durante l'avvio o il riavvio. Dopo l'avvio dell'esecuzione delle transazioni, la gestione del carico di lavoro ignora gli obiettivi di velocità CICS o IMS e assegna le priorità in base agli obiettivi di tempo di risposta delle transazioni in esecuzione nelle regioni. Questi obiettivi di transazione devono riflettere la priorità relativa delle applicazioni aziendali che implementano. In genere, possono avere un valore di importanza pari a 2. Tutte le applicazioni batch che utilizzano IBM MQ devono avere obiettivi di velocità e importanza che riflettono la priorità relativa delle applicazioni di business che implementano. In genere gli obiettivi di importanza e velocità saranno inferiori a quelli di PRODREGN.

z/OS *Configurazione dello spazio di archiviazione*

In uno spazio di indirizzo a 64 bit, esiste una riga virtuale denominata "la barra" che contrassegna l'indirizzo 2GB . La barra separa l'archiviazione al di sotto dell'indirizzo 2GB , denominato "al di sotto del limite", dall'archiviazione al di sopra dell'indirizzo 2GB , denominato "al di sopra del limite". Lo storage sotto la barra utilizza l'indirizzabilità a 31 bit, mentre lo storage sopra la barra utilizza l'indirizzabilità a 64 bit.

È possibile specificare il limite dello storage a 31 - bit utilizzando il parametro JCL REGION e il limite dello storage a 64-bit utilizzando il parametro MEMLIMIT. Questi valori specificati possono essere sovrascritti dalle uscite z/OS .

Configurazione memoria consigliata

La seguente tabella mostra i valori **REGION** e **MEMLIMIT** suggeriti per il gestore code, l'iniziatore di canali e gli spazi di indirizzi AMS. Questi suggerimenti dovrebbero essere utilizzati come punto di partenza e regolati utilizzando le informazioni in:

- “Configurazione della memoria del gestore code” a pagina 150
- “Configurazione della memoria dell'iniziatore di canali in IBM MQ 9.3” a pagina 153
- V 9.3.1 “Configurazione memoria iniziatore di canali da IBM MQ 9.3.1” a pagina 154

Tabella 19. Definizioni suggerite per REGION e MEMLIMIT

Spazio indirizzo	**Configurazione dello spazio di archiviazione**
Gestore code	REGION=0M, MEMLIMIT=3G
Iniziatore del canale in IBM MQ 9.3.0	REGION=0M, MEMLIMIT=256M
V 9.3.1 Iniziatore di canali da IBM MQ 9.3.1	REGION=0M, MEMLIMIT=2G
Spazio di indirizzo AMS	REGION=0M

Gestione della dimensione MEMLIMIT e REGION

Altri meccanismi, ad esempio il parametro **MEMLIMIT** nel membro SMFPRMxx di SYS1.PARMLIB o l'uscita IEFUSI potrebbero essere utilizzati durante l'installazione per fornire una quantità predefinita di memoria virtuale al di sopra della barra per gli spazi di indirizzo z/OS . Consultare Gestione della memoria sopra la barra per dettagli completi sulla limitazione della memoria sopra la barra.

z/OS *Configurazione della memoria del gestore code*

È probabile che lo spazio di indirizzo del gestore code sia l'utente principale dello storage a 64 bit in un'installazione IBM MQ . Ogni collegamento con il gestore code richiede l'allocazione di memoria

comune come descritto nel seguente testo. Oltre allo storage a 64 bit, è necessario consentire al gestore code di utilizzare tutto lo storage a 31 bit disponibile specificando REGION=0M nel JCL del gestore code.

Memoria comune

Ogni sistema secondario IBM MQ for z/OS ha i seguenti requisiti di memoria approssimativi:

- CSA 4KB
- ECSA 800KB, più la dimensione della tabella di traccia specificata nel parametro **TRACTBL** della macro del parametro di sistema CSQ6SYSP . Per ulteriori informazioni, consultare Utilizzo di CSQ6SYSP.

Inoltre, ciascuna connessione logica simultanea al gestore code richiede circa 5 KB di ECSA. Quando un'attività termina, altre attività IBM MQ possono riutilizzare questa memoria.

IBM MQ non rilascia lo storage fino a quando il gestore code non viene arrestato, pertanto è possibile calcolare la quantità massima di ECSA richiesta moltiplicando per 5KBil numero massimo di connessioni simultanee. Il numero di connessioni logiche simultanee è la somma del numero di:

- Attività (TCB) nelle aree Batch, TSO, z/OS UNIX System Services, IMSe SPAS (stored procedure address space) Db2 connesse a IBM MQ, ma non disconnesse.
- Transazioni CICS che hanno emesso una richiesta IBM MQ , ma non sono terminate
- JMS Connessioni, sessioni, TopicSessions o QueueSessions che sono state create (per la connessione dei collegamenti), ma non ancora eliminate o raccolte di dati inutilizzati.
- Canali IBM MQ attivi

È possibile impostare un limite per la memoria comune, utilizzata dalle connessioni logiche al gestore code, con il parametro di configurazione **ACELIM** . Il controllo **ACELIM** è principalmente di interesse per i siti in cui le procedure memorizzate Db2 causano operazioni sulle code IBM MQ .

Quando si utilizza una procedura memorizzata, ciascuna operazione IBM MQ può risultare in una nuova connessione logica al gestore code. Unità di lavoro Db2 di grandi dimensioni, ad esempio a causa del carico della tabella, possono causare una richiesta eccessiva di memoria comune.

ACELIM ha lo scopo di limitare l'utilizzo della memoria comune e proteggere il sistema z/OS , limitando il numero di connessioni nel sistema. Impostare **ACELIM** solo sui gestori code identificati come gestori code che utilizzano quantità eccessive di memoria ECSA. Per ulteriori informazioni, vedere la sezione **ACELIM** in *Utilizzo di CSQ6SYSP* .

Per impostare un valore per **ACELIM**, determinare innanzitutto la quantità di memoria attualmente nel pool secondario controllato dal valore **ACELIM** . Queste informazioni si trovano nei record SMF 115 sottotipo 5 prodotti dalla traccia CLASS (3) delle statistiche.

IBM MQ I dati SMF possono essere formattati utilizzando SupportPac MP1B. Il numero di byte in uso nel pool secondario controllato da **ACELIM** viene visualizzato in STGPOOL DD, nella linea denominata *ACE/PEB*.

Per ulteriori informazioni sui record di statistiche SMF 115, consultare Interpretazione delle statistiche delle prestazioni di IBM MQ for z/OS.

Aumentare il valore normale di un margine sufficiente per fornire spazio per la crescita e i picchi del carico di lavoro. Dividere il nuovo valore per 1024 per ottenere una dimensione di memoria massima in KB da utilizzare nella configurazione **ACELIM** .

Memoria privata

Lo spazio di indirizzo del gestore code utilizza la memoria a 64 bit per molti blocchi di controllo interni. Il parametro **MEMLIMIT** del JCL del gestore code definisce la quantità massima di memoria a 64 bit disponibile. 3GB di archiviazione, `MEMLIMIT=3G`, è il minimo che dovresti utilizzare, tuttavia, a seconda della tua configurazione potrebbe essere richiesto un numero significativamente maggiore.

È necessario specificare un valore **MEMLIMIT** specifico piuttosto che `MEMLIMIT=NOLIMIT` per evitare potenziali problemi. Se si specifica `NOLIMIT` o un valore molto grande, è possibile utilizzare tutta la

memoria virtuale z/OS disponibile, il che porta al paging nel proprio sistema. Quando si aumenta il valore di **MEMLIMIT** , è necessario discutere la nuova impostazione con il proprio programmatore di sistema z/OS nel caso in cui vi sia un limite a livello di sistema sulla quantità di memoria che è possibile utilizzare.

Se si dispone di un valore elevato per **MEMLIMIT** , potrebbe essere necessario aumentare la dimensione dei dataset di dump man mano che vengono catturati più dati in un dump.

È possibile monitorare l'utilizzo della memoria dello spazio di indirizzo dal messaggio CSQY220I che indica la quantità di memoria privata a 31 e 64 bit in uso e la quantità libera rimanente.

Pool di buffer

I pool di buffer sono un utente significativo della memoria privata nello spazio di indirizzo del gestore code. Ciascuna dimensione del pool di buffer viene determinata al momento dell'inizializzazione del gestore code e la memoria viene assegnata per il pool di buffer quando una serie di pagine che utilizza tale pool di buffer è connessa. Il parametro **LOCATION (ABOVE|BELOW)** viene utilizzato per specificare dove vengono assegnati i buffer. È possibile utilizzare il comando ALTER BUFFPOOL per modificare dinamicamente la dimensione dei pool di buffer.

Quando si calcola un valore per **MEMLIMIT** , è fondamentale considerare le dimensioni del pool di buffer se sono configurate con **LOCATION(ABOVE)**. È necessario eseguire il calcolo come segue.

Calcolare il valore di **MEMLIMIT** come 2GB più la dimensione dei pool di buffer configurati con **LOCATION(ABOVE)**, arrotondati al GB più vicino. Impostare MEMLIMIT su un minimo di 3GB e aumentarlo come necessario quando è necessario aumentare la dimensione dei pool di buffer.

Ad esempio, per tre pool di buffer configurati con **LOCATION(ABOVE)**, il pool di buffer uno ha 10.000 buffer e i pool di buffer due e tre hanno 50.000 buffer ciascuno. L'utilizzo di memoria al di sopra della barra è uguale a 110.000 (numero totale di buffer) * 4096 = 450.560.000 byte = 430MB.

Tutti i pool di buffer indipendentemente da **LOCATION** utilizzano lo storage a 64 bit per le strutture di controllo. Poiché il numero di pool di buffer e il numero di buffer in tali pool aumentano, ciò può diventare significativo. Ogni buffer richiede circa 200 byte aggiuntivi di storage a 64 bit. Per la configurazione precedente che richiederebbe: 200 * 110.000 = 22.000.000 byte = 21MB.

Pertanto, in questo scenario 3GB può essere utilizzato per **MEMLIMIT**, che consente un ambito di crescita: 21MB + 430MB + 2GB che arrotonda a 3GB.

Per alcune configurazioni, l'utilizzo dei pool di buffer i cui buffer sono permanentemente supportati dalla memoria reale può offrire notevoli vantaggi in termini di prestazioni. È possibile ottenere tale risultato specificando il valore FIXED4KB dell'attributo **PAGECLAS** del pool di buffer. Tuttavia, si consiglia di eseguire questa operazione solo se è disponibile memoria reale sufficiente sulla LPAR, altrimenti potrebbero essere interessati altri spazi di indirizzo. Per informazioni su quando utilizzare il valore FIXED4KB per **PAGECLAS**, consultare IBM MQ Support Pac MP16: IBM MQ for z/OS - Capacity planning & tuning.

Rendere i pool di buffer così grandi da avere la paginazione MVS potrebbe influire negativamente sulle prestazioni. Si potrebbe considerare l'utilizzo di un pool di buffer più piccolo che non esegue la paginazione, con IBM MQ che sposta il messaggio da e verso la serie di pagine.

V 9.3.1 RECUPERO CFSTRUCT

Da IBM MQ 9.3.1 il comando **RECOVER CFSTRUCT** fa un uso maggiore dello storage a 64 bit. In molti casi dovrebbe essere disponibile uno storage a 64 bit di riserva, pertanto l'utilizzo del comando non richiede un aumento del valore di **MEMLIMIT**. Tuttavia, se è probabile che si disponga di backup di strutture di grandi dimensioni, contenenti più di alcuni milioni di messaggi, è necessario aumentare **MEMLIMIT** per tutti i gestori code che potrebbero elaborare il comando **RECOVER CFSTRUCT** di 500MB.

Ad esempio, se si dispone già di MEMLIMIT=3G , si consiglia di utilizzare MEMLIMIT=4G poiché il parametro **MEMLIMIT** non consente le virgole decimali.

Buffer SMDS (Shared Message Data Set) e MEMLIMIT

Quando si eseguono i carichi di lavoro di messaggistica utilizzando i dataset di messaggi condivisi, esistono due livelli di ottimizzazione che possono essere raggiunti regolando gli attributi DSBUFS e DSBLOCK.

La quantità di memoria del gestore code sopra riportata utilizzata dal buffer SMDS è DSBUFS x DSBLOCK. Ciò significa che per impostazione predefinita, vengono utilizzati 100 x 256KB (25MB) per ogni struttura CFLEVEL (5) nel gestore code.

Sebbene questo valore non sia troppo elevato, se la propria azienda o le aziende hanno molte CFSTRUCTs, alcune di esse potrebbero assegnare un valore elevato di MEMLIMIT per i pool di buffer e, a volte, avere code indicizzate in profondità, quindi in totale, potrebbero esaurire la memoria al di sopra della barra.

z/OS *Configurazione della memoria dell'iniziatore di canali in IBM MQ 9.3*

L'iniziatore di canali in genere utilizza meno memoria a 64 bit rispetto al gestore code. Oltre allo storage a 64 bit, è necessario consentire all'iniziatore di canali di utilizzare tutta la memoria a 31 bit disponibile specificando REGION=0M nel JCL del gestore code.

Memoria comune

L'iniziatore di canali generalmente richiede l'utilizzo di ECSA fino a 160KB.

Storage privato a 31 bit

La memoria a 31 bit disponibile per l'iniziatore di canali limita il numero di connessioni simultanee che CHINIT può avere.

Ogni canale utilizza circa 170KB di regione privata estesa nello spazio di indirizzi dell'iniziatore di canali. Per i canali dei messaggi, ad esempio, i canali mittente o destinatario, la memoria viene aumentata della dimensione del messaggio se vengono trasmessi messaggi più grandi di 32KB . Questa memoria aumentata viene liberata quando:

- Un canale di invio o client richiede meno della metà della dimensione buffer corrente per 10 messaggi consecutivi.
- Viene inviato o ricevuto un heartbeat.

La memoria viene liberata per essere riutilizzata all'interno di Language Environment, tuttavia, la memoria non viene considerata libera dal gestore memoria virtuale z/OS . Ciò significa che il limite superiore per il numero di canali dipende dalla dimensione del messaggio e dai modelli di arrivo e dalle limitazioni dei sistemi utente individuali sulla dimensione della regione privata estesa.

È probabile che il limite superiore sul numero di canali sia circa 9000 su molti sistemi perché è improbabile che la dimensione della regione estesa superi 1.6GB. L'utilizzo di dimensioni dei messaggi superiori a 32KB riduce il numero massimo di canali nel sistema. Ad esempio, se i messaggi lunghi 100MB vengono trasmessi e si assume una dimensione dell'area estesa di 1.6GB , il numero massimo di canali è 15.

La traccia dell'iniziatore di canali viene scritta in uno spazio dati. La dimensione della memoria dello spazio dati è controllata dal parametro **TRAXTBL** . Vedere ALTER QMGR.

Storage privato a 64 bit

Il parametro MEMLIMIT del JCL dell'iniziatore di canali definisce la quantità massima di memoria a 64 bit disponibile. 256MB di memoria, MEMLIMIT=256M, è il valore minimo da utilizzare. A seconda della configurazione, potrebbe essere richiesto un numero significativamente maggiore.

È necessario specificare un valore MEMLIMIT sensibile piuttosto che MEMLIMIT = NOLIMIT per evitare potenziali problemi. Se si specifica NOLIMIT o un valore molto grande, esiste la possibilità di utilizzare tutta la memoria virtuale z/OS disponibile, portando alla paginazione nel sistema. Quando si aumenta il

valore di MEMLIMIT, è necessario discutere la nuova impostazione con il programmatore del sistema z/OS nel caso in cui vi sia un limite a livello di sistema sulla quantità di memoria che può essere utilizzata.

Se si dispone di un valore elevato per MEMLIMIT, potrebbe essere necessario aumentare la dimensione dei dataset di dump man mano che vengono acquisiti più dati in un dump.

Esiste un singolo utente di storage a 64 bit nell'iniziatore di canali: SMF.

SMF

Se abilitato, l'account o le statistiche SMF di classe 4 richiedono lo storage a 64 bit. È richiesto un minimo di 256MB di memoria. Se la memoria disponibile non è sufficiente, l'iniziatore del canale emette il messaggio CSQX124E e le statistiche e l'account della classe 4 non sono disponibili.

Configurazione memoria iniziatore di canali da IBM MQ 9.3.1

L'iniziatore di canali in genere utilizza meno memoria a 64 bit rispetto al gestore code. Tuttavia, da IBM MQ 9.3.1 l'utilizzo è aumentato. Oltre all'archiviazione a 64 bit, è necessario consentire all'iniziatore di canale di utilizzare tutta l'archiviazione a 31 bit disponibile specificando REGION=0M nel JCL dell'iniziatore di canale.

Memoria comune

L'iniziatore di canali generalmente richiede l'utilizzo di ECSA fino a 160KB.

Storage privato a 31 bit

La memoria a 31 bit disponibile per l'iniziatore di canali limita il numero di connessioni simultanee che CHINIT può avere.

Ogni canale utilizza circa 170KB di regione privata estesa nello spazio di indirizzi dell'iniziatore di canali. Per i canali dei messaggi, ad esempio, i canali mittente o ricevente, la memoria viene aumentata in base alla dimensione del messaggio se vengono trasmessi messaggi più grandi di 32KB . Questa memoria aumentata viene liberata quando:

- Un canale di invio o client richiede meno della metà della dimensione buffer corrente per 10 messaggi consecutivi.
- Viene inviato o ricevuto un heartbeat.

La memoria viene liberata per essere riutilizzata all'interno di Language Environment, tuttavia, la memoria non viene considerata libera dal gestore memoria virtuale z/OS . Ciò significa che il limite superiore per il numero di canali dipende dalla dimensione del messaggio e dai modelli di arrivo e dalle limitazioni dei sistemi utente individuali sulla dimensione della regione privata estesa.

È probabile che il limite superiore sul numero di canali sia circa 9000 su molti sistemi perché è improbabile che la dimensione della regione estesa superi 1.6GB.

La traccia dell'iniziatore di canali viene scritta in uno spazio dati. La dimensione della memoria dello spazio dati è controllata dal parametro **TRAXTBL** . Vedere ALTER QMGR.

Storage privato a 64 bit

Il parametro **MEMLIMIT** del JCL dell'inizializzatore di canale definisce la quantità massima di memoria a 64 bit disponibile. 2 GB di memoria, `MEMLIMIT=2G`, è il valore minimo da utilizzare. A seconda della configurazione, potrebbe essere richiesto un numero significativamente maggiore.

Si dovrebbe specificare un valore sensato di **MEMLIMIT** piuttosto che di `MEMLIMIT=NOLIMIT` per evitare potenziali problemi. Se si specifica `NOLIMIT` o un valore molto grande, è possibile che venga utilizzato tutto lo spazio di archiviazione virtuale z/OS disponibile, con conseguente paging nel sistema. Quando si aumenta il valore di **MEMLIMIT**, è necessario discutere la nuova impostazione con il programmatore del sistema z/OS, nel caso in cui vi sia un limite a livello di sistema sulla quantità di memoria disponibile che può essere utilizzata.

Se il valore di **MEMLIMIT** è elevato, potrebbe essere necessario aumentare le dimensioni dei set di dati del dump, in quanto vengono acquisiti più dati in un dump.

Esistono due utenti di storage a 64 bit nell'iniziatore di canali: SMF e canali di connessione server.

SMF

Se abilitato, l'account o le statistiche SMF di classe 4 richiedono lo storage a 64 bit. È richiesto un minimo di 256MB di memoria. Se la memoria disponibile non è sufficiente, l'iniziatore del canale emette il messaggio CSQX124E e le statistiche e l'account della classe 4 non sono disponibili.

Canali di connessione server

Dai canali di connessione server IBM MQ 9.3.1 allocare i buffer di messaggi nello storage a 64 bit, se stanno trasferendo messaggi di dimensione superiore a 32 KB.

Questi buffer vengono resi disponibili se i canali richiedono meno della metà della dimensione del buffer corrente per 10 messaggi consecutivi o se viene inviato o ricevuto un heartbeat.

Il valore di **MEMLIMIT** stabilisce un limite superiore al numero di canali di connessione al server che possono funzionare contemporaneamente. Dovreste usare un valore minimo di `MEMLIMIT=2G` per garantire che possa funzionare lo stesso numero di canali delle versioni precedenti di IBM MQ 9.3.1, oltre a fornire una certa capacità di crescita.

È possibile calcolare un valore approssimativo per **MEMLIMIT** calcolando il numero massimo di picchi di canali di connessione al server attivi simultaneamente e la dimensione massima dei messaggi che si prevede di trasferire. Si consiglia di utilizzare `MEMLIMIT=2G` come punto di partenza e di arrotondare per eccesso.

Ad esempio, se si imposta un numero massimo di canali di connessione al server pari a 2.000 e ogni canale ha una dimensione massima del messaggio di 1MB, i canali di connessione al server utilizzano un massimo di poco meno di 2GB di memoria a 64 bit. Poiché è molto vicino a 2GB, si dovrebbe arrotondare a `MEMLIMIT=3G`.

z/OS *Storage su disco*

Utilizzare questo argomento quando si pianifica i requisiti di archiviazione disco per i dataset di log, la memoria Db2 , la memoria CF e i dataset di pagina.

Rivolgersi all'amministratore della memoria per determinare dove inserire i dataset del gestore code. Ad esempio, l'amministratore dell'archiviazione può fornire volumi DASD specifici o classi di archiviazione SMS, classi di dati e classi di gestione per i diversi tipi di dataset.

- I dataset di log devono essere su DASD. Questi log possono avere un'attività I/O elevata con un tempo di risposta ridotto e non è necessario eseguire il backup.
- I log di archivio possono essere su DASD o nastro. Una volta creati, potrebbero non essere più letti se non in una situazione anomala, ad esempio il ripristino di una serie di pagine da un backup. Dovrebbero avere una data di conservazione lunga.
- Le serie di pagine potrebbero avere un'attività da bassa a media e dovrebbero essere sottoposte a backup regolarmente. Su un sistema ad alto utilizzo, dovrebbero essere sottoposti a backup due volte al giorno.
- I dataset BSDS devono essere sottoposti a backup quotidianamente; non hanno un'elevata attività I/O.

Tutti i dataset sono simili a quelli utilizzati da Db2e procedure di manutenzione simili possono essere utilizzate per IBM MQ.

Consultare le sezioni seguenti per i dettagli su come pianificare l'archiviazione dei propri dati:

- **Log e archiviazione**

  “Per quanto tempo devo conservare i log di archivio” a pagina 173 descrive come determinare la quantità di memoria richiesta dai dataset di archivio e di log attivi, in base al volume di messaggi gestiti dal sistema IBM MQ e alla frequenza con cui i log attivi vengono scaricati nei dataset di archivio.

- **Db2 memoria**

  “Db2 archiviazione” a pagina 190 descrive come determinare la quantità di memoria Db2 necessaria per i dati IBM MQ .
- **memoria CF**

  La “Definizione delle risorse CF (Coupling Facility)” a pagina 181 descrive come determinare la dimensione delle strutture CFS.
- **Serie di pagine e memoria messaggi**

  “Pianificazione delle serie di pagine e dei pool di buffer” a pagina 156 descrive come determinare la quantità di memoria richiesta per i dataset di pagina, in base alle dimensioni dei messaggi scambiati dalle proprie applicazioni, al numero di tali messaggi e alla frequenza con cui vengono creati o scambiati.

z/OS *Dove trovare ulteriori informazioni sui requisiti di archiviazione e prestazioni*

Utilizzare questo argomento come riferimento per trovare ulteriori informazioni sui requisiti di archiviazione e prestazioni.

È possibile trovare ulteriori informazioni dalle seguenti fonti:

Tabella 20. Dove trovare ulteriori informazioni sui requisiti di archiviazione

Argomento	**Dove cercare**
Parametri di sistema	Utilizzo di CSQ6SYSP e Personalizzazione dei gestori code
Memoria richiesta per installare IBM MQ	Directory programma. Per i link di download degli elenchi dei programmi, vedere IBM MQ for z/OS File PDF degli elenchi dei programmi.
Uscite IEALIMIT e IEFUSI	Consultare IEALIMIT e IEFUSI nella documentazione *z/OS:MVS Installation Exits* .
Informazioni più recenti	IBM MQ Sito Web SupportPac SupportPacs perIBMMQ e altre aree di progetto.
Gestione del carico di lavoro e definizione degli obiettivi tramite la definizione del servizio	*z/OS Pianificazione MVS: Gestione del carico di lavoro*

z/OS Pianificazione delle serie di pagine e dei pool di buffer

Informazioni che consentono di pianificare il numero iniziale e le dimensioni dei dataset di pagina e dei pool di buffer.

Il presente argomento contiene le seguenti sezioni:

- “Pianificare le serie di pagine” a pagina 157
  - Utilizzo della serie di pagine
  - Numero di serie di pagine
  - Dimensione delle serie di pagine
  - Pianificazione per la codifica del dataset z/OS
- “Calcolare la dimensione dei set di pagine” a pagina 158
  - Serie di pagine zero
  - Serie di pagine 01-99
  - Calcolo del requisito di memoria per i messaggi

- “Abilitazione dell'espansione della serie di pagine dinamica” a pagina 160
- “Definizione dei pool di buffer” a pagina 161

Pianificare le serie di pagine

Utilizzo serie di pagine

Per i messaggi di breve durata, vengono normalmente utilizzate poche pagine nella serie di pagine e non vi è alcun I/O per i dataset tranne all'avvio, durante un checkpoint o all'arresto.

Per i messaggi di lunga durata, tali pagine contenenti messaggi vengono normalmente scritte su disco. Questa operazione viene eseguita dal gestore code per ridurre il tempo di riavvio.

Separare i messaggi di breve durata dai messaggi di lunga durata collocandoli in serie di pagine differenti e in pool di buffer differenti.

Numero di serie di pagine

L'utilizzo di diverse serie di pagine di grandi dimensioni può rendere più semplice il ruolo dell'amministratore di IBM MQ , poiché ciò significa che è necessario un numero minore di serie di pagine, rendendo più semplice l'associazione delle code alle serie di pagine.

L'utilizzo di più serie di pagine più piccole presenta una serie di vantaggi. Ad esempio, il backup richiede meno tempo e l'I/O può essere eseguito in parallelo durante il backup e il riavvio. Tuttavia, si consideri che ciò aggiunge un costo significativo per le prestazioni al ruolo dell'amministratore IBM MQ , che è richiesto per associare ogni coda a uno di un numero molto maggiore di serie di pagine.

Definire almeno cinque serie di pagine, come segue:

- Una serie di pagine riservata per le definizioni di oggetto (serie di pagine zero)
- Una serie di pagine per i messaggi relativi al sistema
- Una serie di pagine per i messaggi di lunga durata critici per le prestazioni
- Una serie di pagine per messaggi di breve durata critici per le prestazioni
- Una serie di pagine per tutti gli altri messaggi

“Definizione dei pool di buffer” a pagina 161 spiega i vantaggi delle prestazioni della distribuzione dei messaggi sulle serie di pagine in questo modo.

Dimensione delle serie di pagine

Definire uno spazio sufficiente nelle serie di pagine per la capacità massima di messaggi prevista. Considerare eventuali picchi di capacità imprevisti, ad esempio quando si sviluppa un accumulo di messaggi perché un programma del server di coda non è in esecuzione. È possibile farlo assegnando la serie di pagine con estensioni secondarie o, in alternativa, abilitando l'espansione della serie di pagine dinamica. Per ulteriori informazioni, consultare “Abilitazione dell'espansione della serie di pagine dinamica” a pagina 160. È difficile rendere un set di pagine più piccolo, quindi è spesso meglio assegnare un set di pagine più piccolo e consentirgli di espandersi quando necessario.

Quando si pianificano le dimensioni della serie di pagine, considerare tutti i messaggi che potrebbero essere generati, inclusi i dati dei messaggi non dell'applicazione. Ad esempio, attivare i messaggi, i messaggi di evento e tutti i messaggi di report richiesti dall'applicazione.

La dimensione della serie di pagine determina il tempo impiegato per ripristinare una serie di pagine durante il ripristino da un backup, poiché il ripristino di una serie di pagine di grandi dimensioni richiede più tempo.

Nota: Il ripristino di una serie di pagine dipende anche dal tempo impiegato dal gestore code per elaborare i record di log scritti dopo l'esecuzione del backup; questo periodo di tempo è determinato dalla frequenza del backup. Per ulteriori informazioni, consultare “Pianificazione del backup e del ripristino” a pagina 192.

Nota: Le serie di pagine più grandi di 4 GB richiedono l'utilizzo dell'indirizzabilità estesa SMS.

Pianificazione per la codifica del dataset z/OS

È possibile applicare la funzione di codifica del dataset z/OS ai set di pagine per i gestori code in esecuzione su IBM MQ for z/OS 9.1.4 o versioni successive.

È necessario assegnare queste serie di pagine con gli attributi EXTENDED e un'etichetta della chiave del dataset che garantisce che i dati siano codificati AES.

Consultare la sezione, Riservatezza per i dati inattivi su IBM MQ for z/OS con la crittografia del dataset. per ulteriori informazioni.

Calcolare la dimensione dei set di pagine

Per le definizioni di oggetti del gestore code (ad esempio, code e processi), è semplice calcolare il requisito di memoria perché questi oggetti hanno una dimensione fissa e sono permanenti. Per i messaggi, tuttavia, il calcolo è più complesso per i seguenti motivi:

- La dimensione dei messaggi varia.
- I messaggi sono transitori.
- Lo spazio occupato dai messaggi che sono stati richiamati viene recuperato periodicamente da un processo asincrono.

Se necessario, è possibile creare serie di pagine di grandi dimensioni superiori a 4 GB che forniscono ulteriore capacità per i messaggi se la rete si arresta. Non è possibile modificare le serie di pagine esistenti. Invece, è necessario creare nuove serie di pagine con indirizzabilità estesa e attributi di formato esteso. I nuovi set di pagine devono avere la stessa dimensione fisica di quelli vecchi e i vecchi set di pagine devono essere copiate nei nuovi. Se è richiesta la migrazione all'indietro, la serie di pagine zero non deve essere modificata. Se le serie di pagine inferiori a 4 GB sono adeguate, non è necessaria alcuna azione.

Serie di pagine zero

La serie di pagine zero è riservata per definizioni di oggetti.

Per la serie di pagine zero, la memoria richiesta è:

```
    (maximum number of local queue definitions x 1010)
       (excluding shared queues)
+   (maximum number of model queue definitions x 746)
+   (maximum number of alias queue definitions x 338)
+   (maximum number of remote queue definitions x 434)
+   (maximum number of permanent dynamic queue definitions x 1010)
+   (maximum number of process definitions x 674)
+   (maximum number of namelist definitions x 12320)
+   (maximum number of message channel definitions x 2026)
+   (maximum number of client-connection channel definitions x 5170)
+   (maximum number of server-connection channel definitions x 2026)
+   (maximum number of storage class definitions x 266)
+   (maximum number of authentication information definitions x 1010)
+   (maximum number of administrative topic definitions x 15000)
+   (total length of topic strings defined in administrative topic definitions)
```

Dividere questo valore per 4096 per determinare il numero di record da specificare nel cluster per il dataset della serie di pagine.

Non è necessario consentire gli oggetti memorizzati nel repository condiviso, ma è necessario consentire gli oggetti memorizzati o copiati nella serie di pagine zero (oggetti con disposizione GROUP o QMGR).

Il numero totale di oggetti che è possibile creare è limitato dalla capacità della serie di pagine zero. Il numero di code locali che è possibile definire è limitato a 524 287.

Serie di pagine 01-99

Per le serie di pagine da 01 a 99, la memoria richiesta per ciascuna serie di pagine è determinata dal numero e dalla dimensione dei messaggi memorizzati in tale serie di pagine. I messaggi sulle code condivise non vengono memorizzati nelle serie di pagine.

Dividere questo valore per 4096 per determinare il numero di record da specificare nel cluster per il dataset della serie di pagine.

Calcolo del requisito di memoria per i messaggi

Questa sezione descrive il modo in cui i messaggi vengono memorizzati nelle pagine. Ciò consente di calcolare la quantità di memoria della serie di pagine che è necessario definire per i messaggi. Per calcolare lo spazio approssimativo richiesto per tutti i messaggi su una serie di pagine, è necessario considerare la profondità massima della coda di tutte le code associate alla serie di pagine e la dimensione media dei messaggi su tali code.

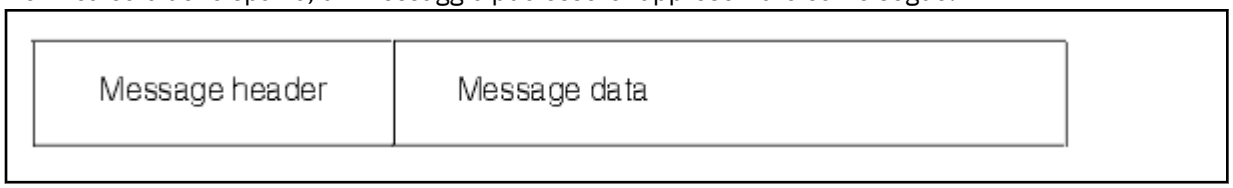
Nota: Le dimensioni delle strutture e le informazioni di controllo fornite in questa sezione possono variare tra le principali emissioni. Per i dettagli specifici della release di IBM MQ, fare riferimento a SupportPac MP16 -IBMMQ perz/OS Pianificazione e ottimizzazione della capacità e IBMMQ Famiglia - Rapporti sulle prestazioni

È necessario consentire la possibilità che il messaggio "gets" possa essere ritardato per motivi al di fuori del controllo di IBM MQ (ad esempio, a causa di un problema con il protocollo di comunicazione). In questo caso, la frequenza "put" dei messaggi potrebbe superare di gran lunga la frequenza "get". Ciò può comportare un notevole aumento del numero di messaggi memorizzati nelle serie di pagine e un conseguente aumento della dimensione di memoria richiesta.

Ogni pagina nella serie di pagine è lunga 4096 byte. Consentendo informazioni di intestazione fissa, ogni pagina ha 4057 byte di spazio disponibile per la memorizzazione dei messaggi.

Quando si calcola lo spazio richiesto per ogni messaggio, la prima cosa da considerare è se il messaggio si adatta a una pagina (un messaggio breve) o se deve essere suddiviso su due o più pagine (un messaggio lungo). Quando i messaggi vengono suddivisi in questo modo, è necessario consentire ulteriori informazioni di controllo nei calcoli dello spazio.

Per il calcolo dello spazio, un messaggio può essere rappresentato come segue:



La sezione dell'intestazione del messaggi contiene il descrittore del messaggio e altre informazioni di controllo, la cui dimensione varia in base alla dimensione del messaggio. La sezione dei dati del messaggio contiene tutti i dati effettivi del messaggio e tutte le altre intestazioni (ad esempio, l'intestazione di trasmissione o l'intestazione del bridge IMS).

Sono richieste almeno due pagine per le informazioni di controllo della serie di pagine che, in genere, sono inferiori all ' 1% dello spazio totale richiesto per i messaggi.

Messaggi brevi

Un messaggio breve è definito come un messaggio che si adatta a una pagina.

I piccoli messaggi vengono memorizzati uno su ogni pagina.

Messaggi lunghi

Se la dimensione dei dati del messaggio è maggiore di 3596 byte, ma non maggiore di 4 MB, il messaggio viene classificato come un messaggio lungo. Quando viene visualizzato un messaggio lungo, IBM MQ memorizza il messaggio su una serie di pagine e memorizza le informazioni di controllo che puntano a queste pagine nello stesso modo in cui memorizzerebbe un messaggio breve. Questo è mostrato in Figura 41 a pagina 160:

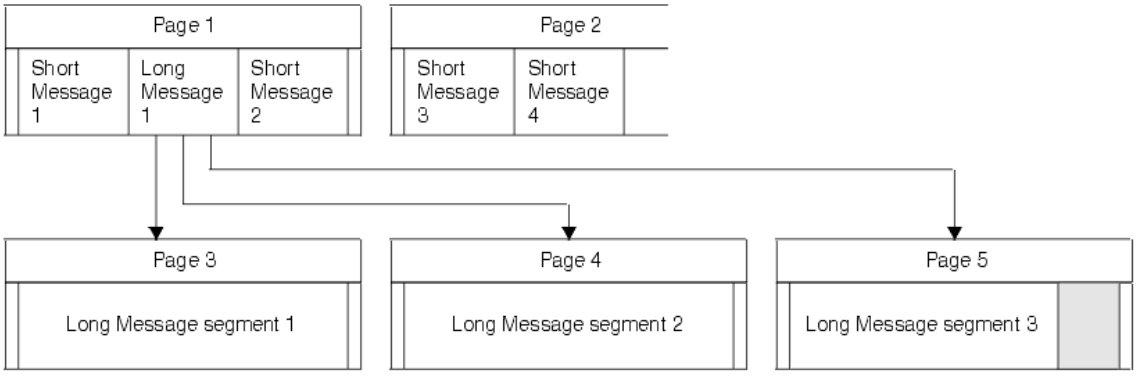


Figura 41. Modalità con cui IBM MQ memorizza i messaggi lunghi nelle serie di pagine

Messaggi molto lunghi

I messaggi molto lunghi sono messaggi con una dimensione superiore a 4 MB. Questi sono memorizzati in modo che ogni 4 MB utilizzi 1037 pagine. Tutto il resto viene memorizzato nello stesso modo di un messaggio lungo, come descritto sopra.

z/OS *Abilitazione dell'espansione della serie di pagine dinamica*

I set di pagine possono essere estesi dinamicamente mentre il gestore code è in esecuzione. Una serie di pagine può avere 123 estensioni e può essere distribuita su più volumi disco.

Ogni volta che una serie di pagine si espande, viene utilizzata una nuova estensione della serie di dati. Il gestore code continua ad espandere una serie di pagine quando richiesto, fino a quando non viene raggiunto il numero massimo di estensioni o fino a quando non è disponibile ulteriore memoria per l'assegnazione su volumi idonei.

Una volta che l'espansione della serie di pagine non riesce per uno dei motivi sopra indicati, il gestore code contrassegna la serie di pagine per non ulteriori tentativi di espansione. Questo contrassegno può essere reimpostato modificando la serie di pagine in EXPAND (SYSTEM).

L'espansione della serie di pagine avviene in maniera asincrona a tutte le altre attività della serie di pagine, quando viene allocato il 90% dello spazio esistente nella serie di pagine.

Il processo di espansione della serie di pagine formatta l'estensione appena assegnata e la rende disponibile per l'utilizzo da parte del gestore code. Tuttavia, nessuno spazio è disponibile per l'uso, fino a quando l'intera estensione non è stata formattata. Ciò significa che l'espansione in larga misura potrebbe richiedere del tempo, e l'inserimento di applicazioni potrebbe 'bloccare' se riempiono il restante 10% della serie di pagine prima che l'espansione sia stata completata.

L'esempio thlqual.SCSQPROC(CSQ4PAGE) mostra come definire le estensioni secondarie.

Per controllare la dimensione delle nuove estensioni, utilizzare una delle seguenti opzioni della parola chiave EXPAND dei comandi DEFINE PSID e ALTER PSID:

- UTENTE
- SISTEMA
- Nessuna

UTENTE

Utilizza la dimensione dell'estensione secondaria specificata quando è stata assegnata la serie di pagine. Se non è stato specificato un valore o se è stato specificato un valore zero, non è possibile che si verifichi un'espansione della serie di pagine dinamica.

L'espansione della serie di pagine si verifica quando lo spazio nella pagina è utilizzato al 90% e viene eseguito in maniera asincrona con altre attività della serie di pagine.

Ciò può portare all'espansione di più di una singola estensione alla volta.

Considerare il seguente esempio: si assegna una serie di pagine con un'estensione primaria di 100.000 pagine e un'estensione secondaria di 5000 pagine. Viene inserito un messaggio che richiede 9999 pagine. Se la serie di pagine utilizza già 85.000 pagine, la scrittura del messaggio supera il limite massimo del 90% (90.000 pagine). A questo punto, un'ulteriore estensione secondaria viene allocata all'estensione primaria di 100.000 pagine, portando la dimensione della serie di pagine a 105.000 pagine. Le restanti 4999 pagine del messaggio continuano ad essere scritte. Quando lo spazio di pagina utilizzato raggiunge 94.500 pagine, ovvero il 90% della dimensione della serie di pagine aggiornata di 105.000 pagine, viene assegnata un'altra estensione di 5000 pagine, portando la dimensione della serie di pagine a 110.000 pagine. Alla fine di MQPUT, la serie di pagine è stata espansa due volte e vengono utilizzate 94.500 pagine. Nessuna delle pagine nella seconda espansione della serie di pagine è stata utilizzata, sebbene siano state assegnate.

Al riavvio, se una serie di pagine precedentemente utilizzata viene sostituita con un data set simile, allora la serie di pagine verrà espansa fino al raggiungimento della dimensione del data set utilizzato in precedenza. Per raggiungere questa dimensione è necessario eseguire soltanto un'estensione.

SISTEMA

Ignora la dimensione dell'estensione secondaria specificata quando è stata definita la serie di pagine. Invece, il gestore code imposta un valore che è approssimativamente il 10% della dimensione della serie di pagine corrente. Il valore viene arrotondato al cilindro più vicino di DASD.

Se non è stato specificato un valore o se è stato specificato un valore pari a zero, l'espansione della serie di pagine dinamica può ancora verificarsi. Il gestore code imposta un valore che è circa il 10% della dimensione della serie di pagine corrente. Il nuovo valore viene arrotondato in base alle caratteristiche del DASD.

L'espansione della serie di pagine si verifica quando lo spazio nella serie di pagine è circa il 90% utilizzato e viene eseguito in maniera asincrona con altre attività della serie di pagine.

Al riavvio, se una serie di pagine precedentemente utilizzata viene sostituita con un data set simile, allora la serie di pagine verrà espansa fino al raggiungimento della dimensione del data set utilizzato in precedenza.

Nessuna

Non deve essere eseguita alcuna ulteriore espansione della serie di pagine.

Riferimenti correlati

PSID ALTER

DEFINE PSID

VISUALIZZAZIONEUTILIZZO

Definizione dei pool di buffer

Utilizzare questo argomento per pianificare il numero di pool di buffer da definire e le relative impostazioni.

Questo argomento è suddiviso nelle sezioni seguenti:

1. “Decidere il numero di pool di buffer da definire” a pagina 161
2. “Decidere le impostazioni per ciascun pool di buffer” a pagina 162
3. “Monitorare le prestazioni dei pool di buffer sotto il carico previsto” a pagina 163
4. “Regola caratteristiche del pool di buffer” a pagina 163

Decidere il numero di pool di buffer da definire

È necessario definire inizialmente quattro pool di buffer:

Bufferpool 0
Utilizzare per le definizioni di oggetto (nella serie di pagine zero) e per le code di messaggi relative al sistema, come SYSTEM.CHANNEL.SYNCQ e SYSTEM.CLUSTER.COMMAND.QUEUE e SYSTEM.CLUSTER.REPOSITORY.QUEUE QUEUE.

Tuttavia, è importante considerare il punto "7" a pagina 164 in *Regolazione delle caratteristiche del pool di buffer* se deve essere utilizzato un numero elevato di canali o un cluster.

Utilizzare i restanti tre pool di buffer per i messaggi utente.

Pool di buffer 1
Utilizzare per importanti messaggi di lunga durata.

I messaggi di lunga durata sono quelli che rimangono nel sistema per più di due checkpoint, a quel punto vengono scritti nella serie di pagine. Se si dispone di molti messaggi di lunga durata, questo pool di buffer dovrebbe essere relativamente piccolo, in modo che l'I/O della serie di pagine sia distribuito in modo uniforme (i messaggi più vecchi vengono scritti in DASD ogni volta che il pool di buffer diventa pieno all ' 85%).

Se il pool di buffer è troppo grande e il pool di buffer non raggiunge mai l'85% di riempimento, l'I/O della serie di pagine viene ritardato fino all'elaborazione del punto di controllo. Ciò potrebbe influire sui tempi di risposta in tutto il sistema.

Se si prevedono solo pochi messaggi di lunga durata, definire questo pool di buffer in modo che sia sufficientemente grande da contenere tutti questi messaggi.

Pool di buffer 2
Utilizzare per messaggi di breve durata, critici per le prestazioni.

Esiste normalmente un elevato grado di riutilizzo del buffer, utilizzando pochi buffer. Tuttavia, è necessario rendere questo pool di buffer grande per consentire un accumulo di messaggi non previsto, ad esempio, quando un'applicazione server ha esito negativo.

Pool di buffer 3
Utilizzare per tutti gli altri messaggi (generalmente, non critici per le prestazioni).

Code come la coda di messaggi non recapitabili, SYSTEM.COMMAND.* e SYSTEM.ADMIN.* le code possono essere associate anche al bufferpool 3.

Dove esistono vincoli di memoria virtuale e i pool di buffer devono essere più piccoli, il pool di buffer 3 è il primo candidato per la riduzione della dimensione.

Potrebbe essere necessario definire ulteriori pool di buffer nelle seguenti circostanze:

- Se una particolare coda è nota per richiedere l'isolamento, forse perché mostra un comportamento diverso in vari momenti.
  - Una coda di questo tipo potrebbe richiedere le migliori prestazioni possibili nelle diverse circostanze o deve essere isolata in modo che non influisca negativamente sulle altre code in un pool di buffer.
  - Ogni coda di questo tipo può essere isolata nel proprio pool di buffer e serie di pagine.
- Si desidera isolare diverse serie di code l'una dall'altra per motivi di classe di servizio.
  - Ogni serie di code potrebbe quindi richiedere uno o entrambi i due tipi di pool di buffer 1 o 2, come descritto in Definizioni suggerite per le impostazioni del pool di buffer, richiedendo la creazione di diversi pool di buffer di un tipo specifico.

Decidere le impostazioni per ciascun pool di buffer

Se si utilizzano i quattro pool di buffer descritti in "Decidere il numero di pool di buffer da definire" a pagina 161, Definizioni consigliate per le impostazioni del pool di buffer fornisce due serie di valori per la dimensione dei pool di buffer.

Il primo set è adatto per un sistema di test, l'altro per un sistema di produzione o un sistema che alla fine diventerà un sistema di produzione. In tutti i casi, definire i pool di buffer con l'attributo **LOCATION**(*SOPRA*)

Tabella 21. Definizioni suggerite per le impostazioni del pool di buffer		
Impostazione definizione	**Sistema di test**	**Sistema di produzione**
BUFFERPOOL 0	1 050 buffer	50 000 buffer
BUFFPOOL 1	1 050 buffer	20 000 buffer
BUFFPOOL 2	1 050 buffer	50 000 buffer
BUFFPOOL 3	1 050 buffer	20 000 buffer

Se sono necessari più dei quattro pool di buffer suggeriti, selezionare il pool di buffer (1 o 2) che descrive più accuratamente il funzionamento previsto delle code nel pool di buffer e ridimensionarlo utilizzando le informazioni in Definizioni suggerite per le impostazioni del pool di buffer.

Assicurarsi che MEMLIMIT sia impostato su un valore sufficientemente elevato, in modo che tutti i pool di buffer possano essere posizionati sopra la barra.

Monitorare le prestazioni dei pool di buffer sotto il carico previsto

È possibile monitorare l'utilizzo dei pool di buffer analizzando le statistiche sulle prestazioni del pool di buffer. In particolare, è necessario assicurarsi che i pool di buffer siano sufficientemente grandi in modo che i valori di QPSTSOS, QPSTLA e QPSTDMC rimangano su zero.

Per ulteriori informazioni, consultare Buffer manager data records.

Regola caratteristiche del pool di buffer

Utilizzare i seguenti punti per modificare le impostazioni del pool di buffer da “Decidere le impostazioni per ciascun pool di buffer” a pagina 162, se necessario.

Utilizzare le statistiche delle prestazioni da “Monitorare le prestazioni dei pool di buffer sotto il carico previsto” a pagina 163 come guida.

1. Se stai migrando da una versione precedente di IBM MQ, modifica le tue impostazioni esistenti solo se hai più spazio di archiviazione reale disponibile.
2. In generale, i pool di buffer più grandi sono migliori per le prestazioni e i pool di buffer possono essere molto più grandi se sono al di sopra della barra.

   Tuttavia, in ogni momento è necessario disporre di memoria reale sufficiente in modo che i pool di buffer siano residenti nella memoria reale. È meglio avere pool di buffer più piccoli che non risultano nella paginazione, rispetto a quelli più grandi che lo fanno.

   Inoltre, non ha senso avere un pool di buffer più grande della dimensione totale delle serie di pagine che lo utilizzano, anche se è necessario prendere in considerazione l'espansione della serie di pagine se è probabile che si verifichi.
3. Puntare ad una serie di pagine per pool di buffer, in quanto ciò fornisce un migliore isolamento dell'applicazione.
4. Se si dispone di memoria reale sufficiente, in modo che i pool di buffer non vengano mai scaricati dal sistema operativo, prendere in considerazione l'utilizzo di buffer fissi per pagina nel pool di buffer.

   Ciò è particolarmente importante se è probabile che il pool di buffer subisca molte operazioni di I/O, in quanto consente di risparmiare il costo CPU associato alla correzione della pagina dei buffer prima delle operazioni di I/O e annullando la correzione della pagina in seguito.
5. Ci sono diversi vantaggi nell'individuare i pool di buffer al di sopra della barra anche se sono abbastanza piccoli da adattarsi al di sotto della barra. Essi sono:
   - Limitazione dello storage virtuale a 31 bit - ad esempio più spazio per lo storage comune.
   - Se la dimensione di un pool di buffer deve essere aumentata inaspettatamente mentre viene utilizzato in modo intensivo, l'impatto e il rischio per il gestore code e il relativo carico di lavoro

sono minori, aggiungendo più buffer a un pool di buffer che è già al di sopra della barra, rispetto allo spostamento del pool di buffer al di sopra della barra e all'aggiunta di ulteriori buffer.

6. Ottimizzare il pool di buffer zero e il pool di buffer per i messaggi di breve durata (pool di buffer 2) in modo che la soglia libera del 15% non venga mai superata (ovvero, QPSTCBSL diviso per QPSTNBUF è sempre maggiore del 15%). Se più del 15% dei buffer rimane libero, l'I/O alle serie di pagine che utilizzano questi pool di buffer può essere ampiamente evitato durante il normale funzionamento, anche se i messaggi più vecchi di due checkpoint vengono scritti nelle serie di pagine.

   Attenzione: Il valore ottimale per questi parametri dipende dalle caratteristiche del singolo sistema. I valori forniti sono intesi solo come linee guida e potrebbero non essere appropriati per il sistema.

7. SYSTEM.* code molto profonde, ad esempio SYSTEM.CHANNEL.SYNCQ, potrebbe trarre vantaggio dall'essere collocato nel proprio pool di buffer, se è disponibile memoria sufficiente.

IBM MQ SupportPac MP16 -IBMMQ perz/OS Pianificazione e ottimizzazione della capacità fornisce ulteriori informazioni sull'ottimizzazione dei pool di buffer.

z/OS Pianificazione dell'ambiente di registrazione

Utilizzare questo argomento per pianificare numero, dimensione e posizione dei log e degli archivi di log utilizzati da IBM MQ.

I log vengono utilizzati per:

- Scrivere le informazioni di ripristino sui messaggi persistenti
- Registrare le informazioni sulle unità di lavoro utilizzando i messaggi persistenti
- Registrare le informazioni sulle modifiche agli oggetti, ad esempio definire la coda
- Strutture CF di backup

e per altre informazioni interne.

L'ambiente di log IBM MQ viene stabilito utilizzando le macro dei parametri di sistema per specificare le opzioni, come ad esempio: se disporre di log attivi singoli o doppi, quale supporto utilizzare per i volumi di log di archivio e quanti buffer di log devono avere.

Queste macro sono descritte in Creazione dei dataset bootstrap e log e in Modulo dei parametri di sistema.

Nota: Se si utilizzano gruppi di condivisione code, assicurarsi di definire i dataset bootstrap e log con SHAREOPTIONS (2 3).

Questa sezione contiene informazioni sui seguenti argomenti:

z/OS *Definizioni dataset di log*

Utilizzare questo argomento per decidere la configurazione più appropriata per i dataset di log.

Questo argomento contiene informazioni che consentono di rispondere alle domande seguenti:

- L'installazione deve utilizzare la registrazione singola o doppia?
- Quanti dataset di log attivi sono necessari?
- “Quanto devono essere grandi i log attivi?” a pagina 166
- Posizionamento log attivo
- “Codifica del log attivo con la codifica del dataset z/OS” a pagina 167

L'installazione deve utilizzare la registrazione singola o doppia?

In generale, è necessario utilizzare la registrazione doppia per la produzione, per ridurre il rischio di perdita di dati. Se si desidera che il sistema di test rifletta la produzione, entrambi devono utilizzare la registrazione doppia, altrimenti i sistemi di test possono utilizzare la registrazione singola.

Con i singoli dati di registrazione vengono scritti in una serie di dataset di log. Con la doppia registrazione i dati vengono scritti in due serie di dataset di log, quindi in caso di problemi con un dataset di log, come ad esempio l'eliminazione accidentale del dataset, è possibile utilizzare il dataset equivalente nell'altro insieme di log per recuperare i dati.

Con la registrazione doppia è necessario il doppio di DASD rispetto alla registrazione singola.

Se si utilizza la doppia registrazione, utilizzare anche i BSDS doppi e la doppia archiviazione per garantire un adeguato provisioning per il recupero dei dati.

La doppia registrazione attiva aggiunge un piccolo costo di prestazioni.

Attenzione: L'utilizzo delle tecnologie di mirroring disco, come Metro Mirror, non è necessariamente una sostituzione per la registrazione doppia e BSDS duale. Se un dataset sottoposto a mirroring viene eliminato accidentalmente, entrambe le copie vengono perse.

Se si utilizzano i messaggi persistenti, la registrazione singola può aumentare la capacità massima del 10-30% e può anche migliorare i tempi di risposta.

La registrazione singola utilizza 2-310 dataset di log attivi, mentre la registrazione doppia utilizza 4-620 dataset di log attivi per fornire lo stesso numero di log attivi. Pertanto, la registrazione singola riduce la quantità di dati registrati, il che potrebbe essere importante se l'installazione è vincolata all'I/O.

Quanti dataset di log attivi sono necessari?

Il numero di log dipende dalle attività del gestore code. Per un sistema di test con bassa velocità di trasmissione, potrebbero essere adatti tre dataset di log attivi. Per un sistema di produzione ad alta velocità di trasmissione si potrebbe desiderare il numero massimo di log disponibili, quindi, se si verifica un problema con lo scaricamento dei log, si ha più tempo per risolvere i problemi.

È necessario disporre di almeno tre dataset di log attivi, ma è preferibile definirne altri. Ad esempio, se il tempo impiegato per riempire un log si avvicina al tempo impiegato per archiviare un log durante il carico di picco, definire ulteriori log.

Nota: Le serie di pagine e i dataset di log attivi sono idonei a risiedere nello spazio di indirizzamento esteso (EAS) parte di un EAV (extended address volumes) e anche un dataset di log di archivio può risiedere nell'EAS.

È inoltre necessario definire più log per compensare i possibili ritardi nell'archiviazione dei log. Se si utilizzano i log di archivio su nastro, attendere il tempo richiesto per montare il nastro.

Considerare la possibilità di avere spazio di log attivo sufficiente per conservare un giorno di dati, nel caso in cui il sistema non sia in grado di archiviare a causa della mancanza di DASD o perché non è in grado di scrivere su nastro. Se tutti i log attivi si riempiono, IBM MQ non è in grado di elaborare le transazioni o i messaggi persistenti. È molto importante disporre di spazio di log attivo sufficiente.

È possibile definire dinamicamente nuovi dataset di log attivi come un modo per ridurre al minimo l'effetto dei ritardi o dei problemi di archiviazione. I nuovi dataset possono essere portati in linea rapidamente, utilizzando il comando **DEFINE LOG** per evitare il 'stallo' del gestore code dovuto a mancanza di spazio nel log attivo.

Se si desidera definire più di 31 dataset di log attivi, è necessario configurare l'ambiente di registrazione per utilizzare un formato BSDS della versione 2. Una volta in uso un formato BSDS della versione 2, è possibile definire fino a 310 dataset di log attivi per ciascun anello di copia di log. Consultare “Pianificazione per aumentare l'intervallo di log indirizzabile massimo” a pagina 174 per informazioni su come convertire in un formato BSDS versione 2.

È possibile determinare se il gestore code sta utilizzando un BSDS versione 2 o superiore, eseguendo il programma di utilità di mappa del log di stampa (CSQJU004) o dal messaggio CSQJ034I emesso durante l'inizializzazione del gestore code. Una fine dell'intervallo RBA di log di FFFFFFFFFFFFFFFF, nel

messaggio CSQJ034I , indica che è in uso un formato BSDS versione 2 o superiore. Una fine dell'intervallo RBA del log 0000FFFFFFFFFFFF, nel messaggio CSQJ034I , indica che è in uso un formato BSDS versione 1.

Quando un gestore code utilizza un formato BSDS versione 2, o superiore, è possibile utilizzare il comando **DEFINE LOG** per aggiungere dinamicamente più di 31 dataset di log attivi a un ring di copia di log.

Quanto devono essere grandi i log attivi?

Da IBM MQ 8.0, la dimensione massima del log attivo supportato, durante l'archiviazione su disco, è 4 GB. Nei rilasci precedenti del prodotto, la dimensione massima del log attivo supportato durante l'archiviazione su disco è di 3 GB.

Durante l'archiviazione su nastro la dimensione massima del log attivo è di 4 GB.

È necessario creare log attivi di almeno 1 GB di dimensione per i sistemi di produzione e test.

Importante: È necessario prestare attenzione durante l'assegnazione dei dataset, poiché IDCAMS arrotonda per eccesso la dimensione assegnata.

Per assegnare un log da 3 GB specificare una delle seguenti opzioni:

- Cilindri (4369)
- Megabyte (3071)
- TRACCE (65535)
- RECORD (786420)

Uno di questi alloca 2.99995 GB.

Per assegnare un log 4GB specificare una delle seguenti opzioni:

- Cilindri (5825)
- Megabyte (4095)
- TRACCE (87375)
- RECORD (1048500)

Uno di questi alloca 3.9997 GB.

Quando si utilizzano dataset con striping, dove il dataset è distribuito su più volumi, il valore della dimensione specificato viene assegnato su ciascun volume DASD utilizzato per lo striping. Quindi, se si desidera utilizzare 4 GB di log e quattro volumi per lo striping, è necessario specificare:

- CYLinders (1456)
- Megabyte (1023)

L'impostazione di questi attributi assegna 4 * 1456 = 5824 Cilindri o 4 * 1023 = 4092 Megabyte.

Nota: Lo striping è supportato quando si utilizzano dataset in formato esteso. Questo è di solito impostato dallo Storage Manager.

Consultare Aumento della dimensione del log attivo per informazioni sull'esecuzione della procedura.

Posizionamento log attivo

È necessario lavorare con il team di gestione della memoria per impostare i pool di memoria per i gestori code. È necessario considerare:

- Una convenzione di denominazione, per cui i gestori code utilizzano le definizioni SMS corrette.
- Spazio richiesto per i log attivi e di archivio. Il pool di memoria deve avere spazio sufficiente per i log attivi da un giorno intero.

- Prestazioni e resilienza ai guasti.

Per motivi legati alle prestazioni, è consigliabile eseguire lo striping dei dataset di log attivi. L'I/O è distribuito su più volumi e riduce i tempi di risposta I/O, aumentando la velocità di trasmissione. Consultare il testo precedente per informazioni sull'allocazione della dimensione dei log attivi quando si utilizza lo striping.

È necessario esaminare le statistiche I/O utilizzando i report di RMF o di un prodotto simile. Eseguire l'analisi di queste statistiche mensilmente (o più frequentemente) per i dataset IBM MQ , per assicurarsi che non vi siano ritardi dovuti all'ubicazione dei dataset.

In alcune situazioni, è possibile che vi siano molte serie di pagine I/O IBM MQ e ciò può influire sulle prestazioni del log IBM MQ se si trovano sullo stesso DASD.

Se si utilizza la registrazione doppia, assicurarsi che ogni serie di log attivi e di archivio sia tenuta separata. Ad esempio, assegnarli su sottosistemi DASD separati o su unità differenti.

Ciò riduce il rischio di perdita di entrambi se uno dei volumi è danneggiato o distrutto. Se entrambe le copie del log vengono perse, la probabilità di perdita di dati è elevata.

Quando si creano nuovi dati di log attivi, è necessario preformattarli utilizzando CSQJUFMT. Se il log non è preformattato, il gestore code lo formatta la prima volta che viene utilizzato, il che influisce sulle prestazioni.

Con un DASD più vecchio con dischi di rotazione di grandi dimensioni, è stato necessario fare attenzione a quali volumi sono stati utilizzati per ottenere le prestazioni migliori.

Con il DASD moderno, in cui i dati sono distribuiti su molti dischi di dimensioni PC, non è necessario preoccuparsi così tanto di quali volumi vengono utilizzati.

Il gestore memoria deve controllare il DASD aziendale per esaminare e risolvere eventuali problemi di prestazioni. Per la disponibilità, è possibile utilizzare una serie di log su un sottosistema DASD e i log doppi su un sottosistema DASD differente.

Codifica del log attivo con la codifica del dataset z/OS

È possibile applicare la funzione di codifica del dataset z/OS ai dataset di log attivi per i gestori code in esecuzione su IBM MQ for z/OS 9.1.4 o versioni successive.

È necessario assegnare questi dataset di log attivi con attributi EXTENDED e un'etichetta della chiave del dataset che garantisca che i dati siano codificati AES.

Consultare la sezione, Riservatezza per i dati inattivi su IBM MQ for z/OS con la crittografia del dataset. per ulteriori informazioni.

z/OS *Utilizzo di MetroMirror con IBM MQ*

IBM Metro Mirror, precedentemente noto come PPRC (Synchronous Peer to Peer Remote Copy), è una soluzione di replica sincrona tra due sottosistemi di memoria, dove le operazioni di scrittura vengono completate sui volumi primari e secondari prima che l'operazione di scrittura venga considerata completa. Metro Mirror può essere utilizzato in ambienti che non richiedono alcuna perdita di dati in caso di errore di un sottosistema di archiviazione.

Tipi di dataset supportati

Tutti i seguenti tipi di dataset IBM MQ possono essere replicati utilizzando Metro Mirror. Tuttavia, esattamente quelli replicati dipendono dai requisiti di disponibilità della propria azienda:

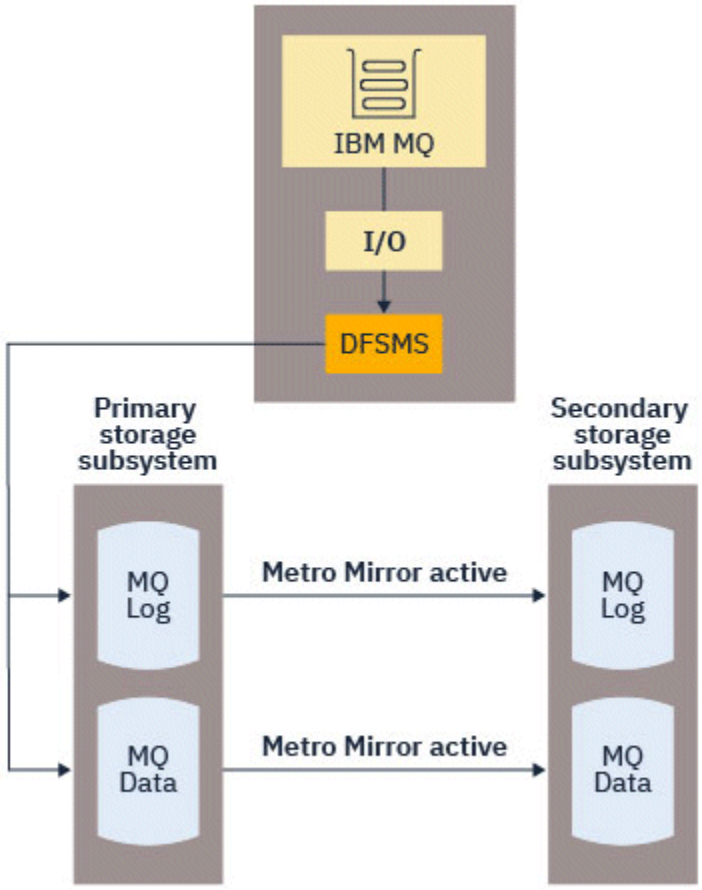
- Log attivi
- Archivia log
- bootstrap data set (BSDS)
- Set di pagine
- SDS (Shared Message Data Set)

- Dataset utilizzati per la configurazione, ad esempio, nelle schede CSQINP* DD sul JCL MSTR

Utilizzo di zHyperWrite with IBM MQ active logs

Quando viene eseguita una scrittura su un dataset replicato utilizzando Metro Mirror, la scrittura viene eseguita prima nel volume primario e quindi replicata sul volume secondario. Questa replica viene eseguita dal sottosistema di memoria ed è trasparente all'applicazione che ha emesso la scrittura, ad esempio IBM MQ.

Questo processo è illustrato nel seguente diagramma.

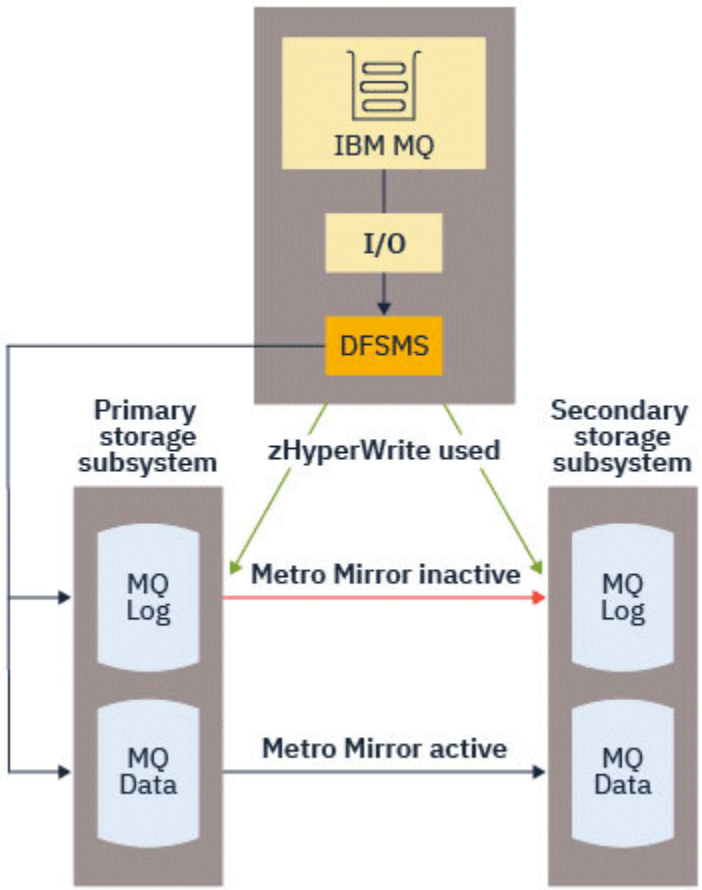


Poiché entrambe le scritture sui sottosistemi di archiviazione primario e secondario devono essere completate prima che la scrittura ritorni a IBM MQ, l'uso di Metro Mirror può avere un impatto sulle prestazioni. È necessario bilanciare questo impatto sulle prestazioni rispetto ai vantaggi di disponibilità dell'uso di Metro Mirror.

I log attivi di IBM MQ sono più sensibili all'impatto sulle prestazioni dell'utilizzo di Metro Mirror. IBM MQ consente di utilizzare la scrittura zHypercon i log attivi per ridurre questo impatto sulle prestazioni.

zHyperWrite è una tecnologia del sottosistema di archiviazione che funziona con z/OS per ridurre l'impatto sulle prestazioni delle scritture effettuate nei dataset replicati utilizzando Metro Mirror. Quando viene utilizzata la scrittura zHyper, la scrittura sui volumi primario e secondario viene emessa in parallelo al livello Data Facility Storage Management Subsystem (DFSMS), invece che in modo sequenziale al livello del sottosistema di memoria, riducendo così l'impatto sulle prestazioni.

Il seguente diagramma illustra l'utilizzo di zHyperWrite per i log attivi e l'utilizzo di Metro Mirror per altri tipi di dataset IBM MQ . Tenere presente che se una scrittura zHyperha esito negativo, DFSMS riemetterà in modo trasparente la scrittura utilizzando Metro Mirror.



zHyperWrite on IBM MQ, è supportato solo sui dataset di log attivi.

Per utilizzare zHyperWrite con i log attivi, devi:

- Configurare IBM MQ per utilizzare zHyperWrite e
- I log attivi devono essere su volumi con capacità di scrittura zHyper

Puoi configurare IBM MQ per utilizzare zHyperWrite utilizzando uno dei seguenti metodi:

- Specificare ZHYWRITE(YES) nel modulo dei parametri di sistema.
- Immettere il comando SET LOG ZHYWRITE(YES).

Impostare le seguenti condizioni per i dataset di log attivi sui volumi con capacità di scrittura zHyper:

- Abilitare i volumi per Metro Mirrore i volumi supportano la scrittura zHyper
- Verificare che i volumi siano abilitati per HyperSwap
- Specificare HYPERWRITE=YES nel parametro IECIOSxx

V 9.3.5 Prima di IBM MQ 9.3.5, se vengono soddisfatte tutte le condizioni precedenti, le scritture nei log attivi sono abilitate per la scrittura zHyper. Se una o più di queste condizioni non vengono soddisfatte, IBM MQ scrive nei log attivi normalmente e Metro Mirror replica le scritture, se configurate.

V 9.3.5 Da IBM MQ 9.3.5, se viene specificato ZHYWRITE (YES), IBM MQ tenta sempre di utilizzare la scrittura zHyperdurante la scrittura nei log attivi, indipendentemente dal fatto che i log si trovino su volumi con capacità di scrittura zHyper. Se i log non si trovano su volumi con capacità di scrittura zHyper, Metro Mirror replica le scritture, se configurate. Non ci sono effetti negativi nel tentativo di utilizzare la scrittura zHyperse i log non si trovano su volumi con capacità di scrittura zHyper

Note:

- IBM MQ non richiede che tutti i dataset di log attivi siano su volumi con capacità di scrittura zHyper.

  Se IBM MQ rileva che alcuni dataset di log attivi si trovano su volumi con capacità di scrittura zHypere altri no, emette il messaggio CSQJ166E e continua l'elaborazione.
- IBM MQ verifica se i dataset di log attivi sono zHypercon capacità di scrittura quando i dataset vengono aperti per la prima volta.

  I dataset di log vengono aperti all'avvio del gestore code o quando vengono aggiunti in modo dinamico utilizzando il comando DEFINE LOG. Se i dataset di log sono resi zHypercon capacità di scrittura mentre un gestore code li ha aperti, il gestore code non li rileverà fino a quando non verrà riavviato.

È possibile utilizzare l'output del comando DISPLAY LOG per indicare se i dataset di log attivi correnti sono con capacità di scrittura zHyper. Il seguente esempio mostra che entrambi i dataset sono con capacità di scrittura zHyper. Se il gestore code è stato configurato con ZHYWRITE (YES), le scritture su questi log saranno abilitate per la scrittura zHyper:

```
Copy %Full zHyperWrite DSName
 1      4  CAPABLE     MQTST.SUBSYS.MQDL.LOGCOPY1.DS001
 2      4  CAPABLE     MQTST.SUBSYS.MQDL.LOGCOPY2.DS001
```

z/OS *Pianificazione della memoria dell'archivio di log*

Utilizzare questo argomento per comprendere i diversi modi di gestione dei dataset di log di archivio.

È possibile collocare i dataset di log di archiviazione su nastri con etichetta standard o DASD ed è possibile gestirli mediante DFHSM (Data Facility Hierarchical Storage Manager). Ogni record logico z/OS in un dataset di log di archiviazione è un intervallo di controllo VSAM dal dataset di log attivo. La dimensione del blocco è un multiplo di 4 KB.

I dataset di log di archivio vengono assegnati in modo dinamico, con nomi scelti da IBM MQ. Il prefisso del nome dataset, la dimensione blocco, il nome unità e le dimensioni DASD necessarie per tale assegnazione sono specificati nel modulo del parametro di sistema. È inoltre possibile scegliere, in fase di installazione, di fare in modo che IBM MQ aggiunga una data e un'ora al nome del dataset del log di archivio.

Non è possibile specificare con IBM MQ, volumi specifici per i nuovi log di archivio, ma è possibile utilizzare le routine di gestione della memoria per gestirli. Se si verificano errori di allocazione, l'offload viene posticipato fino al successivo avvio dell'offload.

Se si specificano i log di archiviazione doppi al momento dell'installazione, ogni intervallo di controllo log richiamato dal log attivo viene scritto in due dataset di log di archiviazione. I record di log contenuti nella coppia di dataset di log di archivio sono identici, ma i punti di fine volume non sono sincronizzati per i dataset multivolume.

I log di archivio devono risiedere su nastro o DASD?

Quando si decide se utilizzare il nastro o DASD per i log di archivio, è necessario considerare una serie di fattori:

- Rivedere le procedure operative prima di decidere su nastro o disco. Ad esempio, se si sceglie di archiviare su nastro, è necessario che vi sia un'unità nastro sufficiente quando sono richieste. Dopo una situazione di emergenza, tutti i sottosistemi potrebbero richiedere unità nastro e l'utente potrebbe non disporre di un numero di unità nastro libere pari a quello previsto.
- Durante il ripristino, le registrazioni di archivio su nastro sono disponibili non appena il nastro viene montato. Se sono stati utilizzati archivi DASD e i dataset sono stati migrati su nastro utilizzando HSM (hierarchical storage manager), si verifica un ritardo mentre HSM richiama ciascun dataset su disco. È possibile richiamare i dataset prima di utilizzare il log di archivio. Tuttavia, non è sempre possibile prevedere l'ordine corretto in cui sono richiesti.
- Quando si utilizzano i log di archivio su DASD, se sono richiesti molti log (come nel caso del ripristino di una serie di pagine dopo un ripristino da un backup) potrebbe essere necessaria una quantità significativa di DASD per contenere tutti i log di archivio.

- In un sistema a basso utilizzo o in un sistema di test, potrebbe essere più conveniente disporre di log di archivio su DASD per eliminare la necessità di montaggi nastro.
- Sia emettendo un comando RECOVER CFSTRUCT che eseguendo il backout di un'unità di lavoro persistente, il log viene letto all'indietro. Le unità nastro con compressione hardware vengono eseguite in modo non corretto sulle operazioni di lettura all'indietro. Pianificare dati di log sufficienti su DASD per evitare la lettura all'indietro dal nastro.

L'archiviazione su DASD offre una recuperabilità più rapida, ma è più costosa dell'archiviazione su nastro. Se si utilizza la registrazione doppia, è possibile specificare che la copia principale del log di archiviazione vada nella DASD e la copia secondaria vada su nastro. Ciò aumenta la velocità di ripristino senza utilizzare la stessa quantità di DASD ed è possibile utilizzare il nastro come backup.

Consultare “Modifica del supporto di memorizzazione per i log di archiviazione” a pagina 172 per dettagli su come archiviare i log da nastro a DASD e su come eseguire il processo inverso.

Archiviazione su nastro

Se si sceglie di archiviare su un'unità nastro, IBM MQ può estendersi fino a un massimo di 20 volumi.

Se si sta considerando di modificare la dimensione del dataset di log attivo in modo che la serie si adatti a un volume nastro, tenere presente che una copia di BSDS viene posizionata sullo stesso volume nastro della copia del dataset di log attivo. Regolare la dimensione del dataset del log attivo verso il basso per scostare lo spazio richiesto per il BSDS sul volume nastro.

Se si utilizzano i log di archivio duali su nastro, è tipico che una copia venga conservata localmente e l'altra copia venga conservata offsite per essere utilizzata nel ripristino di emergenza.

Archiviazione su volumi DASD

IBM MQ richiede che vengano catalogati tutti i dataset di log di archivio assegnati su unità non nastro (DASD). Se si sceglie di archiviare in DASD, il parametro CATALOG della macro CSQ6ARVP deve essere YES. Se questo parametro è NO e si decide di posizionare i dataset di log di archiviazione su DASD, si riceve il messaggio CSQJ072E ogni volta che viene assegnato un dataset di log di archivio, anche se IBM MQ cataloga ancora il dataset.

Se il dataset del log di archivio è conservato su DASD, i dataset del log di archiviazione possono estendersi ad un altro volume; è supportato il multivolume.

Se si sceglie di utilizzare DASD, assicurarsi che l'assegnazione dello spazio primario (sia la quantità che la dimensione del blocco) sia sufficientemente grande da contenere i dati provenienti dal dataset del log attivo o dal BSDS corrispondente, qualunque sia il più grande dei due.

Ciò riduce al minimo la possibilità di codici di interruzione z/OS X'B37' o X'E37' indesiderati durante il processo di offload. L'allocazione dello spazio primario è impostata con il parametro PRIQTY (quantità primaria) della macro CSQ6ARVP .

I dataset di log di archiviazione possono esistere su dataset sequenziali di grandi dimensioni o di formato esteso. Le routine SMS ACS ora utilizzano DSNTYPE (LARGE) o DSNTYPE (EXT).

IBM MQ supporta l'allocazione dei log di archivio come dataset in formato esteso. Quando viene utilizzato il formato esteso, la dimensione massima del log di archivio viene aumentata da 65535 tracce alla dimensione massima del log attivo di 4GB. I log di archivio sono idonei per l'allocazione nello spazio di indirizzamento esteso (EAS) dei volumi di indirizzo esteso (EAV).

Quando sono disponibili i livelli hardware e software richiesti, l'allocazione dei log di archiviazione a una classe di dati definita con COMPACTION utilizzando zEDC potrebbe ridurre la memoria su disco richiesta per conservare i log di archiviazione. Per ulteriori informazioni, consultare IBM MQ for z/OS: Ridurre l'occupazione dello storage con IBM zEnterprise Data Compression (zEDC) e zEnterprise Data Compression (zEDC) .

La funzione di codifica del dataset z/OS può essere applicata ai log di archivio per gestori code in esecuzione su IBM MQ. Questi log di archivio devono essere assegnati tramite le routine ACS

(Automatic Class Selection) a una classe di dati definita con attributi EXTENDED e un'etichetta della chiave del dataset che garantisce la codifica AES dei dati.

Utilizzo di SMS con dataset di log di archivio

Se è installato il sottosistema di gestione memoria MVS/DFP (DFSMS), è possibile scrivere un filtro di uscita utente ACS (Automatic Class Selection) per i data set dei log di archivio, che consente di convertirli per l'ambiente SMS.

Tale filtro, ad esempio, può instradare l'output a un dataset DASD, che può essere gestito da DFSMS . È necessario prestare attenzione se si utilizza un filtro ACS in questo modo. Poiché SMS richiede che i dataset DASD siano catalogati, è necessario assicurarsi che il campo CATALOG DATA della macro CSQ6ARVP contenga YES. In caso contrario, viene restituito il messaggio CSQJ072E ; tuttavia, il dataset è ancora catalogato da IBM MQ.

Per ulteriori informazioni sui filtri ACS, consultare Data set che DFSMShsm assegna dinamicamente durante l'elaborazione del backup aggregato.

z/OS *Modifica del supporto di memorizzazione per i log di archiviazione*

La procedura per modificare il supporto di memorizzazione utilizzato dai log di archivio.

Informazioni su questa attività

Questa attività descrive come modificare il supporto di memorizzazione utilizzato per i log di archivio, ad esempio il passaggio dall'archiviazione al nastro all'archiviazione nella DASD.

È possibile scegliere come apportare le modifiche:

1. Apportare le modifiche solo utilizzando la macro CSQ6ARVP , in modo che vengano applicate al successivo riavvio del gestore code.
2. Apportare le modifiche utilizzando la macro CSQ6ARVP e in modo dinamico utilizzando il comando SET ARCHIVE . Ciò significa che le modifiche vengono applicate la volta successiva che il gestore code archivia un file di log e persistono dopo il riavvio del gestore code.

Procedura

1. Modifica in modo che i log di archiviazione siano memorizzati su DASD invece che su nastro:
   a) Leggere la sezione “Archiviazione su volumi DASD” a pagina 171 ed esaminare i parametri CSQ6ARVP .
   b) Apportare modifiche ai seguenti parametri in CSQ6ARVP
      - Aggiornare i parametri UNIT e, se necessario, UNIT2 .
      - Aggiornare il parametro BLKSIZE, poiché l'impostazione ottimale per DASD differisce dal nastro.
      - Impostare i parametri PRIQTY e SECQTY in modo che siano abbastanza grandi da contenere il log attivo più grande o BSDS.
      - Impostare il parametro CATALOG su YES.
      - Confermare che l'impostazione ALCUNIT è quella desiderata. Dovresti usare BLK, perché è indipendente dal tipo di dispositivo.
      - Impostare il parametro ARCWTOR su NO se non lo è già.
2. Modifica in modo che le registrazioni di archivio siano memorizzate su nastro invece che su DASD:
   a) Leggere la sezione “Archiviazione su nastro” a pagina 171ed esaminare i parametri di CSQ6ARVP .
   b) Apportare modifiche ai seguenti parametri in CSQ6ARVP:
      - Aggiornare i parametri UNIT e, se necessario, UNIT2 .
      - Aggiornare il parametro BLKSIZE, poiché l'impostazione ottimale per il nastro differisce da DASD.

- Confermare che l'impostazione ALCUNIT è quella desiderata. Dovresti usare BLK, perché è indipendente dal tipo di dispositivo.
- Esaminare l'impostazione del parametro ARCWTOR.

z/OS *Per quanto tempo devo conservare i log di archivio*

Utilizzare le informazioni contenute in questa sezione per pianificare la strategia di backup.

Specificare per quanto tempo i log di archiviazione vengono conservati in giorni, utilizzando il parametro ARCRETN in USING CSQ6ARVP o il comando SET SYSTEM . Dopo questo periodo, i dataset possono essere eliminati da z/OS.

È possibile eliminare manualmente i dataset di log di archivio quando non più necessari.

- Il gestore code potrebbe richiedere i log di archivio per il recupero.

  Il gestore code può conservare solo i 1000 archivi più recenti in BSDS. Quando i log di archiviazione non si trovano in BSDS, non possono essere utilizzati per il recupero e sono utilizzati solo per scopi di controllo, analisi o tipo di ripetizione.
- È possibile conservare i log di archiviazione in modo da poter estrarre le informazioni dai log. Ad esempio, l'estrazione dei messaggi dal log e la revisione dell'ID utente che ha inserito o ottenuto il messaggio.

BSDS contiene informazioni sui log e altre informazioni di ripristino. Questo dataset è una dimensione fissa. Quando il numero di log di archivio raggiunge il valore di MAXARCH in CSQ6LOGPo quando BSDS si riempie, le informazioni sul log di archivio meno recenti vengono sovrascritte.

Esistono programmi di utilità per rimuovere le voci del log di archiviazione da BSDS, ma in generale, il BSDS esegue il wrapping e si sovrappone al record del log di archiviazione più vecchio.

Quando è necessario un log di archiviazione

È necessario eseguire regolarmente il backup delle serie di pagine. La frequenza dei backup determina quali log di archivio sono necessari in caso di perdita di una serie di pagine.

È necessario eseguire regolarmente il backup delle strutture CF. La frequenza dei backup determina quali log di archivio sono necessari in caso di perdita di dati nella struttura CF.

Il log di archivio potrebbe essere necessario per il ripristino. Le seguenti informazioni spiegano quando potrebbe essere necessario il log di archivio, dove si verificano problemi con diverse risorse IBM MQ .

Perdita di una serie di pagine

È necessario recuperare il sistema dal backup e riavviare il gestore code.

Sono necessari i log da quando è stato eseguito il backup e fino a tre dataset di log prima dell'esecuzione del backup.

Tutte le LPAR perdono la connettività a una struttura CF o la struttura non è disponibile

Utilizzare il comando RECOVER CFSTRUCT per ripristinare la struttura.

Il ripristino della struttura richiede i log da tutti i gestori code che hanno eseguito l'accesso alla struttura dall'ultimo backup (indietro al momento in cui è stato eseguito il backup) più il backup della struttura stesso nel log del gestore code che ha eseguito il backup.

Se sono stati eseguiti backup frequenti delle strutture CF, i dati dovrebbero essere nei log attivi e non dovrebbero essere necessari i log di archivio.

Se non è presente alcun backup recente della struttura CF, potrebbe essere necessario archiviare i log.

Nota: Tutti i messaggi non persistenti andranno persi; tutti i messaggi persistenti verranno ricreati effettuando le seguenti attività:

1. Lettura dell'ultimo backup della struttura CF dal log
2. Lettura dei log da tutti i gestori code che hanno utilizzato la struttura

3. Unione degli aggiornamenti dal backup

Ricostruzione della struttura di gestione

Se è necessario ricreare la struttura di gestione, le informazioni vengono lette dall'ultimo punto di controllo del log per ciascun gestore code in QSG.

Se un gestore code non è attivo, un altro gestore code nel QSG legge il log.

Non è necessario archiviare i log.

Perdita di un dataset SMDS

Se si perde un dataset SMDS o il dataset viene danneggiato, il dataset diventa inutilizzabile e lo stato per esso è impostato su NON RIUSCITO. La struttura CF non è stata modificata.

Per ripristinare il data set SMDS, è necessario:

1. Ridefinire il data set SMDS e
2. Ripristinare la struttura CF immettendo il comando RECOVER CFSTRUCT .

   Nota: Tutti i messaggi non persistenti nella struttura CF andranno persi; tutti i messaggi persistenti verranno ripristinati.

Il requisito per i log del gestore code è lo stesso per il recupero da una struttura non disponibile.

z/OS *Pianificazione per aumentare l'intervallo di log indirizzabile massimo*

È possibile incrementare l'intervallo di log indirizzabile massimo configurando il gestore code in modo da utilizzare un RBA (relative byte address) di log più grande.

La dimensione RBA del log è stata aumentata da IBM MQ for z/OS 8.0. Per una panoramica di questa modifica, consultare Indirizzo byte relativo log più grande.

V 9.3.0 I gestori code creati in IBM MQ 9.3.0 o versioni successive, hanno un RBA di log di 8 byte abilitato per impostazione predefinita e, quindi, non richiedono la conversione.

È possibile convertire i gestori code per utilizzare i valori RBA di log a 8 byte in qualsiasi momento. Un gruppo di condivisione code può contenere alcuni gestori code con RBA di log di 8 byte abilitato e alcuni gestori code con RBA di log di 6 byte abilitato.

Annullamento della modifica

Impossibile eseguire il backout della modifica.

Quanto tempo ci vuole?

La modifica richiede un riavvio del gestore code. Arrestare il gestore code, eseguire il programma di utilità CSQJUCNV rispetto al dataset di avvio (BSDS) o ai dataset, per creare nuovi dataset, ridenominare questi dataset di avvio e riavviare il gestore code. L'esecuzione del programma di utilità CSQJUCNV generalmente richiede alcuni secondi.

Che impatto ha tutto questo?

- Con RBA di log a 8 byte in uso, ogni scrittura di dati nei dataset di log ha ulteriori byte. Pertanto, per un carico di lavoro costituito da messaggi persistenti, si verifica un piccolo incremento della quantità di dati scritti nei log.
- I dati scritti in una serie di pagine o in una struttura CF (coupling facility) non vengono influenzati.

Attività correlate

Implementazione dell'indirizzo di byte relativo del log più grande

z/OS Pianificazione dell'iniziatore di canali

L'iniziatore di canali fornisce le comunicazioni tra i gestori code e viene eseguito nel proprio spazio di indirizzo.

Esistono due tipi di connessioni:

1. Connessioni dell'applicazione a un gestore code su una rete. Questi sono noti come canali client.
2. Connessioni gestore code a gestore code. Questi sono noti come canali MCA.

Listener

Un programma listener del canale ascolta le richieste di rete in entrata e avvia il canale appropriato quando tale canale è necessario. Per elaborare le connessioni in entrata, l'iniziatore di canali deve configurare almeno un'attività listener IBM MQ . Un listener può essere un listener TCP o un listener LU 6.2 .

Ogni listener richiede una porta TCP o un nome LU.

Tenere presente che è possibile avere più di un listener per ciascun iniziatore di canali.

TCP/IP

Un iniziatore di canali può operare con più di uno stack TCP sulla stessa immagine z/OS . Ad esempio, uno stack TCP potrebbe essere per le connessioni interne e un altro stack TCP per connessioni esterne.

Quando si definisce un canale di output:

1. Impostare l'host e la porta di destinazione della connessione. Può essere:
   - un indirizzo IP, ad esempio `10.20.4.6`
   - un nome host, ad esempio `mvs-prod.myorg.com`

   Se si utilizza un nome host per specificare la destinazione, IBM MQ utilizza il DNS (Domain Name System) per risolvere l'indirizzo IP della destinazione.
2. Se si utilizzano più stack TCP, è possibile specificare il parametro **LOCLADDR** nella definizione del canale, che indica l'indirizzo dello stack IP da utilizzare.

Dovresti pianificare di avere un server DNS ad alta disponibilità, o server DNS. Se il DNS non è disponibile, i canali in uscita potrebbero non essere in grado di avviarsi e le regole di autenticazione di canale che associano una connessione in entrata utilizzando un nome host non possono essere elaborate.

APPC e LU 6.2

Se si utilizza APPC, l'iniziatore di canali ha bisogno di un nome LU e di una configurazione in APPC.

Gruppi di condivisione code

Per fornire una singola immagine di sistema e consentire a una richiesta di connessione IBM MQ in entrata di andare a qualsiasi gestore code nel gruppo di condivisione code, è necessario eseguire alcune operazioni di configurazione. Ad esempio:

1. Un router di rete hardware. Questo router ha un indirizzo IP visualizzato dall'azienda e può instradare la richiesta iniziale a qualsiasi gestore code connesso a questo hardware.
2. Un indirizzo IP virtuale (VIPA). Viene specificato un indirizzo IP a livello aziendale e tale indirizzo può essere instradato a qualsiasi stack TCP in un sysplex. Lo stack TCP può quindi instradarlo a qualsiasi gestore code in ascolto nel sysplex.

Protezione del traffico IBM MQ

È possibile configurare IBM MQ per utilizzare le connessioni TLS per proteggere i dati sul collegamento. Per utilizzare TLS è necessario utilizzare i certificati digitali e i portachiavi.

È inoltre necessario lavorare con il personale all'estremità remota del canale, per assicurarsi di disporre di definizioni e certificati compatibili IBM MQ .

È possibile controllare le connessioni che possono connettersi a IBM MQ e l'ID utente, in base a

- Indirizzo IP
- ID utente client
- Gestore code remoto o
- Certificato digitale (vedere Record di autenticazione di canale)

È inoltre possibile limitare le applicazioni client verificando che forniscano un ID utente e una password validi (consultare Autenticazione della connessione).

Puoi far funzionare l'iniziatore di canali e quindi configurare ogni canale per utilizzare TLS, uno alla volta.

Monitoraggio dell'iniziatore di canali

Esistono comandi MQSC che forniscono informazioni sull'iniziatore di canali e sui canali:

- Il comando DISPLAY CHINIT fornisce informazioni sull'iniziatore di canali e sui listener attivi.
- Il comando DISPLAY CHSTATUS visualizza l'attività e lo stato di un canale.

L'iniziatore di canali può anche produrre record SMF con informazioni sulle attività dell'iniziatore di canali e sull'attività del canale. Per ulteriori informazioni, consultare “Pianificazione dei dati SMF dell'iniziatore di canali” a pagina 177.

L'iniziatore del canale emette messaggi nella registrazione lavoro quando i canali vengono avviati e arrestati. L'automazione nell'azienda può utilizzare questi messaggi per acquisire lo stato. Poiché alcuni canali sono attivi solo per pochi secondi, è possibile produrre molti messaggi. È possibile eliminare questi messaggi utilizzando la funzione di elaborazione dei messaggi z/OS o impostando **EXCLMSG** con il comando SET SYSTEM .

Configurazione delle tue definizioni di canali IBM MQ

Quando si hanno molti gestori code connessi insieme, può essere difficile gestire tutte le definizioni di oggetto. L'utilizzo del cluster IBM MQ può semplificare questa operazione.

Specificare due gestori code come repository completi. Gli altri gestori code necessitano di una connessione e di una connessione da uno dei repository. Quando sono necessarie connessioni ad altri gestori code, il gestore code crea e avvia i canali automaticamente.

Se si prevede di avere un numero elevato di gestori code in un cluster, è necessario pianificare i gestori code che fungono da repository dedicati e non hanno traffico dell'applicazione.

Per ulteriori informazioni, consultare “Pianificazione delle code e dei cluster distribuiti” a pagina 20.

Azioni prima di configurare l'iniziatore di canali

1. Decidere se si sta utilizzando TCP/IP o APPC.
2. Se si sta utilizzando TCP, assegnare almeno una porta per IBM MQ.
3. Se hai bisogno di un server DNS, configura il server in modo che sia altamente disponibile, se necessario.
4. Se si sta utilizzando APPC, assegnare un nome LU e configurare APPC.

Azioni dopo aver configurato l'iniziatore di canali, prima di entrare in produzione

1. Pianificare le connessioni che si avranno:
   a. Connessioni client da applicazioni remote.
   b. Canali MCA da e verso altri gestori code. In genere si dispone di un canale da e verso ogni gestore code remoto.
2. Configurare il clustering o unire un ambiente di clustering esistente.
3. Considerare se è necessario utilizzare più stack TCP, VIPA o un router esterno per la disponibilità davanti all'iniziatore del canale.
4. Se stai pianificando di utilizzare TLS:
   a. Impostare il keyring
   b. Imposta certificati
5. Se si prevede di utilizzare l'autenticazione di canale:
   a. Decidere i criteri per l'associazione delle sessioni in entrata agli ID utente MCA
   b. Abilitare la ricerca DNS inversa impostando il parametro del gestore code **REVDNS**
   c. Esaminare la sicurezza. Ad esempio, eliminare i canali predefiniti e specificare gli ID utente solo con l'autorizzazione necessaria nell'attributo **MCAUSER** per un canale.
6. Acquisire i record SMF di statistiche e account prodotti dall'iniziatore di canali e elaborarli successivamente.
7. Automatizzare il monitoraggio dei messaggi di log del job.
8. Se necessario, ottimizzare l'ambiente di rete per migliorare la velocità di trasmissione. Con TCP, i buffer di invio e ricezione di grandi dimensioni migliorano la velocità di trasmissione. È possibile forzare MQ ad utilizzare specifiche dimensioni del buffer TCP utilizzando i comandi:

   ```
   RECOVER QMGR(TUNE CHINTCPRBDYNSZ nnnnn)
   RECOVER QMGR(TUNE CHINTCPSBDYNSZ nnnnn)
   ```

   che imposta SO_RCVBUF e SO_SNDBUF per i canali alla dimensione in byte specificata in nnnnn.

Concetti correlati

“Pianificazione per il gestore code” a pagina 146
Quando si configura un gestore code, la pianificazione deve consentire la crescita del gestore code, in modo che il gestore code soddisfi le esigenze dell'azienda.

z/OS Pianificazione dei dati SMF dell'iniziatore di canali

È necessario pianificare l'attuazione della raccolta dei dati SMF per l'iniziatore di canali.

L'iniziatore del canale produce due tipi di record:

- Dati statistici con informazioni sull'iniziatore di canali e sulle attività al suo interno.
- Dati di account del canale con informazioni simili al comando DISPLAY CHSTATUS .

È possibile avviare la raccolta dei dati delle statistiche utilizzando il comando:

```
START TRACE(STAT) CLASS(4)
```

e arrestarlo utilizzando il comando:

```
STOP TRACE(STAT) CLASS(4)
```

Si avvia la raccolta dei dati di account utilizzando il comando:

```
START TRACE(ACCTG) CLASS(4)
```

e arrestarlo utilizzando il comando:

```
STOP TRACE(ACCTG) CLASS(4)
```

È possibile controllare quali canali dispongono di dati di account raccolti per l'utilizzo dell'attributo **STATCHL** nella definizione del canale o nel gestore code.

- Per i canali client, è necessario impostare **STATCHL** a livello di gestore code.
- Per i canali mittente del cluster definiti automaticamente, è possibile controllare la raccolta di dati di account con l'attributo del gestore code **STATACLS** .

Il valore predefinito di **STATCHL** per il gestore code è OFF. Per raccogliere i dati di account del canale, è necessario modificare il valore di **STATCHL** dal valore predefinito sul gestore code o sulla definizione del canale, in aggiunta alla traccia di account della classe 4 iniziale.

I record SMF vengono prodotti quando:

- V 9.3.0 Da IBM MQ for z/OS 9.3.0 in poi, l'intervallo di tempo indicato dai parametri CSQ6SYSP **STATIME** o **ACCTIME** è trascorso oppure, se **STATIME** o **ACCTIME** è zero sul broadcast di raccolta dati SMF. Le richieste per raccogliere i dati SMF per l'iniziatore di canali e il gestore code sono sincronizzate.
- Viene emesso un comando `STOP TRACE(ACCTG) CLASS(4)` o `STOP TRACE(STAT) CLASS(4)` oppure
- L'iniziatore del canale è chiuso. A questo punto, tutti i dati SMF vengono scritti.

Se un canale si arresta durante l'intervallo SMF, i dati di account vengono scritti in SMF la volta successiva che viene eseguita l'elaborazione SMF. Se un client si connette, esegue alcune operazioni e si disconnette, quindi si riconnette e si disconnette, vengono prodotti due insiemi di dati di contabilità del canale.

I dati statistici normalmente si adattano a un record SMF, tuttavia, è possibile creare più record SMF se è in uso un numero elevato di attività.

I dati di account vengono raccolti per ogni canale per cui è abilitato e normalmente si adattano a un record SMF. Tuttavia, è possibile creare più record SMF se è attivo un numero elevato di canali.

Il costo di raccolta dei dati SMF dell'iniziatore di canali è basso. In genere l'aumento dell'utilizzo della CPU è inferiore a qualche percentuale e spesso rientra nell'errore di misurazione.

Prima di utilizzare questa funzione, è necessario lavorare con il programmatore di sistemi z/OS per garantire che SMF disponga della capacità per i record aggiuntivi e che modifichino i processi di estrazione dei record SMF per includere i nuovi dati SMF.

Per i dati delle statistiche dell'iniziatore di canali, il tipo di record SMF è 115 e il sottotipo 231.

Per i dati di account dell'iniziatore di canali, il tipo di record SMF è 116 e il sottotipo 10.

È possibile scrivere programmi propri per elaborare questi dati oppure utilizzare SupportPac MP1B che contiene un programma, MQSMF, per stampare i dati e creare dati in formato CSV (Comma Separated Values) adatti per l'importazione in un foglio di calcolo.

Se si verificano problemi con l'acquisizione dei dati SMF dell'iniziatore di canali, consultare Gestione dei problemi durante l'acquisizione dei dati SMF per l'iniziatore di canali (CHINIT) per ulteriori informazioni.

Attività correlate

Interpretazione delle statistiche delle prestazioni IBM MQ

Risoluzione dei problemi relativi ai dati di account del canale

z/OS Pianificazione dell'ambiente TCP/IP z/OS

Per ottenere la migliore velocità di trasmissione attraverso la rete, è necessario utilizzare i buffer di invio e ricezione TCP/IP con una dimensione di 64 KB o superiore. Con questa dimensione, il sistema ottimizzerà le dimensioni del buffer.

Vedi Cos' è Dynamic Right Sizing for High Latency Networks? per ulteriori informazioni.

È possibile controllare la propria dimensione del buffer di sistema utilizzando il seguente comando Netstat, ad esempio:

```
TSO NETSTAT ALL (CLIENT csq1CHIN
```

I risultati visualizzano molte informazioni, inclusi i seguenti due valori:

```
ReceiveBufferSize: 0000065536
SendBufferSize: 0000065536
```

65536 è 64 KB. Se le dimensioni del buffer sono inferiori a 65536, è necessario lavorare con il proprio team di rete per incrementare i valori **TCPSENDBFRSIZE** e **TCPRCVBUFRSIZE** in `PROFILE DDName` nella procedura TCPIP. Ad esempio, è possibile utilizzare il seguente comando:

```
TCPCONFIG TCPSENDBFRSZE 65536 TCPRCVBUFRSIZE 65536
```

Se non è possibile modificare le impostazioni del sistema **TCPSENDBFRSIZE** o **TCPRCVBUFRSIZE** , contattare il centro di supporto software IBM .

z/OS Pianificazione del gruppo di condivisione code (QSG)

Il modo più semplice per implementare un ambiente di accodamento condiviso è configurare un gestore code, aggiungere tale gestore code a un QSG, quindi aggiungere altri gestori code al QSG.

Un gruppo di condivisione code utilizza tabelle Db2 per memorizzare le informazioni di configurazione. Esiste una serie di tabelle utilizzate da tutti i QSG che condividono lo stesso gruppo di condivisione dati Db2 .

I messaggi della coda condivisa vengono memorizzati in una struttura in una CF (coupling facility). Ogni QSG ha una propria serie di strutture CF. È necessario configurare le strutture per soddisfare le proprie esigenze.

I messaggi di dimensione superiore a 63KB non possono essere memorizzati nella CF. È necessario utilizzare SMDS (Shared Message Data Sets) o Db2 per questi messaggi.

Profili di messaggi e pianificazione della capacità

È necessario comprendere il profilo dei messaggi della coda condivisa. Di seguito sono riportati esempi di fattori che è necessario considerare:

- Dimensione media e massima dei messaggi
- La grandezza della coda tipica e la grandezza della coda di eccezioni. Ad esempio, potrebbe essere necessaria una capacità sufficiente per conservare i messaggi per un intero giorno e la tipica profondità della coda è inferiore a 100 messaggi.

Se il profilo del messaggio viene modificato, è possibile aumentare la dimensione delle strutture o implementare SMDS in un secondo momento.

Se si desidera essere in grado di gestire un elevato volume di picco di messaggi, è possibile configurare IBM MQ per scaricare i messaggi in SMDS quando l'utilizzo della struttura raggiunge le soglie specificate dall'utente.

È necessario decidere se si desidera eseguire il duplex delle strutture CF. Questo è controllato dalla definizione della struttura CF nella politica CFRM:

1. Una struttura duplex utilizza due CF (coupling facilities). Se si verifica un problema con una CF, non vi è alcuna interruzione del servizio e la struttura può essere ricostruita su una terza CF, se disponibile. Le strutture duplex possono avere un impatto significativo sulle prestazioni delle operazioni sulle code condivise.
2. Se la struttura non è duplex, un problema con la CF significa che le code condivise sulle strutture in tale CF diventeranno non disponibili fino a quando la struttura non potrà essere ricreata in un'altra CF.

   IBM MQ può essere configurato per ricreare automaticamente le strutture in un'altra CF in questo caso. I messaggi persistenti verranno recuperati dai log dei gestori code.

Notare che è facile modificare le definizioni CF.

È possibile definire una struttura in modo che possa contenere solo messaggi non persistenti o messaggi persistenti e non persistenti.

Le strutture che possono contenere messaggi persistenti devono essere sottoposte a backup periodicamente. Esegui il backup delle tue strutture CF almeno ogni ora per ridurre al minimo il tempo necessario per ripristinare la struttura in caso di errore. Il backup viene memorizzato nel dataset di log del gestore code che esegue il backup.

Se si prevede di avere una velocità di trasmissione dei messaggi elevata nelle code condivise, è consigliabile disporre di un gestore code dedicato per eseguire il backup delle strutture CF. In questo modo si riduce il tempo necessario per ripristinare le strutture, poiché è necessario leggere meno dati dai log del gestore code.

Canali

Per fornire una singola immagine di sistema per le applicazioni che si collegano in un IBM MQ QSG, è possibile definire canali di input condivisi. Se questi sono impostati, una connessione in arrivo nell'ambiente del gruppo di condivisione code può andare a qualsiasi gestore code nel QSG.

Potrebbe essere necessario configurare un router di rete o un indirizzo IP virtuale (VIPA) per questi canali.

È possibile definire canali di output condivisi. Un'istanza del canale di output condiviso può essere avviata da qualsiasi gestore code nel QSG.

Per ulteriori informazioni, vedi Canali condivisi .

Sicurezza

Le risorse IBM MQ vengono protette utilizzando un gestore della sicurezza esterno. Se si utilizza RACF, i profili RACF hanno come prefisso il nome del gestore code. Ad esempio, una coda denominata APPLICATION.INPUT viene protetto utilizzando un profilo della classe MQQUEUE denominato `qmgrName.APPLICATION.INPUT.`

Quando si utilizza un gruppo di condivisione code, è possibile continuare a proteggere le risorse con profili prefissati con il nome del gestore code oppure è possibile aggiungere un prefisso ai profili con il nome del gruppo di condivisione code. Ad esempio `qsgName.APPLICATION.INPUT`.

Si consiglia di utilizzare il prefisso dei profili con il nome del gruppo di condivisione code perché ciò significa che esiste una singola definizione per tutti i gestori code, che consente di salvare il lavoro e di evitare una mancata corrispondenza nelle definizioni tra gestori code.

Concetti correlati

“Pianificazione per il gestore code” a pagina 146
Quando si configura un gestore code, la pianificazione deve consentire la crescita del gestore code, in modo che il gestore code soddisfi le esigenze dell'azienda.

z/OS Pianificazione dell'ambiente di storage CF (coupling facility) e offload

Utilizzare questo argomento quando si pianificano le dimensioni e i formati iniziali delle strutture CF (coupling facility), dell'ambiente SMDS (shared message data set) o dell'ambiente Db2 .

Questa sezione contiene informazioni sui seguenti argomenti:

- “Definizione delle risorse CF (Coupling Facility)” a pagina 181
  - Come decidere il meccanismo di storage offload
  - Pianificazione delle strutture
  - Pianificazione della dimensione delle strutture
  - Associazione delle code condivise alle strutture

- “Pianificazione dell'ambiente SMDS (shared message data set)” a pagina 186
- “Pianificazione del tuo ambiente Db2” a pagina 189

Definizione delle risorse CF (Coupling Facility)

Se si intende utilizzare le code condivise, è necessario definire le strutture CF (Coupling Facility) che IBM MQ utilizzerà nella politica CFRM. A tale scopo, è necessario prima aggiornare la politica CFRM con le informazioni sulle strutture, quindi attivare la politica.

L'installazione probabilmente ha una politica CFRM esistente che descrive le CF disponibili. Il programma di utilità per i dati amministrativi viene utilizzato per modificare il contenuto della politica in base alle istruzioni testuali fornite. È necessario aggiungere le istruzioni alla politica che definisce i nomi delle nuove strutture, le CF in cui sono definite e la dimensione delle strutture.

La politica CFRM determina anche se le strutture IBM MQ sono duplex e come vengono riassegnate in scenari di errore. Ripristino della coda condivisa contiene suggerimenti per la configurazione di CFRM per la resilienza agli errori che influiscono sulla CF (Coupling Facility).

Scelta dell'ambiente di memoria offload

I dati del messaggio per le code condivise possono essere scaricati dalla CF (Coupling Facility) e memorizzati in una tabella Db2 o in un dataset gestito IBM MQ denominato SMDS (*shared message data set*). I messaggi che sono troppo grandi per essere memorizzati nella CF (Coupling Facility) (ossia, più grandi di 63 KB) devono sempre essere scaricati e i messaggi più piccoli possono essere scaricati facoltativamente per ridurre l'utilizzo dello spazio CF.

Per ulteriori informazioni, consultare Specifica delle opzioni di offload per i messaggi condivisi.

Pianificazione delle proprie strutture

Un gruppo di condivisione code (QSG) richiede la definizione di almeno due strutture. La prima struttura, nota come struttura di gestione, viene utilizzata per coordinare l'attività interna IBM MQ nel gruppo di condivisione code. Nessun dato utente è contenuto in questa struttura. Ha un nome fisso di *qsg - name*CSQ_ADMIN (dove *qsg - name* è il nome del gruppo di condivisione code). Le strutture successive sono note come strutture dell'applicazione e vengono utilizzate per conservare i messaggi sulle code condivise IBM MQ . Ogni struttura può contenere fino a 512 code condivise.

Per le code di sistema viene utilizzata una struttura dell'applicazione denominata *qsg - name*CSQSYSAPPL. La definizione di questa struttura è facoltativa, ma è necessaria per utilizzare determinate funzioni. Per impostazione predefinita, il SISTEMA SYSTEM.QSG.CHANNEL.SYNCQ e SYSTEM.QSG.UR.RESOLUTION.QUEUE QUEUE sono definite sulla struttura CSQSYAPPL *qsg*.

Utilizzo di più strutture

Un gruppo di condivisione code può connettersi fino a 64 strutture CFS (coupling facility structure). Una di queste strutture deve essere la struttura amministrativa. Se è definito, un'altra di queste strutture potrebbe essere la struttura *qsg - name*CSQSYSAPPL. È possibile utilizzare fino a 63 (62 se è definito *qsg - name*CSQSYSAPPL) strutture per i dati del messaggio. È possibile scegliere di utilizzare più strutture dell'applicazione per uno dei seguenti motivi:

- Si dispone di alcune code che probabilmente contengono un numero elevato di messaggi e quindi richiedono tutte le risorse di un'intera CF (Coupling Facility).
- Si ha un requisito per un numero elevato di code condivise, quindi devono essere suddivise in più strutture poiché ciascuna struttura può contenere solo 512 code.
- I report RMF sulle caratteristiche di utilizzo di una struttura suggeriscono che è necessario distribuire le code contenute in un numero di CF (Coupling Facility).

- Si desidera che alcuni dati della coda vengano conservati in una CF (Coupling Facility) fisicamente diversa da altri dati della coda per motivi di isolamento dei dati.
- Il recupero dei messaggi condivisi persistenti viene eseguito utilizzando gli attributi e comandi del livello di struttura, ad esempio BACKUP CFSTRUCT. Per semplificare il backup e il recupero, è possibile assegnare code che contengono messaggi non persistenti a strutture diverse da quelle che contengono messaggi persistenti.

Quando si scelgono le CF in cui assegnare le strutture, considerare i seguenti punti:

- Requisiti di isolamento dei dati.
- La volatilità della CF (Coupling Facility) (ossia, la sua capacità di preservare i dati attraverso un'interruzione dell'alimentazione).
- Indipendenza non riuscita tra i sistemi di accesso e la CF (coupling facility) o tra le CF (coupling facilities).
- Il livello di CFCC (coupling facility control code) installato sulla CF (IBM MQ richiede il livello 9 o superiore).

Pianificazione delle dimensioni delle strutture

La struttura amministrativa

La struttura di amministrazione (*qsg - name*CSQ_ADMIN) deve essere abbastanza grande da contenere 1000 voci di elenco per ciascun gestore code nel gruppo di condivisione code. Quando si avvia un gestore code, la struttura viene controllata per verificare se è abbastanza grande per il numero di gestori code attualmente *definiti* per il gruppo di condivisione code. I gestori code vengono considerati come definiti nel gruppo di condivisione code se sono stati aggiunti dal programma di utilità CSQ5PQSG . È possibile controllare quali gestori code sono definiti per il gruppo con il comando MQSC DISPLAY GROUP .

Nota: Quando si calcola la dimensione della struttura, è necessario consentire la dimensione di grandi unità di lavoro, oltre al numero di gestori code nel gruppo di condivisione code.

Tabella 22 a pagina 182 mostra la dimensione minima richiesta per la struttura amministrativa per vari numeri di gestori code definiti nel gruppo di condivisione code. Queste dimensioni sono state stabilite per una struttura CFCC di livello 14; per i livelli più elevati di CFCC, probabilmente devono essere più grandi.

Tabella 22. Dimensioni minime della struttura amministrativa

Numero di gestori code definiti nel gruppo di condivisione code	Memoria richiesta
1	6144 KB
2	6912 KB
3	7976 KB
4	8704 KB
5	9728 KB
6	10496 KB
7	11520 KB
8	12288 KB
9	13056 KB
10	14080 KB
11	14848 KB

Tabella 22. Dimensioni minime della struttura amministrativa (Continua)	
Numero di gestori code definiti nel gruppo di condivisione code	**Memoria richiesta**
12	15616 KB
13	16640 KB
14	17408 KB
15	18176 KB
16	19200 KB
17	19968 KB
18	20736 KB
19	21760 KB
20	22528 KB
21	23296 KB
22	24320 KB
23	25088 KB
24	25856 KB
25	27136 KB
26	27904 KB
27	28672 KB
28	29696 KB
29	30464 KB
30	31232 KB
31	32256 KB

Quando si aggiunge un gestore code a un gruppo di condivisione code esistente, il requisito di memoria potrebbe essere aumentato oltre la dimensione consigliata in Tabella 22 a pagina 182. In caso affermativo, utilizzare la seguente procedura per stimare la memoria richiesta per la struttura *qsg* - *name*CSQ_ADMIN:

1. Immettere il comando MQSC **DISPLAY CFSTATUS(CSQ_ADMIN)** su un membro esistente del gruppo di condivisione code.
2. Estrarre le informazioni ENTSMAX per la struttura CSQ_ADMIN.
3. Se questo numero è inferiore a 1000 volte il numero totale di gestori code che si desidera definire nel gruppo di condivisione code, incrementare la dimensione della struttura.

Strutture dell'applicazione

La dimensione delle strutture dell'applicazione richieste per contenere i messaggi IBM MQ dipende dal numero e dalla dimensione probabili dei messaggi da conservare simultaneamente su una struttura.

Il grafico in Figura 42 a pagina 184 mostra quanto è necessario creare le strutture CF per conservare i messaggi nelle code condivise. Per calcolare la dimensione di allocazione sono necessarie le seguenti informazioni:

- La dimensione media dei messaggi nelle code.

- Il numero totale di messaggi che è possibile memorizzare nella struttura.

Individuare il numero di messaggi lungo l'asse orizzontale. Selezionare la curva che corrisponde alla dimensione del messaggio e determinare il valore richiesto dall'asse verticale. Ad esempio, per 200 000 messaggi di lunghezza 1 KB fornisce un valore compreso tra 256 e 512 MB.

Tabella 23 a pagina 184 fornisce le stesse informazioni in formato tabella.

Figura 42. Calcolo della dimensione di una struttura CF (Coupling Facility)

Utilizzare questa tabella per calcolare la dimensione delle strutture CFS:

Tabella 23. Calcolo della dimensione di una struttura CF (Coupling Facility)

Numero di messaggi	**1 kB**	**2 KB**	**4 KB**	**8 KB**	**16 KB**	**32 KB**	**63 KB**
100	6 MB	6 MB	7 MB	7 MB	8 MB	10 MB	14 MB
1000	8 MB	9 MB	12 MB	17 MB	27 MB	48 MB	88 MB
10000	25 MB	38 MB	64 MB	115 MB	218 MB	423 MB	821 MB
100000	199 MB	327 MB	584 MB	1097 MB	2124 MB	4177 MB	8156 MB

La politica CFRM deve includere le seguenti istruzioni:

- `INITSIZE` è la dimensione in KB con cui la struttura viene assegnata quando il primo gestore code si connette ad essa.

- SIZE è la dimensione massima che la struttura può raggiungere.
- FULLTHRESHOLD imposta il valore percentuale della soglia alla quale z/OS emette il messaggio IXC585E per indicare che la struttura si sta riempiendo.

Una procedura ottimale consiste nel garantire che INITSIZE e SIZE si trovino all'interno di un fattore 2. Ad esempio, con le cifre stabilite in precedenza, è possibile includere le seguenti istruzioni:

```
STRUCTURE NAME(structure-name)
INITSIZE(value from graph in KB, that is, multiplied by 1024)
SIZE(something larger)
FULLTHRESHOLD(85)
```

```
STRUCTURE NAME(QSG1APPLICATION1)
INITSIZE(262144) /* 256 MB */
SIZE(524288)     /* 512 MB */
FULLTHRESHOLD(85)
```

Se l'utilizzo della struttura raggiunge la soglia in cui vengono emessi i messaggi di avvertenza, è richiesto l'intervento. È possibile utilizzare IBM MQ per inibire le operazioni MQPUT ad alcune delle code nella struttura per impedire alle applicazioni di scrivere più messaggi, avviare più applicazioni per richiamare i messaggi dalle code o sospendere alcune delle applicazioni che stanno inserendo messaggi nella coda.

In alternativa, è possibile utilizzare le funzioni z/OS per modificare la dimensione della struttura. Il seguente comando z/OS :

```
SETXCF START,ALTER,STRNAME=structure-name,SIZE=newsize
```

modifica la dimensione della struttura in *newsize*, dove *newsize* è un valore inferiore al valore di SIZE specificato nella politica CFRM per la struttura, ma superiore alla dimensione CF corrente.

È possibile monitorare l'utilizzo di una struttura CF (Coupling Facility) con il comando MQSC DISPLAY CFSTATUS .

Se non viene eseguita alcuna azione e una struttura della coda si riempie, viene restituito all'applicazione un codice di ritorno MQRC_STORAGE_MEDIUM_FULL. Se la struttura di amministrazione si riempie, i sintomi esatti dipendono da quali processi riscontrano l'errore, ma potrebbero includere i seguenti problemi:

- Nessuna risposta ai comandi.
- Errore del gestore code a causa di problemi durante l'elaborazione del commit.

La struttura CSQSYSAPPL

La struttura *qsg - name*CSQSYSAPPL è una struttura dell'applicazione per code di sistema. La tabella 3 illustra un esempio di come stimare le dimensioni dei dati dei messaggi per le code predefinite definite nella struttura *qsg - name*CSQSYSAPPL.

Tabella 24. Tabella che mostra l'utilizzo di CSQSYSAPPL rispetto al dimensionamento.

***qsg - name*utilizzo CSQSYSAPPL**	**Dimensionamento**
SYSTEM.QSG.CHANNEL.SYNCQ	2 messaggi di 500 byte per istanza attiva di un canale condiviso
SYSTEM.QSG.UR.RESOLUTION.QUEUE	1000 messaggi di 2 KB

I valori di definizione della struttura iniziale suggeriti sono i seguenti:

```
STRUCTURE NAME(qsg-nameCSQSYSAPPL)
INITSIZE(20480)        /* 20 MB */
SIZE(30720)            /* 30 MB */
FULLTHRESHOLD(85)
```

Questi valori possono essere modificati in base all'uso dei canali condivisi e delle unità di ripristino del gruppo.

Associazione delle code condivise alle strutture

Per definire una struttura dell'applicazione in IBM MQ, utilizzare il comando DEFINE CFSTRUCT . Quando si definisce una struttura su IBM MQ, non includere il prefisso del nome QSG nel nome struttura. Ad esempio, per definire una struttura dell'applicazione per IBM MQ con il nome *qsg - name*APPLICATION1 nella politica CFRM, immettere il seguente comando:

```
DEFINE CFSTRUCT(APPLICATION1)
```

L'attributo CFSTRUCT della definizione della coda viene utilizzato per associare la coda ad una struttura. Specificare il nome della struttura CF senza il prefisso del nome QSG in questo attributo. Ad esempio, il seguente comando definisce una coda condivisa nella struttura APPLICATION1 :

```
DEFINE QLOCAL(myqueue) QSGDISP(SHARED) CFSTRUCT(APPLICATION1)
```

z/OS *Pianificazione dell'ambiente SMDS (shared message data set)*

Se si utilizzano gruppi di condivisione code con offload SMDS, IBM MQ deve connettersi a un gruppo di dataset di messaggi condivisi. Utilizzare questo argomento per comprendere i requisiti del dataset e la configurazione richiesta per memorizzare i dati del messaggio IBM MQ .

Un *dataset di messaggi condivisi* (descritto dalla parola chiave SMDS) è un dataset utilizzato da un gestore code per memorizzare i dati di messaggi scaricati per i messaggi condivisi memorizzati in una struttura CFS (coupling facility structure).

Nota: Quando si definiscono i dataset SMDS per una struttura, è necessario averne uno per ciascun gestore code.

Quando questo modulo di scaricamento dati è abilitato, **CFSTRUCT** richiede un gruppo associato di dataset di messaggi condivisi, un dataset per ogni gestore code nel gruppo di condivisione code. Il gruppo di dataset di messaggi condivisi è definito in IBM MQ utilizzando il parametro **DSGROUP** nella definizione **CFSTRUCT** . Ulteriori parametri possono essere utilizzati per fornire ulteriori informazioni facoltative, come il numero di buffer da utilizzare e gli attributi di espansione per i dataset.

Ciascun gestore code può scrivere nel dataset di cui è proprietario, per memorizzare i dati dei messaggi condivisi per i messaggi scritti tramite tale gestore code e può leggere tutti i dataset del gruppo.

Un elenco che descrive lo stato e gli attributi per ogni dataset associato alla struttura viene gestito internamente come parte della definizione **CFSTRUCT** , in modo che ogni gestore code possa controllare la definizione per scoprire quali dataset sono attualmente disponibili.

Queste informazioni sul data set possono essere visualizzate utilizzando il comando **DISPLAY CFSTATUS TYPE(SMDS)** per visualizzare lo stato corrente e la disponibilità e il comando **DISPLAY SMDS** per visualizzare le impostazioni dei parametri per i data set associati a un **CFSTRUCT**specificato.

I singoli dataset di messaggi condivisi vengono effettivamente identificati dalla combinazione del nome del gestore code proprietario (generalmente specificato utilizzando la parola chiave **SMDS**) e del nome della struttura **CFSTRUCT** .

Questa sezione descrive i seguenti argomenti:

- Il parametro DSGROUP
- Il parametro DSBLOCK
- Caratteristiche del dataset del messaggio condiviso
- Gestione spazio dataset di messaggi condivisi
- Accesso ai dataset di messaggi condivisi
- Creazione di un dataset di messaggi condiviso
- Considerazioni sulle prestazioni e sulla capacità del dataset di messaggi condivisi
- Attivazione di un dataset di messaggi condiviso

Consultare DEFINE CFSTRUCT per dettagli su questi parametri.

Per informazioni sulla gestione dei dataset di messaggi condivisi, consultare Gestione dei dataset di messaggi condivisi per ulteriori dettagli.

Parametro DSGROUP

Il parametro **DSGROUP** nella definizione **CFSTRUCT** identifica il gruppo di dataset in cui devono essere memorizzati i messaggi di grandi dimensioni per quella struttura. È possibile utilizzare ulteriori parametri per specificare la dimensione del blocco logico da utilizzare per l'assegnazione dello spazio e i valori per le opzioni di espansione del pool di buffer e del dataset automatico.

Il parametro **DSGROUP** deve essere impostato prima di poter abilitare l'offload nei dataset.

- Se un nuovo **CFSTRUCT** viene definito in **CFLEVEL(5)** e l'opzione **OFFLOAD(SMDS)** viene specificata o assunta, il parametro **DSGROUP** deve essere specificato sullo stesso comando.
- Se un **CFSTRUCT** esistente viene modificato per aumentare il valore di **CFLEVEL** a **CFLEVEL(5)** e l'opzione **OFFLOAD(SMDS)** viene specificata o assunta, il parametro **DSGROUP** deve essere specificato sullo stesso comando se non è già impostato.

Parametro DSBLOCK

Lo spazio all'interno di ciascun dataset viene assegnato alle code come blocchi logici di dimensione fissa (di solito 256 KB) specificati utilizzando il parametro **DSBLOCK** nella definizione **CFSTRUCT** , quindi assegnati ai singoli messaggi come intervalli di pagine di 4 KB (corrispondenti alla dimensione del blocco fisico e alla dimensione dell'intervallo di controllo) all'interno di ogni blocco logico. La dimensione del blocco logico determina inoltre la quantità massima di dati del messaggio che possono essere letti o scritti in una singola operazione I/O, che è uguale alla dimensione del buffer per il pool di buffer SMDS.

Un valore maggiore del parametro **DSBLOCK** può migliorare le prestazioni per messaggi molto grandi riducendo il numero di operazioni I/O separate. Tuttavia, un valore inferiore diminuisce la quantità di memoria di buffer richiesta per ogni richiesta attiva. Il valore predefinito per il parametro **DSBLOCK** è 256 KB, che fornisce un ragionevole equilibrio tra questi requisiti, quindi la specifica di questo parametro potrebbe non essere normalmente necessaria.

Caratteristiche del dataset del messaggio condiviso

Un dataset di messaggi condivisi è definito come un dataset lineare VSAM (LDS). Ogni messaggio scaricato viene memorizzato in uno o più blocchi nel dataset. I dati memorizzati vengono indirizzati direttamente dalle informazioni nelle voci CF (Coupling Facility), come una forma estesa di memoria virtuale. Non vi è alcun indice separato o informazioni di controllo simili memorizzate nel dataset stesso.

Lo schema di indirizzamento diretto indica che per i messaggi che rientrano in un blocco, è necessaria una sola operazione di I/O per leggere o scrivere il blocco. Quando un messaggio occupa più di un blocco, le operazioni I/O per ciascun blocco possono essere completamente sovrapposte per ridurre al minimo il tempo trascorso, a condizione che siano disponibili buffer sufficienti.

Il dataset del messaggio condiviso contiene anche una piccola quantità di informazioni di controllo generali, che consistono in un'intestazione nella prima pagina, che include le informazioni sullo stato di ripristino e riavvio, e un'area di checkpoint della mappa dello spazio utilizzata per salvare la mappa dello spazio di blocco libero al termine normale del gestore code.

Gestione spazio dataset di messaggi condivisi

Come informazioni di base per la capacità, le prestazioni e le considerazioni operative, potrebbe essere utile comprendere i concetti di come lo spazio nei dataset di messaggi condivisi viene gestito dai gestori code.

Lo spazio libero in ciascun dataset di messaggi condivisi viene tracciato dal relativo gestore code proprietario utilizzando una mappa di spazi che indica il numero di pagine in uso all'interno di ciascun blocco logico. La mappa di spazio viene conservata nella memoria principale mentre il dataset viene

aperto e salvato nel dataset quando viene chiuso normalmente. (In situazioni di ripristino, la mappa di spazio viene ricreata automaticamente eseguendo una scansione dei messaggi nella struttura CFS per individuare quali pagine di dataset sono attualmente in uso).

Quando viene scritto un messaggio condiviso con dati di messaggi scaricati, il gestore code assegna un intervallo di pagine per ciascun blocco di messaggi. Se esiste un blocco logico corrente parzialmente utilizzato per la coda specificata, il gestore code assegna lo spazio a partire dalla successiva pagina libera in tale blocco, altrimenti assegna un nuovo blocco logico. Se l'intero messaggio non rientra nel blocco logico corrente, il gestore code suddivide i dati del messaggio alla fine del blocco logico e assegna un nuovo blocco logico per il blocco di messaggi successivo. Ciò viene ripetuto fino a quando non viene assegnato spazio per l'intero messaggio. Qualsiasi spazio inutilizzato nell'ultimo blocco logico viene salvato come nuovo blocco logico corrente per la coda. Quando il dataset viene chiuso normalmente, tutte le pagine inutilizzate nei blocchi logici correnti vengono restituite alla mappa di spazio prima che venga salvata.

Quando un messaggio condiviso con i dati del messaggio scaricati è stato letto ed è pronto per essere eliminato, il gestore code elabora la richiesta di eliminazione trasferendo la voce della CF per il messaggio in un elenco di ripulitura monitorato dal gestore code proprietario (che può essere lo stesso gestore code). Quando le voci arrivano in questo elenco, il gestore code proprietario legge ed elimina le voci e restituisce gli intervalli di pagine liberate alla mappa dello spazio. Quando tutte le pagine utilizzate in un blocco logico sono state liberate, il blocco diventa disponibile per il riutilizzo.

Accesso ai data set di messaggi condivisi

Ciascun dataset di messaggi condivisi deve trovarsi nella memoria di accesso diretto condiviso accessibile a tutti i gestori code nel gruppo di condivisione code.

Durante l'esecuzione normale, ogni gestore code apre il proprio dataset di messaggi condiviso per l'accesso in lettura/scrittura e apre qualsiasi dataset di messaggi condiviso attivo per altri gestori code per l'accesso in sola lettura, in modo da poter leggere i messaggi memorizzati da tali gestori code. Ciò significa che ogni ID utente del gestore code richiede almeno l'accesso UPDATE al proprio dataset di messaggi condivisi e l'accesso READ a tutti gli altri dataset di messaggi condivisi per la struttura.

Se è necessario ripristinare i dataset di messaggi condivisi utilizzando **RECOVER CFSTRUCT**, il processo di recupero può essere eseguito da qualsiasi gestore code nel gruppo di condivisione code. Un gestore code che può essere utilizzato per eseguire l'elaborazione del ripristino richiede l'accesso UPDATE a tutti i dataset che potrebbe essere necessario ripristinare

Creazione di un dataset di messaggi condivisi

Ogni dataset di messaggi condivisi deve essere normalmente creato prima che la definizione **CFSTRUCT** corrispondente venga creata o modificata per consentire l'utilizzo di questo modulo di scaricamento del messaggio, poiché le modifiche della definizione **CFSTRUCT** avranno effetto immediatamente e il dataset verrà richiesto non appena un gestore code tenta di accedere a una coda condivisa che è stata assegnata a quella struttura. Un lavoro di esempio per assegnare e pre - formattare un dataset di messaggi condivisi viene fornito in SCSQPROC (CSQ4SMDS). Il lavoro deve essere personalizzato ed eseguito per assegnare un dataset di messaggi condivisi per ogni gestore code che utilizza un CFSTRUCT con OFFLOAD (SMDS).

Se il gestore code rileva che il supporto offload è stato abilitato e tenta di aprire il relativo dataset di messaggi condivisi ma non è stato ancora creato, il dataset di messaggi condivisi verrà contrassegnato come non disponibile. Il gestore code non sarà quindi in grado di memorizzare messaggi di grandi dimensioni fino a quando il dataset non sarà stato creato e il gestore code non sarà stato avvisato di riprovare, ad esempio utilizzando il comando **START SMDSCONN** .

Un dataset di messaggi condivisi viene creato come un dataset lineare VSAM utilizzando un comando Access Method Services **DEFINE CLUSTER** . La definizione deve specificare **SHAREOPTIONS(2 3)** per consentire a un gestore code di aprirlo per l'accesso in scrittura e a qualsiasi numero di gestori code di leggerlo contemporaneamente. È necessario utilizzare la dimensione dell'intervallo di controllo predefinito di 4 KB. Se è possibile che il dataset debba espandersi oltre i 4 GB, è necessario definirlo utilizzando una classe di dati SMS con l'attributo di indirizzabilità estesa VSAM. Un dataset di messaggi

condivisi è idoneo a risiedere nella parte EAS (extended address space) di un EAV (extended address volumes).

Ogni dataset di messaggi condivisi può essere vuoto o pre - formattato su zeri binari (utilizzando **CSQJUFMT** o un programma di utilità simile come il lavoro di esempio SCSQPROC (CSQ4SMDS)), prima del suo uso iniziale. Se è vuoto o solo parzialmente formattato quando viene aperto, il gestore code formatta automaticamente lo spazio rimanente in zeri binari.

Considerazioni sulle prestazioni e sulla capacità del dataset del messaggio condiviso

Ogni dataset di messaggi condivisi viene utilizzato per memorizzare i dati scaricati per i messaggi condivisi scritti nel **CFSTRUCT** associato dal gestore code proprietario, dalle regioni all'interno dello stesso sistema. Ogni messaggio scaricato impiega fino a 768 byte di memoria CF, costituito da 256 byte per la voce e 512 byte per i due elementi di intestazione e descrittore. Ogni messaggio scaricato viene memorizzato in una o più pagine (blocchi fisici di dimensione 4 KB) nel data set.

Lo spazio del dataset richiesto per un determinato numero di messaggi offload può quindi essere stimato arrotondando la dimensione complessiva del messaggio (incluso il descrittore) al multiplo successivo di 4 KB e moltiplicando per il numero di messaggi.

Come per una serie di pagine, quando un dataset di messaggi condivisi è quasi pieno, è possibile espanderlo automaticamente. Il funzionamento predefinito per questa espansione automatica può essere impostato utilizzando il parametro **DSEXPAND** sulla definizione **CFSTRUCT** . Questa impostazione può essere sovrascritta per ogni gestore code utilizzando il parametro **DSEXPAND** sul comando **ALTER SMDS** . L'espansione automatica viene attivata quando il dataset raggiunge il 90% di riempimento ed è richiesto più spazio. Se l'espansione è consentita ma un tentativo di espansione viene rifiutato da VSAM perché non è stata specificata alcuna assegnazione di spazio secondario quando è stato definito il dataset, l'espansione viene ritentata utilizzando un'assegnazione secondaria del 20% della dimensione corrente del data set.

Se il data set del messaggio condiviso è definito con l'attributo di indirizzabilità estesa, la dimensione massima è limitata solo da considerazioni VSAM a un massimo di 16 TB o 59 volumi. Questo valore è significativamente maggiore della dimensione massima di 64 GB di una serie di pagine locale.

Attivazione di un dataset di messaggi condivisi

Quando un gestore code si connette correttamente a una struttura CFS (application coupling facility), verifica se tale definizione della struttura specifica l'offload utilizzando un parametro **DSGROUP** associato. In tal caso, il gestore code assegna e apre il proprio dataset di messaggi condivisi per l'accesso in scrittura, quindi apre per l'accesso in lettura tutti i dataset di messaggi condivisi esistenti di proprietà di altri gestori code.

Quando un dataset di messaggi condivisi viene aperto per la prima volta (prima che sia stato registrato come attivo nel gruppo di condivisione code), la prima pagina non conterrà ancora un'intestazione valida. Il gestore code compila le informazioni di intestazione per identificare il gruppo di condivisione code, il nome struttura e il gestore code proprietario.

Dopo che l'intestazione è stata completata, il gestore code registra il nuovo dataset di messaggi condivisi come attivo e trasmette un evento per notificare a tutti gli altri gestori code attivi il nuovo dataset.

Ogni volta che un gestore code apre un dataset di messaggi condivisi, convalida le informazioni di intestazione per garantire che il dataset corretto sia ancora in uso e che non sia stato danneggiato.

z/OS *Pianificazione del tuo ambiente Db2*

Se si utilizzano i gruppi di condivisione code, IBM MQ deve collegarsi ad un sottosistema Db2 che è un membro di un gruppo di condivisione dati. Utilizzare questo argomento per comprendere i requisiti Db2 utilizzati per conservare i dati IBM MQ .

IBM MQ deve conoscere il nome del gruppo di condivisione dati a cui deve connettersi e il nome di un sottosistema Db2 (o gruppo Db2) a cui connettersi, per raggiungere questo gruppo di condivisione dati.

Questi nomi vengono specificati nel parametro QSGDATA della macro del parametro di sistema CSQ6SYSP (descritto in Utilizzo di CSQ6SYSP).

All'interno del gruppo di condivisione dati, le tabelle Db2 condivise vengono utilizzate per contenere:

- Informazioni di configurazione per il gruppo di condivisione code.
- Proprietà degli oggetti IBM MQ condivisi e di gruppo.
- Facoltativamente, i dati relativi ai messaggi IBM MQ di cui è stato eseguito l'offload.

IBM MQ fornisce una singola serie di lavori di esempio per la definizione dei tablespace, delle tabelle e degli indici Db2 necessari. Questi lavori utilizzano UTS (Universal Table Spaces). Le versioni precedenti del prodotto avevano due serie di lavori, uno per UTS e uno per i tipi più vecchi di tablespace, che sono stati dichiarati obsoleti dalle versioni più recenti di Db2.

IBM MQ può essere ancora utilizzato con tipi di tablespace meno recenti e ciò potrebbe essere appropriato se si dispone già di un gruppo di condivisione code esistente. Tuttavia, se si sta creando un nuovo gruppo di condivisione code, dovrebbe utilizzare UTS.

Db2 V12 Livello funzione 508 fornisce un processo di migrazione non distruttivo per la migrazione di tablespace a più tabelle in tablespace universali. È possibile utilizzare questo approccio per migrare i tablespace a più tabelle, utilizzati da gruppi di condivisione code esistenti, in tablespace universali senza eseguire un'interruzione dell'intero gruppo di condivisione code.

In Db2 V13, utilizzare l'opzione MOVE TABLE dell'istruzione ALTER TABLESPACE. Per ulteriori informazioni, consultare Spostamento di tabelle da tablespace a più tabelle in tablespace di crescita per partizione .

Per impostazione predefinita, Db2 utilizza l'ID utente della persona che esegue i lavori come proprietario delle risorse Db2 . Se questo ID utente viene eliminato, le risorse ad esso associate vengono eliminate, quindi la tabella viene eliminata. Considerare l'utilizzo di un ID gruppo per possedere le tabelle, piuttosto che un ID utente individuale. È possibile eseguire questa operazione aggiungendo `GROUP=groupname` alla scheda JOB e specificando `SET CURRENT SQLID='groupname'` prima di qualsiasi istruzione SQL.

IBM MQ utilizza la funzione RRS Attach di Db2. Ciò significa che è possibile specificare il nome di un gruppo Db2 a cui si desidera connettersi. Il vantaggio di connettersi a un nome di collegamento di un gruppo Db2 (piuttosto che a un sottosistema Db2 specifico) è che IBM MQ può connettersi (o riconnettersi) a qualsiasi sottosistema Db2 disponibile sull'immagine z/OS che è un membro di tale gruppo. Deve esistere un sottosistema Db2 membro del gruppo di condivisione dati attivo su ogni immagine z/OS in cui si sta per eseguire un sottosistema di condivisione code IBM MQ e RRS deve essere attivo.

Db2 archiviazione

Per la maggior parte delle installazioni, la quantità di memoria Db2 richiesta è di circa 20 o 30 cilindri su una periferica 3390. Tuttavia, se si desidera calcolare il requisito di memoria, la seguente tabella fornisce alcune informazioni che consentono di determinare la quantità di memoria Db2 richiesta per i dati IBM MQ . La tabella descrive la lunghezza di ogni riga Db2 e quando ogni riga viene aggiunta o eliminata dalla tabella Db2 pertinente. Utilizzare queste informazioni insieme alle informazioni sul calcolo dei requisiti di spazio per le tabelle Db2 e i relativi indici nel manuale *Db2 for z/OS Installation Guide*.

Tabella 25. Pianificazione dei requisiti di archiviazione Db2

Db2 nome tabella	**Lunghezza della riga**	**Viene aggiunta una riga quando:**	**Una riga viene eliminata quando:**
CSQ.ADMIN_B_QSG	252 byte	Un gruppo di condivisione della coda viene aggiunto alla tabella con la funzione ADD QSG del programma di utilità CSQ5PQSG .	Un gruppo di condivisione code viene rimosso dalla tabella con la funzione REMOVE QSG del programma di utilità CSQ5PQSG . Tutte le righe correlate a questo gruppo di condivisione code vengono eliminate automaticamente da tutte le altre tabelle Db2 quando il record del gruppo di condivisione code viene eliminato.
CSQ.ADMIN_B_QMGR	Fino a 3828 byte	Un gestore code viene aggiunto alla tabella con la funzione ADD QMGR del programma di utilità CSQ5PQSG .	Un gestore code viene rimosso dalla tabella con la funzione REMOVE QMGR del programma di utilità CSQ5PQSG .
CSQ.ADMIN_B_STRUCTURE	1454 byte	Viene definita la prima definizione di coda locale, specificando l'attributo QSGDISP (SHARED), che denomina una struttura precedentemente sconosciuta all'interno del gruppo di condivisione code.	L'ultima definizione di coda locale, che specifica l'attributo QSGDISP (SHARED), che denomina una struttura all'interno del gruppo di condivisione code viene cancellata.
CSQ.ADMIN_B_SCST	342 byte	È stato avviato un canale condiviso.	Un canale condiviso diventa inattivo.
CSQ.ADMIN_B_SSKT	254 byte	Viene avviato un canale condiviso con l'attributo NPMSPEED (NORMAL).	Un canale condiviso con l'attributo NPMSPEED (NORMAL) diventa inattivo.
CSQ.ADMIN_B_STRBACKUP	514 byte	Viene aggiunta una nuova riga alla CSQ CSQ.ADMIN_B_STRUCTURE . Ogni voce è una voce fittizia finché non viene eseguito il comando BACKUP CFSTRUCT, che sovrascrive le voci fittizie.	Una riga viene eliminata dalla CSQ CSQ.ADMIN_B_STRUCTURE .
CSQ.OBJ_B_AUTHINFO	3400 byte	Viene definito un oggetto delle informazioni di autenticazione con QSGDISP (GROUP).	Viene cancellato un oggetto delle informazioni di autenticazione con QSGDISP (GROUP).
CSQ.OBJ_B_QUEUE	Fino a 3707 byte	• Viene definita una coda con l'attributo QSGDISP (GROUP). • È definita una coda con l'attributo QSGDISP (SHARED). • Viene aperta una coda modello con l'attributo DEFTYPE (SHAREDYN).	• Viene cancellata una coda con l'attributo QSGDISP (GROUP). • Una coda con l'attributo QSGDISP (SHARED) viene cancellata. • Una coda dinamica con l'attributo DEFTYPE (SHAREDYN) viene chiusa con l'opzione DELETE.

Tabella 25. Pianificazione dei requisiti di archiviazione Db2 (Continua)

Db2 nome tabella	Lunghezza della riga	Viene aggiunta una riga quando:	Una riga viene eliminata quando:
CSQ.OBJ_B_NAMELIST	Fino a 15127 byte	Viene definito un elenco nomi con l'attributo QSGDISP (GROUP).	Viene cancellato un elenco nomi con l'attributo QSGDISP (GROUP).
CSQ.OBJ_B_CHANNEL	Fino a 14127 byte	È definito un canale con l'attributo QSGDISP (GROUP).	Viene eliminato un canale con l'attributo QSGDISP (GROUP).
CSQ.OBJ_B_STGCLASS	Fino a 2865 byte	Viene definita una classe di memoria con l'attributo QSGDISP (GROUP).	Viene cancellata una classe di memoria con la classe attributo QSGDISP (GROUP).
CSQ.OBJ_B_PROCESS	Fino a 3347 byte	È definito un processo con l'attributo QSGDISP (GROUP).	Viene cancellato un processo con l'attributo QSGDISP (GROUP).
CSQ.OBJ_B_TOPIC	Fino a 14520 byte	È stato definito un oggetto argomento con attributo QSGDISP (GROUP).	Viene cancellato un oggetto argomento con attributo QSGDISP (GROUP).
CSQ.EXTEND_B_QMGR	Meno di 430 byte	Un gestore code viene aggiunto alla tabella con la funzione ADD QMGR del programma di utilità CSQ5PQSG .	Un gestore code viene rimosso dalla tabella con la funzione REMOVE QMGR del programma di utilità CSQ5PQSG .
CSQ.ADMIN_B_MESSAGES	87 byte	Per il messaggio di grandi dimensioni PUT (1 per BLOB).	Per messaggio di grandi dimensioni GET (1 per BLOB).
CSQ.ADMIN_MSGS_BAUX1 CSQ.ADMIN_MSGS_BAUX2 CSQ.ADMIN_MSGS_BAUX3 CSQ.ADMIN_MSGS_BAUX4		Queste 4 tabelle contengono il payload dei messaggi di grandi dimensioni aggiunti in una di queste 4 tabelle per ogni BLOB del messaggio. I BLOB hanno una lunghezza massima di 511 KB, quindi se la dimensione del messaggio è> 711 KB, ci saranno più BLOB per questo messaggio.	

L'utilizzo di un numero elevato di messaggi di coda condivisi di dimensione superiore a 63 KB può avere implicazioni significative sulle prestazioni del sistema IBM MQ . Per ulteriori informazioni, vedere SupportPac MP16, Capacity Planning and Tuning for IBM MQ for z/OS, all'indirizzo: SupportPacs for IBM MQ and other project areas.

z/OS Pianificazione del backup e del ripristino

Lo sviluppo di procedure di backup e ripristino sul sito è fondamentale per evitare perdite di dati costose e dispendiose in termini di tempo. IBM MQ fornisce i mezzi per il ripristino di code e messaggi allo stato corrente dopo un malfunzionamento del sistema.

Il presente argomento contiene le seguenti sezioni:

- "Procedure di recupero" a pagina 193
- "Suggerimenti per backup e ripristino" a pagina 193
- "Ripristino delle serie di pagine" a pagina 195

- “Recupero strutture CF” a pagina 197
- “Raggiungere obiettivi specifici di recupero” a pagina 197
- “Considerazioni sul backup per altri prodotti” a pagina 199
- “Ripristino e CICS” a pagina 199
- “Ripristino e IMS” a pagina 199
- “Preparazione per il recupero su un sito alternativo” a pagina 199
- “Esempio di attività di backup del gestore code” a pagina 200

Procedure di recupero

Sviluppare le seguenti procedure per IBM MQ:

- Creazione di un punto di ripristino.
- Backup delle serie di pagine.
- Backup delle strutture CF.
- Ripristino delle serie di pagine.
- Ripristino da condizioni di spazio esaurito (log e serie di pagine IBM MQ).
- Recupero strutture CF.

Consultare AmministrareIBM MQ for z/OS per informazioni su tali informazioni.

Acquisire familiarità con le procedure utilizzate nel proprio sito per quanto segue:

- Ripristino da un malfunzionamento dell'hardware o dell'alimentazione.
- Ripristino da un errore del componente di z/OS .
- Ripristino da un'interruzione del sito, utilizzando il ripristino esterno.

z/OS Suggerimenti per backup e ripristino

Utilizzare questo argomento per comprendere alcune attività di backup e ripristino.

Il processo di riavvio del gestore code ripristina i dati in uno stato coerente applicando le informazioni di log alle serie di pagine. Se le serie di pagine sono danneggiate o non disponibili, è possibile risolvere il problema utilizzando le copie di backup delle serie di pagine (se tutti i log sono disponibili). Se i dataset di log sono danneggiati o non disponibili, potrebbe non essere possibile recuperarli completamente.

Considerare quanto segue:

- Eseguire periodicamente le copie di backup
- Non eliminare i log di archivio necessari
- Non modificare l'associazione del DDname alla serie di pagine

Eseguire periodicamente copie di backup

Un *punto di recupero* è il termine utilizzato per descrivere una serie di copie di backup di serie di pagine IBM MQ e i corrispondenti dataset di log richiesti per ripristinare tali serie di pagine. Tali copie di backup forniscono un punto di riavvio potenziale nel caso di una perdita delle serie di pagine (ad esempio, nel caso di un errore I/O). Se si riavvia il gestore code utilizzando queste copie di backup, i dati in IBM MQ sono congruenti fino al punto in cui tali copie sono state eseguite. Se tutti i log sono disponibili da questo punto, IBM MQ può essere ripristinato al punto di errore.

Più recenti sono le copie di backup, più velocemente IBM MQ può recuperare i dati nelle serie di pagine. Il ripristino delle serie di pagine dipende dalla disponibilità di tutte le serie di dati di log necessarie.

Nella pianificazione del ripristino, è necessario determinare la frequenza con cui eseguire le copie di backup e il numero di cicli di backup completi da conservare. Questi valori indicano per quanto tempo è necessario conservare i dataset di log e le copie di backup delle serie di pagine per il ripristino IBM MQ .

Quando si decide la frequenza con cui eseguire le copie di backup, considerare il tempo necessario per ripristinare una serie di pagine. Il tempo necessario è determinato da quanto segue:

- La quantità di log da attraversare.
- Il tempo impiegato da un operatore per montare e rimuovere i volumi nastro di archivio.
- Il tempo impiegato per leggere la parte del log necessaria per il ripristino.
- Il tempo necessario per rielaborare le pagine modificate.
- Il supporto di memorizzazione utilizzato per le copie di backup.
- Il metodo utilizzato per creare e ripristinare copie di backup.

In generale, più frequentemente si eseguono copie di backup, meno tempo impiega il ripristino, ma maggiore è il tempo impiegato per creare le copie.

Per ogni gestore code, è necessario eseguire le copie di backup di quanto segue:

- I dataset di log di archivio
- Le copie BSDS create al momento dell'archiviazione
- Le serie di pagine
- Definizioni di oggetti personali
- Strutture CF dell'utente

Per ridurre il rischio di perdita o danneggiamento delle copie di backup, considerare:

- Memorizzazione delle copie di backup su volumi di archiviazione differenti nelle copie originali.
- Memorizzazione delle copie di backup in un sito differente rispetto alle copie originali.
- Effettuare almeno due copie di ogni backup delle serie di pagine e, se si utilizza una singola registrazione o un singolo BSDS, due copie dei log di archiviazione e BSDS. Se si utilizza la registrazione doppia o BSDS, eseguire una singola copia di entrambi i log di archivio o BSDS.

Prima di spostare IBM MQ in un ambiente di produzione, verificare e documentare completamente le procedure di backup.

Backup delle serie di pagine

È necessario eseguire regolarmente il backup delle serie di pagine. Alcune aziende fanno il backup delle serie di pagine due volte al giorno.

È necessario che i log attivi e di archivio da un backup siano in grado di eseguire il ripristino utilizzando il backup. Sono necessari dati di log sufficienti per tornare indietro di quattro checkpoint se il backup è stato eseguito durante l'esecuzione del gestore code.

È possibile utilizzare ADRDSSU FastReplication per eseguire il back up delle serie di pagine ed è possibile farlo mentre il gestore code è attivo. Tenere presente che è necessario assicurarsi che vi sia spazio sufficiente nel lotto di memoria.

Backup delle definizioni oggetto

Creare copie di riserva delle proprie definizioni oggetto. Per effettuare questa operazione, utilizzare la funzione MAKEDEF della funzione COMMAND del programma di utilità (descritta nella sezione Utilizzo della funzione COMMAND di CSQUTIL).

È necessario eseguire questa operazione ogni volta che si eseguono copie di backup dei dataset del gestore code e si conserva la versione più aggiornata.

Backup delle strutture CFS (coupling facility structure)

Se hai impostato dei gruppi di condivisione code, anche se non li stai utilizzando, devi eseguire backup periodici delle tue strutture CF. A tale scopo, utilizzare il comando IBM MQ BACKUP CFSTRUCT . È possibile utilizzare questo comando solo su strutture CF definite con l'attributo RECOVER (YES). Se le voci CF per i messaggi condivisi persistenti fanno riferimento ai dati dei messaggi scaricati memorizzati in un SMDS (shared message data set) o Db2, i dati scaricati vengono richiamati e sottoposti a backup insieme alle voci CF. I dataset di messaggi condivisi non devono essere sottoposti a backup separatamente.

Si consiglia di eseguire un backup di tutte le strutture CF circa ogni ora, per ridurre al minimo il tempo impiegato per ripristinare una struttura CF.

Puoi eseguire tutti i tuoi backup della struttura CF su un singolo gestore code, il che ha il vantaggio di limitare l'aumento dell'utilizzo del log a un singolo gestore code. In alternativa, è possibile eseguire backup su tutti i gestori code nel gruppo di condivisione code, con il vantaggio di distribuire il carico di lavoro nel gruppo di condivisione code. Indipendentemente dalla strategia utilizzata, IBM MQ può individuare il backup ed eseguire un RECOVER CFSTRUCT da qualsiasi gestore code nel gruppo di condivisione code. È necessario accedere ai log di tutti i gestori code nel gruppo di condivisione code per ripristinare la struttura CF.

Backup delle politiche di sicurezza dei messaggi

Se si utilizza Advanced Message Security per creare un backup delle politiche di sicurezza dei messaggi, creare un backup utilizzando il programma di utilità della politica di sicurezza dei messaggi (CSQ0UTIL) per eseguire **dspmqspl** con il parametro -export, quindi salvare le definizioni di politica che vengono emesse in EXPORT DD.

È necessario creare un backup delle politiche di sicurezza dei messaggi ogni volta che si eseguono copie di backup dei dataset del gestore code e conservare la versione più recente.

Non eliminare i log di archivio necessari

IBM MQ potrebbe dover utilizzare i log di archivio durante il riavvio. È necessario conservare un numero sufficiente di log di archivio in modo che il sistema possa essere ripristinato completamente. IBM MQ potrebbe utilizzare un log di archivio per ripristinare una serie di pagine da una copia di backup ripristinata. Se il log di archivio è stato eliminato, IBM MQ non può ripristinare lo stato corrente della serie di pagine. Quando e come si eliminano i log di archivio è descritto in Eliminazione dei dataset di log archivio.

È possibile utilizzare il comando `/cpf DIS USAGE TYPE(ALL)` per visualizzare l'RBA log e l'LRSN (log range sequence number) necessari per ripristinare le serie di pagine del gestore code e le strutture del gruppo di condivisione code. È quindi necessario utilizzare il programma di utilità di stampa della mappa di log (CSQJU004) per stampare le informazioni BSDS (bootstrap data set) per il gestore code per individuare i log contenenti l'RBA di log.

Per le strutture CF, è necessario eseguire il programma di utilità CSQJU004 su ciascun gestore code nel gruppo di condivisione code per individuare i log contenenti l'LRSN. Hai bisogno di questi log e di eventuali log successivi per essere in grado di recuperare le serie di pagine e le strutture.

Non modificare il DDname nell'associazione della serie di pagine

IBM MQ associa il numero di serie di pagine 00 al DDname CSQP0000, il numero di serie di pagine 01 con DDname CSQP0001e così via, fino a CSQP0099. IBM MQ scrive i record del log di ripristino per una serie di pagine basata sul DDname a cui è associata la serie di pagine. Per questo motivo, non è necessario spostare le serie di pagine che sono già state associate a un PSID DDname.

z/OS Ripristino delle serie di pagine

Utilizzare questo argomento per comprendere i fattori coinvolti durante il ripristino delle serie di pagine e come ridurre i tempi di riavvio.

Un fattore chiave nella strategia di ripristino riguarda il tempo per cui è possibile tollerare un'interruzione del gestore code. Il tempo di interruzione totale potrebbe includere il tempo impiegato per ripristinare

una serie di pagine da un backup o per riavviare il gestore code dopo una chiusura anomala. I fattori che influenzano il tempo di riavvio includono la frequenza con cui si esegue il backup delle serie di pagine e la quantità di dati scritti nel log tra i punti di controllo.

Per ridurre al minimo il tempo di riavvio dopo una terminazione anomala, mantenere le unità di lavoro brevi in modo che, al massimo, vengano utilizzati due log attivi al riavvio del sistema. Ad esempio, se si sta progettando un'applicazione IBM MQ , evitare di inserire una chiamata MQGET che ha un intervallo di attesa lungo tra la prima chiamata MQI nel punto di sincronizzazione e il punto di commit perché ciò potrebbe risultare in un'unità di lavoro di lunga durata. Un'altra causa comune di unità di lavoro lunghe è l'intervallo batch di più di 5 minuti per l'iniziatore del canale.

È possibile utilizzare il comando DISPLAY THREAD per visualizzare l'RBA delle unità di lavoro e per risolvere quelle precedenti.

Con quale frequenza è necessario eseguire il backup di una serie di pagine?

Il backup frequente della serie di pagine è essenziale se è richiesto un tempo di ripristino ragionevolmente breve. Ciò si applica anche quando una serie di pagine è molto piccola o c'è una piccola quantità di attività sulle code in quella serie di pagine.

Se si utilizzano messaggi persistenti in una serie di pagine, la frequenza di backup deve essere espressa in ore anziché in giorni. Ciò vale anche per la serie di pagine zero.

Per calcolare una frequenza di backup approssimativa, iniziare determinando il tempo di ripristino totale di destinazione. Si compone dei seguenti elementi:

1. Il tempo impiegato per reagire al problema.
2. Il tempo impiegato per ripristinare la copia di backup della serie di pagine.

   Se si utilizza il backup / ripristino SnapShot , il tempo impiegato per eseguire questa attività è di pochi secondi. Per informazioni su SnapShot, consultare *DFSMSdss Storage Administration Guide*.
3. Il tempo richiesto dal gestore code per il riavvio, incluso il tempo aggiuntivo necessario per ripristinare la serie di pagine.

   Ciò dipende in modo significativo dalla quantità di dati di log che devono essere letti dai log attivi e di archivio da quando è stato eseguito l'ultimo backup della serie di pagine. Tutti questi dati di log devono essere letti, in aggiunta a quelli direttamente associati alla serie di pagine danneggiate.

   Nota: Quando si utilizza il *backup inesatto* (in cui viene eseguita un'istantanea dei log e delle serie di pagine mentre è attiva un'unità di lavoro), potrebbe essere necessario leggere fino a tre punti di controllo aggiuntivi e ciò potrebbe comportare la necessità di leggere uno o più log aggiuntivi.

Quando si decide per quanto tempo consentire il ripristino della serie di pagine, i fattori da considerare sono:

- La frequenza con cui i dati vengono scritti nei log attivi durante la normale elaborazione dipende dalla modalità di arrivo dei messaggi nel sistema, oltre alla frequenza dei messaggi.

  I messaggi ricevuti o inviati su un canale risultano in una registrazione dati superiore rispetto ai messaggi generati e richiamati localmente.
- La velocità con cui i dati possono essere letti dai log attivi e di archivio.

  Durante la lettura dei log, la velocità dei dati ottenibile dipende dalle periferiche utilizzate e dal carico totale sul sottosistema DASD specifico.

  Con la maggior parte delle unità nastro, è possibile ottenere velocità di dati più elevate per i log archiviati con una grande dimensione di blocco. Tuttavia, se è richiesto un log di archivio per il ripristino, è necessario leggere anche tutti i dati sui log attivi.

z/OS Recupero strutture CF

Utilizzare questo argomento per comprendere il processo di recupero per le strutture CF.

Almeno un gestore code nel gruppo di condivisione code deve essere attivo per elaborare un comando RECOVER CFSTRUCT. Il ripristino della struttura CF non influisce sul tempo di riavvio del gestore code, poiché il recupero viene effettuato da un gestore code attivo.

Il processo di recupero consiste in due passi logici gestiti dal comando RECOVER CFSTRUCT:

1. Individuazione e ripristino del backup.
2. Unione di tutti gli aggiornamenti registrati ai messaggi persistenti conservati nella struttura CF dai log di tutti i gestori code nel gruppo di condivisione code che hanno utilizzato la struttura CF e applicazione delle modifiche al backup.

Il secondo passo potrebbe richiedere molto più tempo perché potrebbe essere necessario leggere molti dati di log. È possibile ridurre il tempo impiegato se si eseguono backup frequenti, se si ripristinano più strutture CF contemporaneamente o entrambi.

Il gestore code che esegue il ripristino individua i backup pertinenti su tutti gli altri log dei gestori code utilizzando i dati in Db2 e i dataset di avvio. Il gestore code riesegue di nuovo questi backup nella sequenza temporale corretta nel gruppo di condivisione code, da poco prima dell'ultima copia di backup fino al momento dell'errore.

Il tempo impiegato per ripristinare una struttura CF dipende dalla quantità di dati di log di recupero che devono essere riprodotti, che a sua volta dipende dalla frequenza dei backup. Nel peggiore dei casi, ci vuole tanto tempo per leggere il log di un gestore code quanto per scriverlo. Quindi, se, ad esempio, si dispone di un gruppo di condivisione code contenente sei gestori code, un'ora di attività di log potrebbe richiedere sei ore per la ripetizione. In generale, ci vuole meno tempo, perché la lettura può essere eseguita in massa e perché i diversi log del gestore code possono essere letti in parallelo. Come punto di partenza, ti consigliamo di eseguire il backup delle strutture CF ogni ora.

Tutti i gestori code possono continuare a lavorare con code non condivise e code in altre strutture CF mentre è presente una struttura CF non riuscita. Se anche la struttura di gestione ha avuto esito negativo, è necessario avviare almeno uno dei gestori code nel gruppo di condivisione code prima di poter immettere il comando RECOVER CFSTRUCT.

Il backup delle strutture CF può richiedere una notevole capacità di scrittura dei log e può quindi imporre un carico elevato sul gestore code che esegue il backup. Scegliere un gestore code leggermente caricato per eseguire backup; per i sistemi occupati, aggiungere un gestore code aggiuntivo al gruppo di condivisione code e dedicarlo esclusivamente per eseguire backup.

z/OS Raggiungere obiettivi specifici di recupero

Utilizzare questo argomento per istruzioni su come raggiungere specifici tempi di destinazione del ripristino regolando la frequenza di backup.

Se si dispone di specifiche destinazioni di ripristino per ottenere, ad esempio, il completamento del ripristino del gestore code e riavviare l'elaborazione in aggiunta al normale tempo di avvio entro *xx* secondi, è possibile utilizzare il seguente calcolo per stimare la frequenza di backup (in ore):

```
Formula (A)
                    Required restart time * System recovery log read rate
                          (in secs)                  (in MB/sec)
Backup frequency  = ------------------------------------------------------
   (in hours)              Application log write rate (in MB/hour)
```

Nota: Gli esempi forniti successivamente hanno lo scopo di evidenziare la necessità di eseguire frequentemente il backup dei set di pagine. I calcoli presuppongono che la maggior parte dell'attività di log derivi da un numero elevato di messaggi persistenti. Tuttavia, ci sono situazioni in cui la quantità di attività di log non viene calcolata facilmente. Ad esempio, in un ambiente di gruppo di condivisione

code, un'unità di lavoro in cui le code condivise vengono aggiornate in aggiunta ad altre risorse potrebbe causare la scrittura di record UOW nel log IBM MQ . Per questo motivo, la velocità di scrittura del log dell'applicazione nella formula (A) può essere derivata in modo accurato solo dalla velocità osservata con cui i log IBM MQ si riempiono.

Ad esempio, considerare un sistema in cui IBM MQ MQI clients genera un carico totale di 100 messaggi persistenti al secondo. In questo caso, tutti i messaggi vengono generati localmente.

Se ogni messaggio è di lunghezza utente di 1 KB, la quantità di dati registrati ogni ora è approssimativamente:

```
100 * (1 + 1.3) KB * 3600 = approximately 800 MB

where
      100           = the message rate a second
      (1 + 1.3) KB  = the amount of data logged for
                      each 1 KB of persistent messages
```

Considerare un tempo di ripristino di destinazione complessivo di 75 minuti. Se sono stati consentiti 15 minuti per reagire al problema e ripristinare la copia di backup della serie di pagine, il ripristino e il riavvio del gestore code devono essere completati entro 60 minuti (3600 secondi) applicando la formula (A). Supponendo che tutti i dati di log richiesti siano su DASD RVA2-T82 , che ha una velocità di recupero di circa 2.7 MB al secondo, ciò richiede una frequenza di backup della serie di pagine di almeno ogni:

```
3600 seconds * 2.7 MB a second / 800 MB an hour = 12.15 hours
```

Se il tuo giorno dell'applicazione IBM MQ dura circa 12 ore, è appropriato un backup ogni giorno. Tuttavia, se il giorno dell'applicazione dura 24 ore, due backup al giorno sono più appropriati.

Un altro esempio potrebbe essere un sistema di produzione in cui tutti i messaggi sono per le applicazioni di richiesta - risposta (ossia, un messaggio persistente viene ricevuto su un canale ricevente e un messaggio di risposta persistente viene generato e inviato su un canale mittente).

In questo esempio, la dimensione batch raggiunta è una e quindi c'è un batch per ogni messaggio. Se ci sono 50 risposte di richiesta al secondo, il carico totale è di 100 messaggi persistenti al secondo. Se ogni messaggio ha una lunghezza di 1 KB, la quantità di dati registrati ogni ora è approssimativamente:

```
50((2 * (1+1.3) KB) + 1.4 KB + 2.5 KB) * 3600 = approximately 1500 MB

where:
 50                 = the message pair rate a second
 (2 * (1 + 1.3) KB) = the amount of data logged for each message pair
 1.4 KB             = the overhead for each batch of messages
                      received by each channel
 2.5 KB             = the overhead for each batch of messages sent
                      by each channel
```

Per ottenere il ripristino e il riavvio del gestore code entro 30 minuti (1800 secondi), sempre supponendo che tutti i dati di log richiesti siano su DASD RVA2-T82 , è necessario che il backup della serie di pagine venga eseguito almeno ogni:

```
1800 seconds * 2.7 MB a second / 1500 MB an hour = 3.24 hours
```

Esame periodico della frequenza di backup

Controlla il tuo utilizzo del log IBM MQ in termini di MB all'ora. Eseguire periodicamente questo controllo e modificare la propria frequenza di backup della serie di pagine, se necessario.

z/OS Considerazioni sul backup per altri prodotti

Se si utilizza IBM MQ con CICS o IMS , è necessario considerare anche le implicazioni per la propria strategia di backup con tali prodotti. DFHSM (Data Facility Hierarchical Storage Manager) gestisce l'archiviazione dei dati e può interagire con l'archiviazione utilizzata da IBM MQ.

Backup e ripristino con DFHSM

DFHSM (Data Facility Hierarchical Storage Manager) esegue la gestione automatica della disponibilità di spazio e dei dati tra le unità di memoria del sistema. Se lo utilizzi, devi sapere che sposta automaticamente i dati da e verso l'archiviazione IBM MQ .

DFHSM gestisce lo spazio DASD in modo efficiente spostando i dataset che non sono stati utilizzati di recente in un'archiviazione alternativa. Inoltre, rende i dati disponibili per il ripristino copiando automaticamente le serie di dati nuove o modificate sui volumi di backup DASD o nastro. Può eliminare i dataset o spostarli su un altro dispositivo. Le sue operazioni si verificano quotidianamente, a un'ora specificata, e consentono di conservare un dataset per un periodo predeterminato prima di eliminarlo o spostarlo.

È anche possibile eseguire tutte le operazioni DFHSM manualmente. Per ulteriori informazioni su DFHSM, consultare la documentazione del prodotto z/OS DFSMS . Se si utilizza DFHSM con IBM MQ, tenere presente che DFHSM effettua le seguenti operazioni:

- Utilizza i dataset catalogati.
- Opera su serie di pagine e log.
- Supporta i dataset VSAM.

Ripristino e CICS

Il ripristino delle risorse CICS non è influenzato dalla presenza di IBM MQ. CICS riconosce IBM MQ come una risorsa nonCICS (o un gestore risorse esterno) e include IBM MQ come partecipante in qualsiasi richiesta di coordinamento del punto di sincronizzazione utilizzando RMI (Resource Manager Interface) CICS . Per ulteriori informazioni sul ripristino CICS e sull'interfaccia del gestore risorse CICS , consultare la documentazione del prodotto CICS .

Ripristino e IMS

IMS riconosce IBM MQ come sottosistema esterno e come partecipante al coordinamento del punto di sincronizzazione. Il ripristino di IMS per le risorse del sottosistema esterno è descritto nella documentazione del prodotto IMS .

z/OS Preparazione per il recupero su un sito alternativo

Se si verifica una perdita totale di un centro di elaborazione IBM MQ , è possibile eseguire il ripristino su un altro sistema IBM MQ in un sito di ripristino.

Per ripristinare un sistema IBM MQ in un sito di ripristino, è necessario eseguire regolarmente il backup delle serie di pagine e dei log. Come per tutte le operazioni di recupero dati, gli obiettivi del recupero di emergenza sono di perdere il minor numero di dati, elaborazione del carico di lavoro (aggiornamenti) e tempo possibile.

Nel sito di recupero:

- Il IBM MQ gestore code **di ripristino deve** avere lo stesso nome del gestore code perso.
- Assicurarsi che il modulo dei parametri di sistema utilizzato sul gestore code di ripristino contenga gli stessi parametri del gestore code perso.

Per ulteriori informazioni, consultare Amministrazione di IBM MQ for z/OS e Risoluzione dei problemi IBM MQ for z/OS .

z/OS Esempio di attività di backup del gestore code

Questo argomento viene mostrato come esempio di attività di backup del gestore code.

Quando si pianifica la strategia di backup del gestore code, una considerazione chiave è la conservazione della quantità corretta di dati di log. La gestione dei log descrive come determinare quali dataset di log sono richiesti, facendo riferimento all'RBA di recupero del sistema del gestore code. IBM MQ determina l'RBA di recupero del sistema utilizzando le seguenti informazioni:

- Unità di lavoro attualmente attive.
- Gli aggiornamenti della serie di pagine che non sono stati ancora cancellati dai pool di buffer sul disco.
- I backup della struttura CF e se questo log del gestore code contiene le informazioni richieste in qualsiasi operazione di ripristino che li utilizza.

È necessario conservare dati di log sufficienti per poter eseguire il ripristino del supporto. Mentre l'RBA di recupero del sistema aumenta nel tempo, la quantità di dati di log che devono essere conservati diminuisce solo quando vengono eseguiti backup successivi. I backup della struttura CF sono gestiti da IBM MQ, e quindi vengono presi in considerazione quando si riporta l'RBA di recupero del sistema. Ciò significa che, in pratica, la quantità di dati di log che devono essere conservati si riduce solo quando vengono eseguiti i backup della serie di pagine.

Figura 43 a pagina 200 mostra un esempio di attività di backup su un gestore code che è membro di un gruppo di condivisione code, il modo in cui l'RBA di ripristino varia con ciascun backup e il modo in cui ciò influisce sulla quantità di dati di log che devono essere conservati. Nell'esempio, il gestore code utilizza risorse locali e condivise: serie di pagine e due strutture CF, STRUCTURE1 e STRUCTURE2.

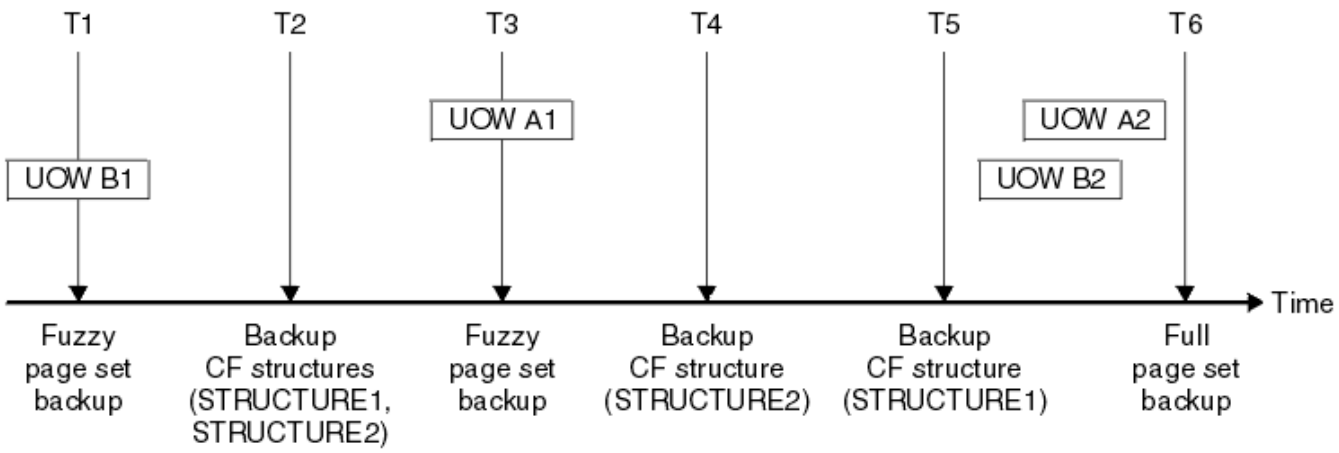


Figura 43. Esempio di attività di backup del gestore code

Questo è ciò che accade in ogni momento:

Riferimento temporale T1

Viene creato un backup inesatto delle serie di pagine, come descritto in Come eseguire il backup e il ripristino delle serie di pagine.

L'RBA di ripristino del sistema del gestore code è il più basso dei seguenti:

- Gli RBA di ripristino delle serie di pagine di cui si sta eseguendo il backup a questo punto.
- L'RBA di ripristino più basso richiesto per ripristinare le strutture dell'applicazione CF. Ciò si riferisce al ripristino dei backup di STRUCTURE1 e STRUCTURE2 creati precedentemente.
- L'RBA di ripristino per l'unità di lavoro meno recente attualmente attiva all'interno del gestore code (UOWB1).

L'RBA di ripristino del sistema per questo momento temporale è fornito dai messaggi emessi dal comando DISPLAY USAGE, che fa parte del processo di backup inesatto.

Point - in - time T2
Vengono creati backup delle strutture CF. Il backup della struttura CF STRUCTURE1 viene eseguito prima, seguito da STRUCTURE2.

La quantità di dati di log che devono essere conservati non viene modificata, poiché gli stessi dati determinati dall'RBA di recupero del sistema in T1 sono ancora richiesti per il ripristino utilizzando i backup della serie di pagine eseguiti in T1.

Riferimento temporale T3
Viene creato un altro backup inesatto.

L'RBA di ripristino del sistema del gestore code è il più basso dei seguenti:

- Gli RBA di ripristino delle serie di pagine di cui si sta eseguendo il backup a questo punto.
- L'RBA di recupero più basso richiesto per ripristinare la struttura CF STRUCTURE1, perché è stato eseguito il backup di STRUCTURE1 prima di STRUCTURE2.
- L'RBA di recupero per l'unità di lavoro più vecchia attualmente attiva nel gestore code (UOWA1).

L'RBA di ripristino del sistema per questo momento temporale è fornito dai messaggi emessi dal comando DISPLAY USAGE, che fa parte del processo di backup inesatto.

È ora possibile ridurre i dati di log conservati, come determinato da questo nuovo RBA di recupero del sistema.

Riferimento temporale T4
Viene eseguito un backup della struttura CF STRUCTURE2. L'RBA di ripristino per il ripristino del backup della struttura CF richiesto più vecchio fa riferimento al backup della struttura CF STRUCTURE1, di cui è stato eseguito il backup al momento T2.

La creazione di questo backup della struttura CF non ha alcun effetto sulla quantità di dati di log che devono essere conservati.

Riferimento temporale T5
Viene eseguito un backup della struttura CF STRUCTURE1. L'RBA di ripristino per il ripristino del backup della struttura CF richiesto più vecchio ora si riferisce al recupero della struttura CF STRUCTURE2, di cui è stato eseguito il backup al momento T4.

La creazione di questo backup della struttura CF non ha alcun effetto sulla quantità di dati di log che devono essere conservati.

Riferimento temporale T6
Viene eseguito un backup completo delle serie di pagine come descritto in Come eseguire il backup e il ripristino delle serie di pagine.

L'RBA di ripristino del sistema del gestore code è il più basso dei seguenti:

- Gli RBA di ripristino delle serie di pagine di cui si sta eseguendo il backup a questo punto.
- L'RBA di recupero più basso richiesto per ripristinare le strutture CF. Ciò si riferisce al recupero della struttura CF STRUCTURE2.
- L'RBA di recupero per l'unità di lavoro più vecchia attualmente attiva nel gestore code. In questo caso, non ci sono unità di lavoro correnti.

L'RBA di ripristino del sistema per questo momento temporale viene fornito dai messaggi emessi dal comando DISPLAY USAGE, che fa parte del processo di backup completo.

Ancora una volta, i dati di log conservati possono essere ridotti, perché l'RBA di ripristino del sistema associato al backup completo è più recente.

z/OS Pianificazione del tuo ambiente z/OS UNIX

Alcuni processi all'interno del gestore code, dell'iniziatore di canali e del server mqweb IBM MQ utilizzano z/OS UNIX System Services (z/OS UNIX) per la normale elaborazione.

Gli ID utente dell'attività avviata del gestore code e dell'iniziatore del canale richiedono un segmento OMVS con un UID definito per poter accedere a z/OS UNIX. Gli ID utente non richiedono autorizzazioni speciali in z/OS UNIX.

Nota: Sebbene il gestore code e l'iniziatore di canali utilizzino le funzionalità di z/OS UNIX (ad esempio, per interfacciarsi con i servizi TCP/IP), non è necessario accedere a nessuno dei contenuti della directory di installazione di IBM MQ nel filesystem z/OS UNIX . Di conseguenza, il gestore code e l'iniziatore di canali non richiedono alcuna configurazione per specificare il percorso per il file system z/OS UNIX .

Il server mqweb, che ospita IBM MQ Console e REST API, utilizza i file nella directory di installazione IBM MQ nel filesystem z/OS UNIX . È inoltre necessario accedere ad un altro sistema di file che viene utilizzato per memorizzare i dati come i file di configurazione e di log. Il JCL dell'attività avviata mqweb deve essere personalizzato per fare riferimento a tali file system z/OS UNIX .

Il contenuto della directory IBM MQ nel filesystem z/OS UNIX viene utilizzato anche dalle applicazioni che si collegano a IBM MQ. Ad esempio, le applicazioni che utilizzano le interfacce IBM MQ classes for Java o IBM MQ classes for JMS .

Consultare i seguenti argomenti per le istruzioni di configurazione pertinenti:

- Variabili di ambiente rilevanti per IBM MQ classes for Java
- LibrerieIBM MQ classes for Java
- Impostazione delle variabili d'ambiente
- Configurazione delle librerie JNI (Java Native Interface

z/OS pianificazione per Advanced Message Security

TLS (o SSL) può essere utilizzato per crittografare e proteggere i messaggi che scorrono su una rete, ma questo non protegge i messaggi quando si trovano su una coda ("inattivi"). Advanced Message Security (AMS) protegge i messaggi dal momento in cui vengono prima inseriti in una coda, fino a quando non vengono ricevuti, in modo che solo i destinatari previsti del messaggio possano leggere tale messaggio. I messaggi vengono codificati e firmati durante l'elaborazione di inserimento e non protetti durante l'elaborazione di acquisizione.

AMS può essere configurato per proteggere i messaggi in modi diversi:

1. È possibile firmare un messaggio. Il messaggio è in testo chiaro, ma c'è un checksum, che è firmato. Ciò consente di rilevare eventuali modifiche nel contenuto del messaggio. Dal contenuto firmato, è possibile identificare chi ha firmato i dati.
2. Un messaggio può essere codificato. Il contenuto non è visibile a nessuno senza la chiave di decodifica. La chiave di decodifica è codificata per ogni destinatario.
3. Un messaggio può essere codificato e firmato. La chiave di decodifica viene codificata per ogni destinatario e dalla firma è possibile identificare chi ha inviato il messaggio.

La crittografia e la firma utilizzano certificati digitali e keyring.

È possibile impostare un client per utilizzare AMS, in modo che i dati siano protetti prima che vengano inseriti sul canale client. I messaggi protetti possono essere inviati a un gestore code remoto ed è necessario configurare il gestore code remoto per elaborare tali messaggi.

Configurazione di AMS

Uno spazio di indirizzo AMS viene utilizzato per eseguire il lavoro AMS . Questo ha un ulteriore sistema di sicurezza, per dare accesso e proteggere l'uso di portachiavi e certificati.

È possibile configurare quali code devono essere protette utilizzando un programma di utilità (CSQ0UTIL) per definire le politiche di sicurezza per le code.

Una volta impostato AMS

È necessario impostare un certificato digitale e un keyring per le persone che inseriscono i messaggi e le persone che ricevono i messaggi.

Se un utente, Alice, su z/OS deve inviare un messaggio a Bob, AMS necessita di una copia del certificato pubblico per Bob.

Se Bob desidera elaborare un messaggio da Alice, AMS ha bisogno del certificato pubblico per Alice o dello stesso certificato dell'autorità di certificazione utilizzato da Alice.

Attenzione: È necessario:

- Pianificare con attenzione chi può inserire o richiamare le code
- Identificare le persone e i loro certificati.

È facile commettere errori e i problemi possono essere difficili da risolvere.

Concetti correlati

“Pianificazione per il gestore code” a pagina 146
Quando si configura un gestore code, la pianificazione deve consentire la crescita del gestore code, in modo che il gestore code soddisfi le esigenze dell'azienda.

z/OS pianificazione per Managed File Transfer

Utilizzare questa sezione come guida su come impostare il sistema per eseguire Managed File Transfer (MFT) su z/OS.

z/OS Pianificazione per Managed File Transfer - requisiti hardware e software

Utilizzare questo argomento come guida su come impostare i requisiti hardware e software sul sistema per eseguire Managed File Transfer (MFT) su z/OS.

Requisiti Software

Managed File Transfer è scritto in Java, con alcuni script shell e JCL per configurare e utilizzare il programma.

Importante: È necessario avere dimestichezza con z/OS UNIX System Services (z/OS UNIX) per configurare Managed File Transfer. Ad esempio:

- La struttura di directory del file, con nomi quali `/u/userID/myfile.txt`
- Comandi z/OS UNIX , ad esempio:
  - `cd` (modifica directory)
  - `ls` (elenca)
  - `chmod` (modificare le autorizzazioni del file)
  - `chown` (modificare la proprietà del file o i gruppi che possono accedere al file o alla directory)

È necessario che i seguenti prodotti in z/OS UNIX siano in grado di configurare ed eseguire MFT:

1. Java, ad esempio, nella directory `/java/java80_bit64_GA/J8.0_64/`
2. IBM MQ 9.3.0, ad esempio, nella directory `/mqm/V9R3M0`
3. Se si desidera utilizzare Db2 per lo stato e la cronologia, è necessario installare le librerie Db2 JDBC , ad esempio, nella directory `/db2/db2v10/jdbc/libs`.

Registrazione del prodotto

All'avvio Managed File Transfer controlla la registrazione nella concatenazione `sys1.parmlib`(IFAPRDxx). Il seguente codice è un esempio di come si registra MFT:

```
PRODUCT OWNER('IBM CORP')
NAME('WS MQ FILE TRANS')
ID(5655-MFT)
VERSION(*) RELEASE(*) MOD(*)
FEATURENAME('WS MQ FILE TRANS')
STATE(ENABLED)
```

Spazio su disco

IBM MQ for z/OS Program Directory indica i requisiti di memoria DASD e di zFS per Managed File Transfer. Per i collegamenti di download per Program Directory per IBM MQ for z/OS, consultare IBM MQ 9.3 File PDF per la documentazione del prodotto e Program Directory.

z/OS Pianificazione per le topologie Managed File Transfer

Utilizzare questo argomento come guida sulla topologia necessaria sul sistema per eseguire Managed File Transfer (MFT) su z/OS.

Managed File Transfer Gestori code

Le topologie di IBM MQ Managed File Transfer sono costituite da:

Agent e relativi gestori code associati
L'agente utilizza le code di sistema ospitate sul gestore code dell'agente per conservare le informazioni sullo stato e ricevere le richieste di lavoro.

Un gestore code comandi
Funziona come un gateway in una topologia MFT . È connesso ai gestori code dell'agent tramite i canali mittente e ricevente o il clustering. Quando vengono eseguiti alcuni comandi, si collegano direttamente al Gestore code comandi e inviano un messaggio all'agente specificato. Questo messaggio viene instradato tramite la rete IBM MQ al gestore code dell'agent, dove viene prelevato dall'agent ed elaborato.

Un gestore code di coordinamento
Questo è un hub centrale che ha conoscenza dell'intera topologia. Il gestore code di coordinamento è connesso a tutti i gestori code dell'agent in una topologia tramite i canali mittente e ricevente o utilizzando il clustering. Gli agent pubblicano regolarmente le informazioni di stato sul gestore code di coordinamento e memorizzano i modelli di trasferimento.

È possibile per un singolo gestore code eseguire più ruoli all'interno di una topologia. Ad esempio, lo stesso gestore code può essere configurato sia come gestore code di coordinamento che come gestore code comandi per una topologia.

Se si utilizzano più gestori code, è necessario configurare i canali tra i gestori code. È possibile eseguire questa operazione utilizzando il clustering o utilizzando connessioni point - to - point.

Quando si utilizza IBM MQ Managed File Transfer for z/OS, è necessario considerare una serie di elementi quando si determinano i gestori code da utilizzare per i diversi ruoli all'interno di una topologia.

Gestori code agent

Il gestore code dell'agente per un agente IBM MQ Managed File Transfer for z/OS deve essere in esecuzione su z/OS.

If:

- L'agent è in esecuzione su Managed File Transfer for z/OS su IBM MQ 9.1 o versioni successive

- Inoltre, il gestore code dell'agent è autorizzato per IBM MQ Advanced for z/OS Value Unit Edition (Advanced VUE)

l'agent può connettersi al gestore code utilizzando il trasporto CLIENT.

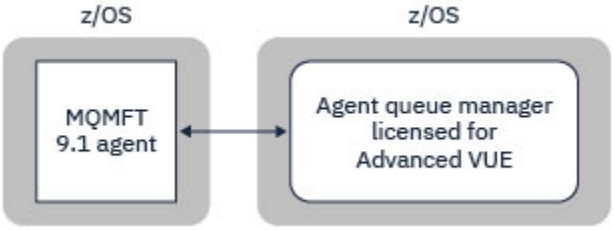


Figura 44. Gli agent di MFT 9.1 su z/OS possono connettersi ad un gestore code utilizzando il trasporto CLIENT, supponendo che il gestore code sia concesso in licenza per Advanced VUE.

If:

- L'agent è in esecuzione Managed File Transfer for z/OS su IBM MQ 9.0 o versioni precedenti
- Oppure, il gestore code dell'agent sta eseguendo Managed File Transfer for z/OS su IBM MQ 9.0 o versioni successive e il gestore code dell'agent è concesso in licenza per MFT, IBM MQ Advanced for z/OSo Advanced VUE

l'agent deve connettersi al gestore code utilizzando il trasporto BINDINGS.

Figura 45. Gli agent MFT 9.0 su z/OS e 9.1 che hanno un gestore code dell'agent concesso in licenza per MFT o IBM MQ Advanced, devono connettersi utilizzando il trasporto BINDINGS.

Gestori code comandi

L'argomento Quali MFT comandi e processi si connettono a quale gestore code mostra tutti i comandi che si connettono al gestore code comandi per una topologia Managed File Transfer .

Nota: Quando si eseguono questi comandi su z/OS, il gestore code comandi deve trovarsi anche su z/OS.

Se il gestore code comandi ha la licenza per Advanced VUE, i comandi possono connettersi al gestore code utilizzando il trasporto CLIENT. Altrimenti, i comandi devono connettersi al gestore code comandi utilizzando il trasporto BINDINGS.

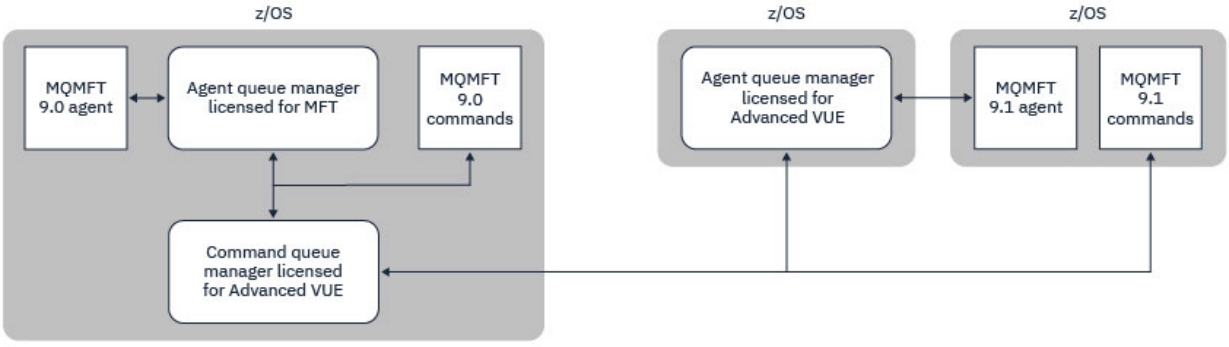


Figura 46. I comandi si connettono al gestore code comandi per una topologia MFT. Quando si eseguono questi comandi su z/OS, il gestore code comandi deve essere anche su z/OS

Gestori code di coordinamento

Gli agenti IBM MQ Managed File Transfer for z/OS possono far parte di una topologia in cui il gestore code di coordinamento è in esecuzione su z/OSo su una piattaforma multipla.

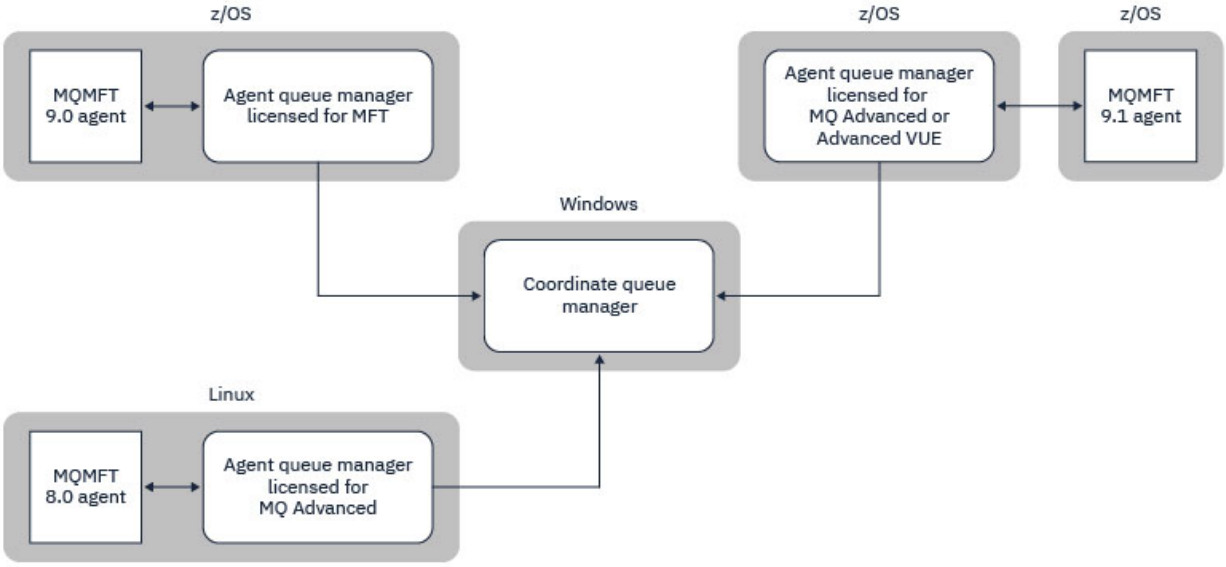


Figura 47. Gli agent MFT in esecuzione su z/OS possono far parte di una topologia MFT in cui il gestore code di coordinamento è in esecuzione su una piattaforma multipla IBM MQ .

L'argomento Quali MFT comandi e processi si connettono a quale gestore code mostra i comandi che si connettono al gestore code di coordinamento per una topologia Managed File Transfer . È possibile eseguire questi comandi su z/OS e connettersi quindi al gestore code di coordinamento in esecuzione su una piattaforma diversa.

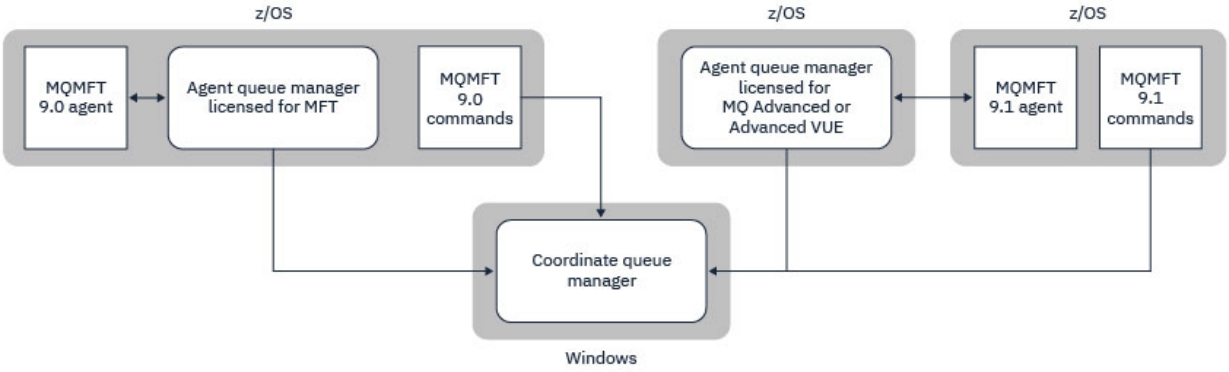


*Figura 48. Alcuni comandi, come **fteListAgents**, si connettono direttamente al gestore code di coordinamento per una topologia MFT .*

Di quanti agenti ho bisogno?

Gli agent eseguono il lavoro di trasferimento dei dati e quando si effettua una richiesta di trasferimento dei dati si specifica il nome di un agent.

Per impostazione predefinita, un agent può elaborare 25 richieste di invio e 25 richieste di ricezione contemporaneamente. È possibile configurare questi processi. Per ulteriori informazioni, consultare Managed File Transfer opzioni di configurazione su z/OS .

Se l'agent è occupato, il lavoro viene accodato. Il tempo impiegato per elaborare una richiesta dipende da più fattori, ad esempio, la quantità di dati da inviare, la larghezza di banda della rete e il ritardo sulla rete.

È possibile che si desideri disporre di più agent per elaborare il lavoro in parallelo.

È anche possibile controllare le risorse a cui un agent può accedere, in modo da poter utilizzare alcuni agent con un sottoinsieme limitato di dati.

Se si desidera elaborare le richieste con priorità diversa, è possibile utilizzare più agent e utilizzare il gestore del carico di lavoro per impostare la priorità dei lavori.

Esecuzione degli agenti

In genere gli agenti sono processi di lunga durata. I processi possono essere inoltrati come lavori eseguiti in batch o come attività avviate.

z/OS Pianificazione per Managed File Transfer - considerazioni sulla sicurezza

Utilizzare questo argomento come guida per le considerazioni sulla sicurezza necessarie sul sistema per eseguire Managed File Transfer (MFT) su z/OS.

Sicurezza

È necessario identificare quali ID utente verranno utilizzati per la configurazione MFT e per l'operazione MFT.

È necessario identificare i file o le code che si trasferiscono e quali ID utente inoltreranno le richieste di trasferimento a MFT.

Quando si personalizzano gli agent e il programma di registrazione, si specifica il gruppo di utenti a cui è consentito eseguire i servizi MFT o eseguire la gestione MFT.

Impostare questo gruppo prima di iniziare la personalizzazione di MFT. Poiché MFT utilizza le code IBM MQ , se la sicurezza è abilitata nel gestore code, MFT richiede l'accesso alle seguenti risorse:

Tabella 26. Classe di risorsa MQADMIN

Nome	Accesso richiesto
QUEUE.SYSTEM.FTE.EVENT.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.COMMAND.agent_name	Aggiornamento
CONTEXT.SYSTEM.FTE.COMMAND.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.STATE.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.DATA.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.REPLY.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.AUTHAGT1.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.AUTHTRN1.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.AUTHOPS1.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.AUTHSCH1.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.AUTHMON1.agent_name	Aggiornamento
QUEUE.SYSTEM.FTE.AUTHADM1.agent_name	Aggiornamento

Tabella 27. classe di risorsa MQQUEUE

Nome	Accesso richiesto
SYSTEM.FTE.AUTHAGT1.agent_name	Aggiornamento
SYSTEM.FTE.AUTHTRN1.agent_name	Aggiornamento

Tabella 27. classe di risorsa MQQUEUE (Continua)	
Nome	**Accesso richiesto**
SYSTEM.FTE.AUTHOPS1.agent_name	Aggiornamento
SYSTEM.FTE.AUTHSCH1.agent_name	Aggiornamento
SYSTEM.FTE.AUTHMON1.agent_name	Aggiornamento

È possibile utilizzare il sandboxing utente per determinare a quale parte del file system può accedere l'utente che richiede il trasferimento.

Per abilitare il sandboxing dell'utente, aggiungere l'istruzione `userSandboxes=true` al file *agent.properties* per l'agente che si desidera limitare e aggiungere i valori appropriati al file `MQ_DATA_PATH/mqft/config/coordination_qmgr_name/agents/agent_name/UserSandboxes.xml` .

Per ulteriori informazioni, consultare Utilizzo delle sandbox utente .

Questo ID utente è configurato nei file `UserSandboxes.xml` .

Questo file XML contiene informazioni come ID utente o ID utente * e un elenco di risorse che possono essere utilizzate (incluse) o non possono essere utilizzate (escluse). È necessario definire ID utente specifici che possono accedere a quali risorse: ad esempio:

Tabella 28. ID utente di esempio insieme all'accesso a specifiche risorse			
ID utente	**Accesso**	**Includi o escludi**	**Risorsa**
Ammin *	Letto	Includi	`/home/user/**`
Ammin *	Letto	Escludi	`/home/user/private/**`
Sysprog	Letto	Includi	`/home/user/**`
Ammin *	Letto	Includi	Application.reply.queue

Note:

1. Se si specifica `type=queue` , la risorsa è un nome coda o `queue@qmgr`.
2. Se la risorsa inizia con `//`, la risorsa è un dataset; altrimenti la risorsa è un file in z/OS UNIX.
3. L'ID utente è l'ID utente della struttura MQMD, quindi potrebbe non riflettere l'ID utente che inserisce effettivamente il messaggio.
4. Per le richieste sul gestore code locale è possibile utilizzare MQADMIN CONTEXT.* per limitare gli utenti che possono impostare questo valore.
5. Per le richieste in arrivo su un gestore code remoto, si deve presumere che i gestori code distribuiti abbiano la sicurezza abilitata per impedire l'impostazione non autorizzata dell'ID utente nella struttura MQMD.
6. Un ID utente SYSPROG1 su una macchina Linux , è lo stesso ID utente SYSPROG1 per il controllo di sicurezza su z/OS.

z/OS Pianificazione dell'uso di IBM MQ Console e REST API su z/OS

IBM MQ Console e REST API sono applicazioni eseguite in un server WebSphere Liberty (Liberty) noto come mqweb. Il server mqweb viene eseguito come attività avviata. IBM MQ Console consente di utilizzare un browser Web per gestire i gestori code. REST API fornisce una semplice interfaccia di programmazione per le applicazioni per eseguire la gestione del gestore code e per eseguire la messaggistica.

File di installazione e configurazione

È necessario installare la funzione IBM MQ for z/OS UNIX System Services Web Components , che installerà i file richiesti per eseguire il server mqweb in z/OS UNIX System Services (z/OS UNIX). È necessario avere dimestichezza con z/OS UNIX per poter configurare e gestire il server mqweb.

Consultare IBM MQ for z/OS Program Directory PDF files per informazioni sull'installazione di IBM MQ for z/OS UNIX System Services Components.

I file IBM MQ in z/OS UNIX sono installati con diversi attributi impostati richiesti per il corretto funzionamento del server mqweb. Se è necessario copiare i file di installazione di IBM MQ z/OS UNIX , ad esempio se è stato installato IBM MQ su un sistema ed è stato eseguito IBM MQ su un sistema differente, è necessario copiare lo ZFS IBM MQ creato durante l'installazione e montarlo in sola lettura nella destinazione. La copia dei file in altri modi potrebbe causare la perdita di alcuni attributi di file.

È necessario decidere il percorso e creare una directory utente Liberty quando viene creato il server mqweb. Questa directory contiene i file di configurazione e di log e l'ubicazione può essere simile a `/var/mqm/mqweb`.

Utilizzo di IBM MQ Console e REST API con gestori code a livelli differenti

REST API può interagire direttamente solo con i gestori code in esecuzione alla stessa versione, release e modifica (VRM) del server mqweb che esegue REST API. Ad esempio, IBM MQ 9.3.0 REST API può interagire direttamente solo con i gestori code locali in IBM MQ 9.3.0e IBM MQ 9.2.5 REST API può interagire direttamente solo con i gestori code locali in IBM MQ 9.2.5.

È possibile utilizzare REST API per gestire un gestore code con una versione diversa da quella del server mqweb configurando un gestore code gateway. Tuttavia, è necessario almeno un gestore code alla stessa versione del server mqweb per agire come gestore code del gateway. Per ulteriori informazioni, consultare Amministrazione remota utilizzando la REST API.

IBM MQ Console può essere utilizzato per gestire gestori code locali che vengono eseguiti alla stessa versione di IBM MQ Console. V 9.3.0 Da IBM MQ 9.3.0, è anche possibile utilizzare IBM MQ Console per gestire un gestore code in esecuzione su un sistema remoto o con una diversa versione di IBM MQ Console. Per ulteriori informazioni, consultare Aggiunta di un gestore code remoto a IBM MQ Console.

Migrazione

Se si dispone di un solo gestore code, è possibile eseguire il server mqweb come una singola attività avviata e modificare le librerie utilizzate durante la migrazione del gestore code.

Se si dispone di più di un gestore code, durante la migrazione è possibile avviare i server mqweb con versioni differenti utilizzando le attività avviate con nomi differenti. Questi nomi possono essere qualsiasi nome si desideri. Ad esempio, è possibile avviare un IBM MQ 9.1.0 server mqweb utilizzando un'attività avviata denominata MQWB0910e un server IBM MQ 9.0.5 mqweb utilizzando un'attività avviata denominata MQWB0905.

Quindi, quando si migrano i gestori code da una versione a una successiva, i gestori code diventano disponibili nel server mqweb per la versione successiva e non sono più disponibili nel server mqweb per la versione precedente.

Una volta migrati tutti i gestori code alla versione più recente, è possibile eliminare il server mqweb per la versione precedente.

Porte Http

Il server mqweb utilizza fino a due porte per HTTP:

- Uno per HTTPS, con un valore predefinito di 9443.
- Uno per HTTP. HTTP non è abilitato per impostazione predefinita, ma se abilitato, ha un valore predefinito di 9080.

Se i valori di porta predefiniti sono in utilizzo, è necessario assegnare altre porte. Se si dispone di più di un server mqweb in esecuzione contemporaneamente per più di una versione di IBM MQ, è necessario assegnare porte separate per ciascuna versione. Per ulteriori informazioni sull'impostazione delle porte utilizzate dal server mqweb, consultare Configurazione delle porte HTTP e HTTPS.

È possibile utilizzare il seguente comando TSO per visualizzare le informazioni su una porta:

```
NETSTAT TCP tcpip (PORT portNumber)
```

dove *tcpip* è il nome dello spazio di indirizzo TCP/IP e *portNumber* specifica il numero della porta di cui visualizzare le informazioni.

Sicurezza - avvio del server mqweb

L'ID utente del server mqweb necessita di determinate autorizzazioni. Per ulteriori informazioni, consultare Autorità richiesta dall'ID utente dell'attività avviata del server mqweb.

Sicurezza - utilizzo di IBM MQ Console e REST API

Quando si utilizzano IBM MQ Console e REST API, è necessaria l'autenticazione come utente incluso in un registro configurato. A questi utenti vengono assegnati ruoli specifici che determinano le azioni che gli utenti possono eseguire. Ad esempio, per utilizzare messaging REST API, a un utente deve essere assegnato il ruolo `MQWebUser` . Per ulteriori informazioni sui ruoli disponibili per IBM MQ Console e REST APIe sull'accesso concesso da questi ruoli, vedi Ruoli su IBM MQ Console e REST API.

Per ulteriori informazioni sulla configurazione della sicurezza per IBM MQ Console e REST API, consultare IBM MQ Console e REST API security.

Informazioni particolari

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti.

IBM potrebbe non offrire i prodotti, i servizi o le funzioni descritti in questo documento in altri paesi. Consultare il rappresentante IBM locale per informazioni sui prodotti e sui servizi disponibili nel proprio paese. Ogni riferimento relativo a prodotti, programmi o servizi IBM non implica che solo quei prodotti, programmi o servizi IBM possano essere utilizzati. In sostituzione a quelli forniti da IBM possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino la violazione dei diritti di proprietà intellettuale o di altri diritti dell'IBM. Tuttavia, è responsabilità dell'utente valutare e verificare il funzionamento di qualsiasi prodotto, programma o servizio non IBM.

IBM potrebbe disporre di applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La fornitura di tale documento non concede alcuna licenza a tali brevetti. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Per richieste di licenze relative ad informazioni double-byte (DBCS), contattare il Dipartimento di Proprietà Intellettuale IBM nel proprio paese o inviare richieste per iscritto a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Il seguente paragrafo non si applica al Regno Unito o a qualunque altro paese in cui tali dichiarazioni sono incompatibili con le norme locali: INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE LA PRESENTE PUBBLICAZIONE "NELLO STATO IN CUI SI TROVA" SENZA GARANZIE DI ALCUN TIPO, ESPRESSE O IMPLICITE, IVI INCLUSE, A TITOLO DI ESEMPIO, GARANZIE IMPLICITE DI NON VIOLAZIONE, DI COMMERCIABILITÀ E DI IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni; quindi la presente dichiarazione potrebbe non essere applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate su base periodica; tali modifiche vengono incorporate nelle nuove edizioni della pubblicazione. IBM si riserva il diritto di apportare miglioramenti o modifiche al prodotto/i e/o al programma/i descritti nella pubblicazione in qualsiasi momento e senza preavviso.

Qualsiasi riferimento a siti Web non IBM contenuto nelle presenti informazioni è fornito per consultazione e non vuole in alcun modo promuovere i suddetti siti Web. I materiali presenti in tali siti Web non sono parte dei materiali per questo prodotto IBM e l'utilizzo di tali siti Web è a proprio rischio.

Tutti i commenti e i suggerimenti inviati potranno essere utilizzati liberamente da IBM e diventeranno esclusiva della stessa.

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a:

IBM Corporation
Coordinatore interoperabilità software, Dipartimento 49XA
Autostrada 3605 52 N

© Copyright IBM Corp. 2007, 2025

Rochester, MN 55901
U.S.A.

Queste informazioni possono essere rese disponibili secondo condizioni contrattuali appropriate, compreso, in alcuni casi, il pagamento di un addebito.

Il programma su licenza descritto in queste informazioni e tutto il materiale su licenza disponibile per esso sono forniti da IBM in base ai termini dell' IBM Customer Agreement, IBM International Program License Agreement o qualsiasi altro accordo equivalente tra le parti.

Tutti i dati relativi alle prestazioni contenuti in questo documento sono stati determinati in un ambiente controllato. Pertanto, i risultati ottenuti in altri ambienti operativi possono variare in modo significativo. Alcune misurazioni potrebbero essere state fatte su sistemi a livello di sviluppo e non vi è alcuna garanzia che queste misurazioni saranno le stesse sui sistemi generalmente disponibili. Inoltre, alcune misurazioni potrebbero essere state stimate mediante estrapolazione. I risultati quindi possono variare. Gli utenti di questo documento dovrebbero verificare i dati applicabili per il loro ambiente specifico.

Le informazioni relative a prodotti non IBM provengono dai fornitori di tali prodotti, dagli annunci pubblicati o da altre fonti pubblicamente disponibili. IBM non ha verificato tali prodotti e, pertanto, non può garantirne l'accuratezza delle prestazioni. Eventuali commenti relativi alle prestazioni dei prodotti non IBM devono essere indirizzati ai fornitori di tali prodotti.

Tutte le dichiarazioni riguardanti la direzione o l'intento futuro di IBM sono soggette a modifica o ritiro senza preavviso e rappresentano solo scopi e obiettivi.

Questa pubblicazione contiene esempi di dati e prospetti utilizzati quotidianamente nelle operazioni aziendali, Per poterli illustrare nel modo più completo possibile, gli esempi riportano nomi di persone, società, marchi e prodotti. Tutti questi nomi sono fittizi e qualsiasi somiglianza con nomi ed indirizzi adoperati da imprese realmente esistenti sono una mera coincidenza.

LICENZA SUL COPYRIGHT:

Queste informazioni contengono programmi applicativi di esempio in lingua originale, che illustrano le tecniche di programmazione su diverse piattaforme operative. È possibile copiare, modificare e distribuire questi programmi di esempio sotto qualsiasi forma senza alcun pagamento alla IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire i programmi applicativi in conformità alle API (application programming interface) a seconda della piattaforma operativa per cui i programmi di esempio sono stati scritti. Questi esempi non sono stati testati approfonditamente tenendo conto di tutte le condizioni possibili. IBM, quindi, non può garantire o sottintendere l'affidabilità, l'utilità o il funzionamento di questi programmi.

Se si sta visualizzando queste informazioni in formato elettronico, le fotografie e le illustrazioni a colori potrebbero non apparire.

Informazioni sull'interfaccia di programmazione

Le informazioni sull'interfaccia di programmazione, se fornite, consentono di creare software applicativo da utilizzare con questo programma.

Questo manuale contiene informazioni sulle interfacce di programmazione che consentono al cliente di scrivere programmi per ottenere i servizi di WebSphere MQ.

Queste informazioni, tuttavia, possono contenere diagnosi, modifica e regolazione delle informazioni. La diagnosi, la modifica e la regolazione delle informazioni vengono fornite per consentire il debug del software applicativo.

Importante: Non utilizzare queste informazioni di diagnosi, modifica e ottimizzazione come interfaccia di programmazione poiché sono soggette a modifica.

Marchi

IBM, il logo IBM , ibm.com, sono marchi di IBM Corporation, registrati in molte giurisdizioni nel mondo. Un elenco aggiornato dei marchi IBM è disponibile sul web in "Copyright and trademark

information"www.ibm.com/legal/copytrade.shtml. Altri nomi di prodotti e servizi potrebbero essere marchi di IBM o altre società.

Microsoft e Windows sono marchi di Microsoft Corporation negli Stati Uniti, in altri paesi o entrambi.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e/o in altri paesi.

Linux è un marchi registrato di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Questo prodotto include il software sviluppato da Eclipse Project (https://www.eclipse.org/).

Java e tutti i marchi e i logo Java sono marchi registrati di Oracle e/o di società affiliate.

Numero parte:

(1P) P/N: