7.5

Configurazione di IBM WebSphere MQ

Nota

Prima di utilizzare queste informazioni e il prodotto che supportano, leggere le informazioni in “Informazioni particolari” a pagina 457.

Questa edizione si applica alla versione 7 release 5 di IBM® WebSphere MQ e a tutte le release e modifiche successive, 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.

Indice

Configurazione

Creare uno o più gestori code su uno o più computer e configurarli sui sistemi di sviluppo, test e produzione per elaborare i messaggi che contengono i dati di business.

Prima di configurare IBM WebSphere MQ, leggere i concetti IBM WebSphere MQ in IBM WebSphere MQ Panoramica tecnica. Leggi come pianificare il tuo ambiente IBM WebSphere MQ in Pianificazione .

Esistono diversi metodi che è possibile utilizzare per creare, configurare e amministrare i gestori code e le relative risorse in IBM WebSphere MQ. Questi metodi includono le interfacce della riga comandi, una GUI e un'API di gestione. Per ulteriori informazioni su queste interfacce, consultare Amministrazione IBM WebSphere MQ .

Per istruzioni su come creare, avviare, arrestare ed eliminare un gestore code, consultare “Creazione e gestione di gestori code” a pagina 20.

Per informazioni su come creare i componenti richiesti per collegare le applicazioni e le installazioni IBM WebSphere MQ , consultare “Connessione di applicazioni mediante l'accodamento distribuito” a pagina 28.

Per istruzioni su come collegare i client a un server di IBM WebSphere MQ utilizzando metodi differenti, consultare “Configurazione delle connessioni tra client e server” a pagina 100.

Per istruzioni su come configurare un cluster di gestore code, consultare “Configurazione di un cluster di gestore code” a pagina 161.

È possibile modificare il comportamento di IBM WebSphere MQ o di un gestore code modificando le informazioni di configurazione. Per ulteriori informazioni, consultare “Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code” a pagina 422. In generale, non è necessario riavviare un gestore code per rendere effettive le modifiche di configurazione, ad eccezione di quando indicato nella documentazione di questo prodotto.

Concetti correlati

Panoramica tecnica di WebSphere MQ

Attività correlate

Gestione degli oggetti WebSphere MQ locali

Gestione degli oggetti WebSphere MQ remoti

Pianificazione

Configurazione di più installazioni su UNIX, Linux, and Windows

Quando si utilizzano più installazioni sullo stesso sistema, è necessario configurare le installazioni e i gestori code.

Queste informazioni si applicano a UNIX, Linux®, and Windows.

Utilizzare le informazioni contenute nei seguenti collegamenti per configurare le installazioni:

- “Modifica dell'installazione primaria” a pagina 16
- “Associazione di un gestore code a un'installazione” a pagina 17
- “Connessione di applicazioni in un ambiente di installazione multiplo” a pagina 6

Concetti correlati

più installazioni

Attività correlate

Scelta di un'installazione primaria

Scelta di un nome di installazione

Connessione di applicazioni in un ambiente di installazione multiplo

Sui sistemi UNIX, Linux, and Windows , se vengono caricate IBM WebSphere MQ Version 7.1o versioni successive, IBM WebSphere MQ utilizza automaticamente le librerie appropriate senza che sia necessario intraprendere ulteriori azioni. IBM WebSphere MQ utilizza le librerie dell'installazione associata al gestore code a cui si connette l'applicazione.

I seguenti concetti vengono utilizzati per spiegare il modo in cui le applicazioni si collegano a IBM WebSphere MQ:

Crea link
Quando l'applicazione viene compilata, l'applicazione viene collegata alle librerie IBM WebSphere MQ per ottenere le esportazioni di funzioni che vengono caricate quando l'applicazione viene eseguita.

Caricamento
Quando l'applicazione viene eseguita, le librerie IBM WebSphere MQ vengono ubicate e caricate. Il meccanismo specifico utilizzato per individuare le librerie varia in base al sistema operativo e al modo in cui viene creata l'applicazione. Per ulteriori informazioni su come individuare e caricare le librerie in un ambiente di installazione multipla, consultare “Caricamento di librerie IBM WebSphere MQ Version 7.1 o successive” a pagina 8.

In fase di connessione
Quando l'applicazione si connette a un gestore code in esecuzione, ad esempio, utilizzando una chiamata `MQCONN` o `MQCONNX` , si connette utilizzando le librerie IBM WebSphere MQ caricate.

Quando un'applicazione server si connette a un gestore code, le librerie caricate devono provenire dall'installazione associata al gestore code. Con più installazioni su un sistema, questa restrizione introduce nuove domande di verifica quando si sceglie il meccanismo utilizzato dal sistema operativo per individuare le librerie IBM WebSphere MQ da caricare:

- Quando il comando **setmqm** viene utilizzato per cambiare l'installazione associata a un gestore code, le librerie che devono essere caricate cambiano.
- Quando un'applicazione si connette a più gestori code appartenenti a installazioni differenti, è necessario caricare più serie di librerie.

Tuttavia, se le librerie IBM WebSphere MQ Version 7.1, o successive, sono ubicate e caricate, IBM WebSphere MQ carica e utilizza le librerie appropriate senza dover intraprendere ulteriori azioni. Quando l'applicazione si connette a un gestore code, IBM WebSphere MQ carica le librerie dall'installazione a cui è associato il gestore code.

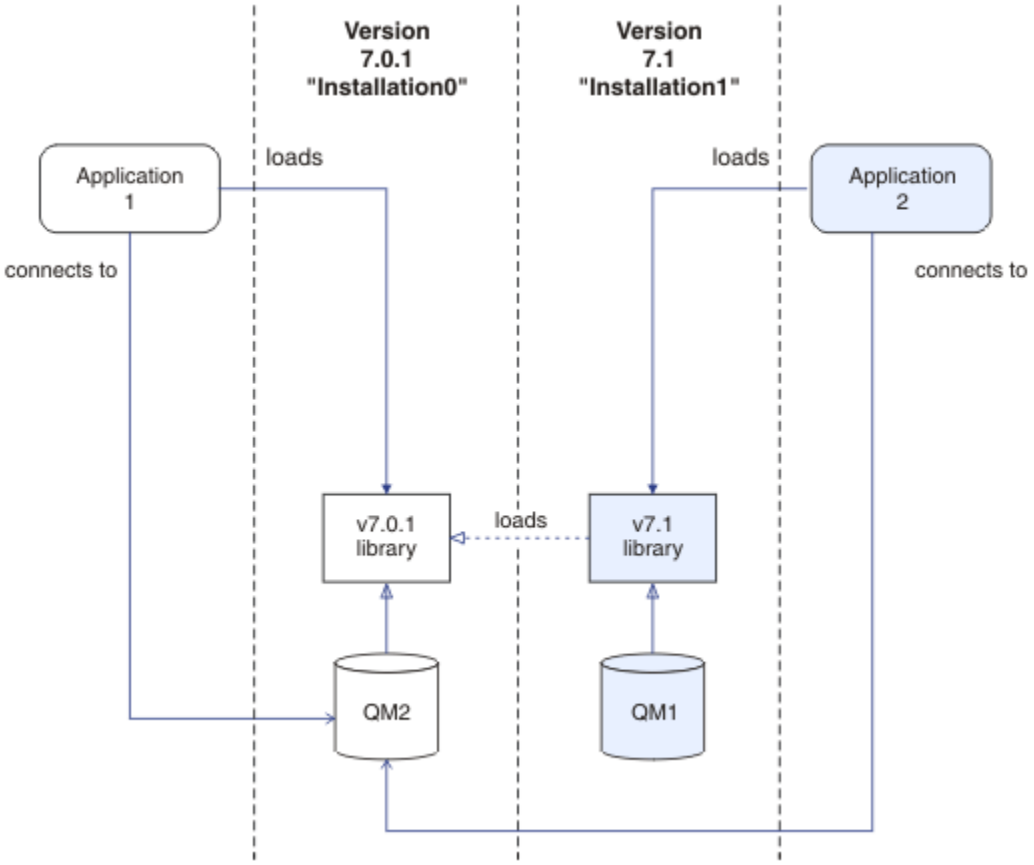


Figura 1. Connessione di applicazioni in un ambiente di installazione multiplo

Ad esempio, Figura 1 a pagina 7 mostra un ambiente di installazione multiplo con un'installazione della versione 7.0.1 (`Installation0`) e un'installazione della versione 7.1 (`Installation1`). Due applicazioni sono collegate a queste installazioni, ma caricano versioni di librerie differenti.

`Application 1` carica direttamente una libreria della versione 7.0.1 . Quando `application 1` si connette a `QM2`, vengono utilizzate le librerie della versione 7.0.1 . Se `application 1` tenta di connettersi a `QM1`, o se `QM2` è associato a `Installation1`, `application 1` ha esito negativo con un errore 2059 (080B) (RC2059): MQRC_Q_MGR_NOT_AVAILABLE . L'applicazione non riesce perché la libreria della versione 7.0.1 non è in grado di caricare altre versioni della libreria. In altre parole, se le librerie della versione 7.0.1 vengono caricate direttamente, non è possibile utilizzare un gestore code associato a un'installazione in una versione successiva di IBM WebSphere MQ.

`Application 2` carica direttamente una libreria della versione 7.1 . Quando `application 2` si connette a `QM2`, la libreria della versione 7.1 carica e utilizza la libreria della versione 7.0.1 . Se `application 2` si connette a `QM1`o se `QM2` è associato a `Installation1`, la libreria della versione 7.1 viene caricata e l'applicazione funziona come previsto.

Gli scenari di migrazione e la connessione delle applicazioni con più installazioni vengono considerati più dettagliatamente in Coesistenza di gestori code a più installazioni su UNIX, Linuxe Windows.

Per ulteriori informazioni su come caricare le librerie IBM WebSphere MQ Version 7.1 , consultare “Caricamento di librerie IBM WebSphere MQ Version 7.1 o successive” a pagina 8.

Supporto e restrizioni

Se una delle seguenti librerie della versione 7.1, o successive, viene individuata e caricata, IBM WebSphere MQ può automaticamente caricare e utilizzare le librerie appropriate:

- Le librerie del server C

- Le librerie del server C + +
- Le librerie del server XA
- Le librerie del server COBOL
- Le librerie del server COM +
- .NET in modalità non gestita

IBM WebSphere MQ inoltre carica e utilizza automaticamente le librerie appropriate per le applicazioni Java e JMS in modalità bind.

Esistono numerose limitazioni per le applicazioni che utilizzano più installazioni. Per ulteriori informazioni, vedere “Limitazioni per le applicazioni che utilizzano più installazioni” a pagina 12.

Concetti correlati

“Associazione di un gestore code a un'installazione” a pagina 17
Quando si crea un gestore code, viene automaticamente associato all'installazione che ha emesso il comando **crtmqm** . Su UNIX, Linux, and Windows, è possibile modificare l'installazione associata a un gestore code utilizzando il comando **setmqm** .

“Limitazioni per le applicazioni che utilizzano più installazioni” a pagina 12
Esistono limitazioni quando si utilizzano le librerie del server CICS , le connessioni fast path, gli handle dei messaggi e le uscite in un ambiente di installazione multiplo.

“Caricamento di librerie IBM WebSphere MQ Version 7.1 o successive” a pagina 8
Quando si decide come caricare le librerie IBM WebSphere MQ , è necessario considerare una serie di fattori, tra cui: l'ambiente, se è possibile modificare le applicazioni esistenti, se si desidera un'installazione primaria, dove è installato IBM WebSphere MQ e se è probabile che l'ubicazione di IBM WebSphere MQ cambi.

Attività correlate

Scelta di un'installazione primaria
“Modifica dell'installazione primaria” a pagina 16
È possibile utilizzare il comando **setmqinst** per impostare o annullare l'impostazione di un'installazione come installazione primaria.

Caricamento di librerie IBM WebSphere MQ Version 7.1 o successive

Quando si decide come caricare le librerie IBM WebSphere MQ , è necessario considerare una serie di fattori, tra cui: l'ambiente, se è possibile modificare le applicazioni esistenti, se si desidera un'installazione primaria, dove è installato IBM WebSphere MQ e se è probabile che l'ubicazione di IBM WebSphere MQ cambi.

Il modo in cui le librerie IBM WebSphere MQ Version 7.1 vengono ubicate e caricate dipende dall'ambiente di installazione:

- Su sistemi UNIX and Linux , se una copia di IBM WebSphere MQ Version 7.1 è installata nell'ubicazione di default, le applicazioni esistenti continuano a funzionare nello stesso modo delle versioni precedenti. Tuttavia, se le applicazioni richiedono collegamenti simbolici in `/usr/lib`, è necessario selezionare un'installazione della versione 7.1 come installazione primaria oppure creare manualmente i collegamenti simbolici.
- Se IBM WebSphere MQ Version 7.1 è installato in un'ubicazione non predefinita, come nel caso in cui anche IBM WebSphere MQ Version 7.0.1 è installato, potrebbe essere necessario modificare le applicazioni esistenti in modo da caricare le librerie corrette.

Il modo in cui le librerie IBM WebSphere MQ Version 7.1, o successive, possono essere ubicate e caricate dipende anche dal modo in cui le applicazioni esistenti sono configurate per caricare le librerie. Per ulteriori informazioni su come è possibile caricare le librerie, consultare “Meccanismi di caricamento della libreria del sistema operativo” a pagina 11.

In modo ottimale, verificare che il gestore code sia associato alla libreria IBM WebSphere MQ caricata dal sistema operativo.

I metodi per caricare le librerie IBM WebSphere MQ variano in base alla piattaforma e ciascun metodo presenta vantaggi e svantaggi.

Tabella 1. Vantaggi e svantaggi delle opzioni per il caricamento delle librerie

Piattaforma	**Opzione**	**Vantaggi**	**Inconvenienti**
Sistemi UNIX and Linux	Impostare o modificare il percorso di ricerca runtime integrato (RPath) dell'applicazione. Questa opzione richiede di ricompilare e collegare l'applicazione. Per ulteriori informazioni sulla compilazione e il collegamento delle applicazioni, consultare Creazione di un'applicazione WebSphere MQ.	• L'ambito della modifica è chiaro.	• È necessario essere in grado di ricompilare e collegare l'applicazione. • Se l'ubicazione di IBM WebSphere MQ cambia, è necessario modificare RPath.

Tabella 1. Vantaggi e svantaggi delle opzioni per il caricamento delle librerie (Continua)			
Piattaforma	**Opzione**	**Vantaggi**	**Inconvenienti**
Sistemi UNIX and Linux	Impostare la variabile di ambiente *LD_LIBRARY_PATH* (*LIBPATH* su AIX), utilizzando setmqenvo crtmqenv, con l'opzione **-k** o **-l** .	• Non sono richieste modifiche alle applicazioni esistenti. • Sovrascrive RPath integrati in un'applicazione. • È facile modificare la variabile se cambia l'ubicazione di IBM WebSphere MQ .	• Le applicazioni `setuid` e `setgid` , o le applicazioni create in altri modi, potrebbero ignorare *LD_LIBRARY_PATH* per ragioni di sicurezza. • Specifico dell'ambiente, deve essere impostato in ogni ambiente in cui viene eseguita l'applicazione. • Possibile impatto su altre applicazioni che si basano su *LD_LIBRARY_PATH*. • HP-UX: le opzioni utilizzate quando l'applicazione è stata compilata potrebbero disabilitare l'utilizzo di *LD_LIBRARY_PATH*. Per ulteriori informazioni, consultare Considerazioni sul collegamento di runtime per HP-UX. • Linux: il compilatore utilizzato per creare l'applicazione potrebbe disabilitare l'utilizzo di *LD_LIBRARY_PATH*. Per ulteriori informazioni, consultare Considerazioni sul collegamento di runtime per Linux.
Sistemi Windows	Impostare la variabile PATH utilizzando setmqo crtmqenv.	• Nessuna modifica richiesta per le applicazioni esistenti. • È facile modificare la variabile se cambia l'ubicazione di IBM WebSphere MQ .	• Specifico dell'ambiente, deve essere impostato in ogni ambiente in cui viene eseguita l'applicazione. • Possibile impatto su altre applicazioni.

Tabella 1. Vantaggi e svantaggi delle opzioni per il caricamento delle librerie (Continua)			
Piattaforma	**Opzione**	**Vantaggi**	**Inconvenienti**
Sistemi UNIX, Linux, and Windows	Impostare l'installazione primaria su una versione 7.1o successiva. Consultare “Modifica dell'installazione primaria” a pagina 16. Per ulteriori informazioni sull'installazione primaria, consultare Scelta di un'installazione primaria .	• Nessuna modifica richiesta per le applicazioni esistenti. • È facile modificare l'installazione primaria se l'ubicazione di IBM WebSphere MQ cambia. • Fornisce un comportamento simile a quello delle precedenti versioni di IBM WebSphere MQ.	• Quando è installato WebSphere MQ versione 7.0.1 , non è possibile impostare l'installazione primaria sulla versione 7.1o successiva. • UNIX and Linux: non funziona se `/usr/lib` non è nel percorso di ricerca predefinito.

Considerazioni sul caricamento della libreria per HP-UX

I comandi di compilazione di esempio nella documentazione del prodotto per le precedenti versioni di IBM WebSphere MQ includevano l'opzione di collegamento `-W1, +noenvvar` per le applicazioni a 64 bit. Questa opzione disabilita l'utilizzo di *LD_LIBRARY_PATH* per caricare le librerie condivise. Se si desidera che le applicazioni caricino le librerie di IBM WebSphere MQ da un'ubicazione diversa da quella specificata in RPath, è necessario aggiornare le applicazioni. È possibile aggiornare le applicazioni ricompilando e collegando senza l'opzione di collegamento `-W1, +noenvvar` oppure utilizzando il comando **chatr** .

Per informazioni sul modo in cui le applicazioni attualmente caricano le librerie, vedere “Meccanismi di caricamento della libreria del sistema operativo” a pagina 11.

Considerazioni sul caricamento della libreria per Linux

Le applicazioni compilate utilizzando alcune versioni di gcc, ad esempio, la versione 3.2.x, possono avere un RPath integrato che non può essere sovrascritto utilizzando la variabile di ambiente *LD_LIBRARY_PATH* . È possibile determinare se un'applicazione è interessata utilizzando il comando `readelf -d` *applicationName* . L'RPath non può essere sovrascritto se il simbolo RPATH è presente e il simbolo RUNPATH non è presente.

Considerazioni sul caricamento della libreria per Solaris

I comandi di compilazione di esempio nella documentazione del prodotto per versioni precedenti di IBM WebSphere MQ includevano le opzioni di collegamento `-lmqmcs -lmqmzse` . Le versioni appropriate di queste librerie vengono ora caricate automaticamente da IBM WebSphere MQ. Se IBM WebSphere MQ è installato in un'ubicazione non predefinita o se sul sistema sono presenti più installazioni, è necessario aggiornare le applicazioni. È possibile aggiornare le applicazioni ricompilando e collegandosi senza le opzioni di collegamento `-lmqmcs -lmqmzse` .

Meccanismi di caricamento della libreria del sistema operativo

Su sistemi Windows, vengono ricercati diversi indirizzari per trovare le librerie:

- La directory da cui è caricata l'applicazione.
- La directory corrente.
- Le directory nella variabile di ambiente *PATH* , sia la variabile *PATH* globale che la variabile *PATH* dell'utente corrente.

Sui sistemi UNIX and Linux , esistono diversi metodi che potrebbero essere stati utilizzati per individuare le librerie da caricare:

- Utilizzando la variabile di ambiente *LD_LIBRARY_PATH* (anche *LIBPATH* su AIXe *SHLIB_PATH* su HP-UX). Se questa variabile è impostata, definisce una serie di directory in cui vengono ricercate le librerie WebSphere MQ richieste. Se in queste directory vengono trovate delle librerie, esse vengono utilizzate al posto di qualsiasi libreria che potrebbe essere trovata utilizzando gli altri metodi.
- Utilizzo di un percorso di ricerca integrato (RPath). L'applicazione potrebbe contenere una serie di directory in cui ricercare le librerie IBM WebSphere MQ . Se *LD_LIBRARY_PATH* non è impostato o se le librerie richieste non sono state trovate utilizzando la variabile, le librerie vengono ricercate in RPath. Se le applicazioni esistenti utilizzano un RPath, ma non è possibile ricompilare e collegare l'applicazione, è necessario installare IBM WebSphere MQ Version 7.1 nell'ubicazione predefinita o utilizzare un altro metodo per trovare le librerie.
- Viene utilizzato il percorso libreria predefinito. Se le librerie WebSphere MQ non vengono trovate dopo la ricerca nella variabile *LD_LIBRARY_PATH* e nelle ubicazioni RPath, viene ricercato il percorso della libreria predefinito. Generalmente, questo percorso contiene `/usr/lib` o `/usr/lib64`. Se le librerie non vengono trovate dopo la ricerca nel percorso libreria predefinito, l'applicazione non riesce ad avviarsi a causa di dipendenze mancanti.

È possibile utilizzare i meccanismi del sistema operativo per verificare se le applicazioni dispongono di un percorso di ricerca integrato. Ad esempio:

- AIX: **dump**
- HP-UX: **chatr**
- Linux: **readelf**
- Solaris: **elfdump**

Concetti correlati

“Associazione di un gestore code a un'installazione” a pagina 17
Quando si crea un gestore code, viene automaticamente associato all'installazione che ha emesso il comando **crtmqm** . Su UNIX, Linux, and Windows, è possibile modificare l'installazione associata a un gestore code utilizzando il comando **setmqm** .

“Limitazioni per le applicazioni che utilizzano più installazioni” a pagina 12
Esistono limitazioni quando si utilizzano le librerie del server CICS , le connessioni fast path, gli handle dei messaggi e le uscite in un ambiente di installazione multiplo.

“Connessione di applicazioni in un ambiente di installazione multiplo” a pagina 6
Sui sistemi UNIX, Linux, and Windows , se vengono caricate IBM WebSphere MQ Version 7.1o versioni successive, IBM WebSphere MQ utilizza automaticamente le librerie appropriate senza che sia necessario intraprendere ulteriori azioni. IBM WebSphere MQ utilizza le librerie dell'installazione associata al gestore code a cui si connette l'applicazione.

Attività correlate

Scelta di un'installazione primaria

“Modifica dell'installazione primaria” a pagina 16
È possibile utilizzare il comando **setmqinst** per impostare o annullare l'impostazione di un'installazione come installazione primaria.

Limitazioni per le applicazioni che utilizzano più installazioni

Esistono limitazioni quando si utilizzano le librerie del server CICS , le connessioni fast path, gli handle dei messaggi e le uscite in un ambiente di installazione multiplo.

Librerie server CICS

Se si utilizzano le librerie del server CICS , IBM WebSphere MQ non seleziona automaticamente il livello di libreria corretto. È necessario compilare e collegare le applicazioni con il livello di libreria appropriato per il gestore code a cui si connette l'applicazione. Per ulteriori informazioni, consultare Building libraries for use with TXSeries for Multiplatforms version 5 .

Handle dei messaggi

Gli handle dei messaggi che utilizzano il valore speciale di MQHC_UNASSOCIATED_HCONN sono limitati per l'utilizzo con la prima installazione caricata in un processo. Se l'handle del messaggio non può essere utilizzato da una particolare installazione, viene restituito il codice di errore MQRC_HMSG_NOT_AVAILABLE .

Questa limitazione influenza le proprietà del messaggio. Non è possibile utilizzare gli handle del messaggio per richiamare le proprietà del messaggio da un gestore code su un'installazione e inserirle in un gestore code su un'installazione diversa. Per ulteriori informazioni sugli handle del messaggio, consultare MQCRTMH - Crea handle del messaggio.

Uscite

In un ambiente di installazione multipla, le uscite esistenti devono essere aggiornate per essere utilizzate con installazioni IBM WebSphere MQ Version 7.1o successive. Le uscite di conversione dati generate utilizzando il comando **crtmqcvx** devono essere rigenerate utilizzando il comando aggiornato.

Tutte le uscite devono essere scritte utilizzando la struttura MQIEP , non possono utilizzare un RPATH incorporato per individuare le librerie IBM WebSphere MQ e non possono collegarsi alle librerie IBM WebSphere MQ . Per ulteriori informazioni, vedi Scrittura e compilazione di uscite e servizi installabili.

Accesso rapido

Su un server con più installazioni, le applicazioni che utilizzano una connessione di accesso rapido a IBM WebSphere MQ Version 7.1 o successive devono rispettare queste regole:

1. Il gestore code deve essere associato alla stessa installazione di quella da cui l'applicazione ha caricato le librerie di runtime di IBM WebSphere MQ. L'applicazione non deve utilizzare una connessione di accesso rapido a un gestore code associato a un'installazione differente. Un tentativo di eseguire la connessione produce un errore e il codice motivo MQRC_INSTALLATION_MISMATCH.
2. Una connessione non ad accesso rapido a un gestore code associato alla stessa installazione da cui l'applicazione ha caricato le librerie di runtime di IBM WebSphere MQ impedisce all'applicazione di stabilire una connessione ad accesso rapido, a meno che non sia soddisfatta una di queste condizioni:
   - L'applicazione converte la sua prima connessione a un gestore code associato alla stessa installazione in una connessione di accesso rapido.
   - La variabile di ambiente, AMQ_SINGLE_INSTALLATION è impostata.
3. La connessione non di accesso rapido a un gestore code associato a un'istallazione di Version 7.1 o successive, non influisce sulla capacità di un'applicazione di effettuare una connessione di accesso rapido.
4. Non è possibile combinare la connessione a un gestore code associato a un'installazione di Version 7.0.1 e la connessione di accesso rapido a un gestore code associato a un'installazione di Version 7.1 o successive.

Con AMQ_SINGLE_INSTALLATION impostato, è possibile convertire qualsiasi connessione a un gestore code in una connessione di accesso rapido. In caso contrario, si applicano quasi tutte le stesse limitazioni:

- L'installazione deve corrispondere a quella da cui sono state caricate le librerie di runtime di IBM WebSphere MQ.
- Ogni connessione sullo stesso processo deve avvenire nella stessa installazione. Se si tenta di connettersi a un gestore code associato a un'installazione differente, la connessione non riesce con codice motivo MQRC_INSTALLATION_MISMATCH. Nota: con AMQ_SINGLE_INSTALLATION impostato, questa limitazione si applica a tutte le connessioni e non solo alle connessioni di accesso rapido.
- Connettere un solo gestore code con le connessioni di accesso rapido.

Riferimenti correlati

MQCONNX - Gestore code di connessione (esteso)

Struttura MQIEP

2583 (0A17) (RC2583): MQRC_INSTALLATION_MISMATCH
2587 (0A1B) (RC2587): MQRC_HMSG_NOT_AVAILABLE
2590 (0A1E) (RC2590): MQRC_FASTPATH_NOT_AVAILABLE

Connessione delle applicazioni .NET in un ambiente di installazione multiplo

Per impostazione predefinita, le applicazioni utilizzano gli assembly .NET dall'installazione primaria. Se non esiste un'installazione primaria o non si desidera utilizzare gli assembly di installazione primari, è necessario aggiornare il file di configurazione dell'applicazione o la variabile di ambiente *DEVPATH* .

Se è presente un'installazione primaria sul sistema, gli assembly .NET e i file di politica di tale installazione vengono registrati nella GAC (global assembly cache). Gli assembly .NET per tutte le altre installazioni si trovano nel percorso di installazione di ciascuna installazione, ma gli assembly non sono registrati in GAC. Pertanto, per impostazione predefinita, le applicazioni vengono eseguite utilizzando gli assembly .NET dell'installazione primaria. È necessario aggiornare il file di configurazione dell'applicazione se si verifica uno dei seguenti casi:

- Non si dispone di un'installazione primaria.
- Non si desidera che l'applicazione utilizzi gli assembly di installazione primari.
- L'installazione principale è una versione inferiore di IBM WebSphere MQ rispetto alla versione con cui è stata compilata l'applicazione.

Per informazioni su come aggiornare il file di configurazione dell'applicazione, consultare “Connessione di applicazioni .NET utilizzando il file di configurazione dell'applicazione” a pagina 14.

Devi aggiornare la variabile di ambiente *DEVPATH* se il seguente caso è true:

- Si desidera che l'applicazione utilizzi gli assembly da un'installazione non primaria, ma l'installazione primaria è alla stessa versione dell'installazione non primaria.

Per ulteriori informazioni su come aggiornare la variabile *DEVPATH* , consultare “Connessione di applicazioni .NET utilizzando DEVPATH” a pagina 15.

Connessione di applicazioni .NET utilizzando il file di configurazione dell'applicazione

All'interno del file di configurazione dell'applicazione, è necessario impostare varie tag per reindirizzare le applicazioni per utilizzare gli assembly che non provengono dall'installazione principale.

La seguente tabella mostra le modifiche specifiche che devono essere apportate al file di configurazione dell'applicazione per consentire alle applicazioni .NET di connettersi utilizzando particolari assembly:

Tabella 2. Configurazione delle applicazioni per l'utilizzo di particolari assembly

	Applicazioni compilate con una versione inferiore di IBM WebSphere MQ	**Applicazioni compilate con una versione superiore di IBM WebSphere MQ**
Per eseguire un'applicazione con un'installazione primaria IBM WebSphere MQ di versione superiore. (assiemi di versione superiore in GAC):	Nessuna modifica necessaria	Nessuna modifica necessaria
Per eseguire un'applicazione con un'installazione primaria di IBM WebSphere MQ versione precedente. (assemblee di versione inferiore in GAC):	Nessuna modifica necessaria	Nel file di configurazione dell'applicazione: • Utilizzare la tag *<bindingRedirect>* per indicare l'utilizzo della versione precedente degli assembly che si trovano in GAC

Tabella 2. Configurazione delle applicazioni per l'utilizzo di particolari assembly (Continua)		
	Applicazioni compilate con una versione inferiore di IBM WebSphere MQ	**Applicazioni compilate con una versione superiore di IBM WebSphere MQ**
Per eseguire un'applicazione con una versione superiore dell'installazione non primaria di IBM WebSphere MQ . (assembly versione superiore nella cartella di installazione):	Nel file di configurazione dell'applicazione: • Utilizzare la tag < *codebase*> per puntare all'ubicazione degli assembly di versioni superiori • Utilizzare la tag *<bindingRedirect>* per indicare l'utilizzo degli assembly di versioni superiori	Nel file di configurazione dell'applicazione: • Utilizzare la tag < *codebase*> per puntare all'ubicazione degli assembly di versioni superiori
Per eseguire un'applicazione con una versione precedente di installazione non primaria di IBM WebSphere MQ . (assembly versione inferiore nella cartella di installazione):	Nel file di configurazione dell'applicazione: • Utilizzare la tag < *codebase*> per puntare all'ubicazione degli assembly delle versioni precedenti • Includere il tag < *publisherpolicy Apply=no*	Nel file di configurazione dell'applicazione: • Utilizzare la tag < *codebase*> per puntare all'ubicazione degli assembly delle versioni precedenti • Utilizzare la tag *<bindingRedirect>* per indicare l'utilizzo degli assembly di versioni precedenti • Includere il tag < *publisherpolicy Apply=no*

Un file di configurazione dell'applicazione di esempio `NonPrimaryRedirect.config` viene fornito nella cartella *MQ_INSTALLATION_PATH*`\tools\dotnet\samples\base`. Questo file può essere modificato con il percorso di installazione IBM WebSphere MQ di qualsiasi installazione non primaria. Il file può essere incluso direttamente in altri file di configurazione utilizzando la tag *<linkedConfiguration>* . Vengono forniti esempi per `nmqsget.exe.config` e `nmqsput.exe.config`. Entrambi gli esempi utilizzano la tag *<linkedConfiguration>* e includono il file `NonPrimaryRedirect.config` .

Connessione di applicazioni .NET utilizzando DEVPATH

Puoi trovare gli assembly utilizzando la variabile di ambiente *DEVPATH* . Gli assembly specificati dalla variabile *DEVPATH* vengono utilizzati di preferenza rispetto a qualsiasi assembly nel GAC. Consulta la documentazione Microsoft appropriata su *DEVPATH* per ulteriori informazioni su quando utilizzare questa variabile.

Per trovare gli assembly utilizzando la variabile di ambiente *DEVPATH* , è necessario impostare la variabile *DEVPATH* sulla cartella che contiene gli assembly che si desidera utilizzare. Quindi, è necessario aggiornare il file di configurazione dell'applicazione e aggiungere le seguenti informazioni di configurazione runtime:

```
<configuration>
   <runtime>
       <developmentMode developerInstallation="true" />
   </runtime>
</configuration>
```

Concetti correlati

“Connessione di applicazioni in un ambiente di installazione multiplo” a pagina 6
Sui sistemi UNIX, Linux, and Windows , se vengono caricate IBM WebSphere MQ Version 7.1o versioni successive, IBM WebSphere MQ utilizza automaticamente le librerie appropriate senza che sia necessario

intraprendere ulteriori azioni. IBM WebSphere MQ utilizza le librerie dell'installazione associata al gestore code a cui si connette l'applicazione.

più installazioni

Attività correlate

Scelta di un'installazione primaria

Usando .Net

Modifica dell'installazione primaria

È possibile utilizzare il comando **setmqinst** per impostare o annullare l'impostazione di un'installazione come installazione primaria.

Informazioni su questa attività

Questa attività si applica a UNIX, Linux, and Windows.

L'installazione primaria è l'installazione a cui fanno riferimento le ubicazioni di sistema richieste. Per ulteriori informazioni sull'installazione primaria e considerazioni sulla scelta dell'installazione primaria, consultare Scelta di un'installazione primaria.

Se un'installazione di IBM WebSphere MQ Version 7.1 o successiva coesiste con un'installazione di IBM WebSphere MQ Version 7.0.1, l'installazione di IBM WebSphere MQ Version 7.0.1 deve essere la principale. Viene contrassegnato come primario quando è installata la versione IBM WebSphere MQ Version 7.1 o successiva e l'installazione IBM WebSphere MQ Version 7.1 o successiva non può essere resa primaria.

Durante il processo di installazione su Windows, è possibile specificare che l'installazione deve essere l'installazione primaria. Su sistemi UNIX and Linux , è necessario immettere un comando **setmqinst** dopo l'installazione per impostare l'installazione come installazione primaria.

“Imposta l'installazione principale” a pagina 16.

“Annulla l'impostazione dell'installazione primaria” a pagina 17.

Imposta l'installazione principale

Procedura

Per impostare un'installazione come installazione primaria:

1. Verificare se un'installazione è già l'installazione primaria immettendo il seguente comando:

   ```
   MQ_INSTALLATION_PATH/bin/dspmqinst
   ```

   dove *MQ_INSTALLATION_PATH* è il percorso di installazione di un'installazione IBM WebSphere MQ Version 7.1 o successiva.
2. Se un'installazione esistente di IBM WebSphere MQ Version 7.1 o successiva è impostata come installazione primaria, annullarne l'impostazione seguendo le istruzioni in “Annulla l'impostazione dell'installazione primaria” a pagina 17. Se IBM WebSphere MQ Version 7.0.1 è installato sul sistema, l'installazione primaria non può essere modificata.
3. Come root su sistemi UNIX and Linux o come membro del gruppo Amministratori su sistemi Windows , immettere uno dei seguenti comandi:
   - Per impostare l'installazione primaria utilizzando il percorso dell'installazione che si desidera sia l'installazione primaria:

     ```
     MQ_INSTALLATION_PATH/bin/setmqinst -i -p MQ_INSTALLATION_PATH
     ```

   - Per impostare l'installazione primaria utilizzando il nome dell'installazione che si desidera sia l'installazione primaria:

```
MQ_INSTALLATION_PATH/bin/setmqinst -i -n installationName
```

4. Su sistemi Windows , riavviare il sistema.

Annulla l'impostazione dell'installazione primaria

Procedura

Per annullare l'impostazione di un'installazione come installazione primaria:

1. Verificare quale installazione è quella primaria immettendo il seguente comando:

   ```
   MQ_INSTALLATION_PATH/bin/dspmqinst
   ```

   dove *MQ_INSTALLATION_PATH* è il percorso di installazione di un'installazione IBM WebSphere MQ Version 7.1 o successiva.

   Se IBM WebSphere MQ Version 7.0.1 è l'installazione primaria, non è possibile annullare l'impostazione dell'installazione primaria.
2. Come root su sistemi UNIX and Linux o come membro del gruppo Amministratori su sistemi Windows , immettere uno dei seguenti comandi:
   - Per annullare l'impostazione dell'installazione primaria utilizzando il percorso dell'installazione che non si desidera più sia l'installazione primaria:

     ```
     MQ_INSTALLATION_PATH/bin/setmqinst -x -p MQ_INSTALLATION_PATH
     ```
   - Per annullare l'impostazione dell'installazione primaria utilizzando il nome dell'installazione che non si desidera più sia l'installazione primaria:

     ```
     MQ_INSTALLATION_PATH/bin/setmqinst -x -n installationName
     ```

Concetti correlati

Funzioni che possono essere utilizzate solo con l'installazione primaria su Windows

La libreria esterna e il comando di controllo si collegano all'installazione primaria su UNIX e Linux

Attività correlate

Disinstallazione, aggiornamento e manutenzione dell'installazione primaria

Scelta di un nome di installazione

Riferimenti correlati

setmqinst

Associazione di un gestore code a un'installazione

Quando si crea un gestore code, viene automaticamente associato all'installazione che ha emesso il comando **crtmqm** . Su UNIX, Linux, and Windows, è possibile modificare l'installazione associata a un gestore code utilizzando il comando **setmqm** .

È possibile utilizzare il comando **setmqm** nei modi seguenti:

- Spostamento di singoli gestori code tra versioni equivalenti di WebSphere MQ. Ad esempio, lo spostamento di un gestore code da una prova a un sistema di produzione.
- Migrazione di singoli gestori code da una versione precedente di WebSphere MQ a una versione più recente di WebSphere MQ. La migrazione dei gestori code tra versioni ha diverse implicazioni di cui è necessario essere consapevoli. Per ulteriori informazioni sulla migrazione, consultare Migrazione e aggiornamento WebSphere MQ.

Per associare un gestore code a un'installazione:

1. Arrestare il gestore code utilizzando il comando **endmqm** dall'installazione attualmente associata al gestore code.
2. Associare il gestore code a un'altra installazione utilizzando il comando **setmqm** da tale installazione.

Ad esempio, per impostare il gestore code QMB in modo che sia associato a un'installazione con il nome Installation2, immettere il comando seguente da Installation2:

```
MQ_INSTALLATION_PATH/bin/setmqm -m QMB -n Installation2
```

dove *MQ_INSTALLATION_PATH* è il percorso in cui è installato Installation2 .

3. Avviare il gestore code utilizzando il comando **strmqm** dall'installazione ora associata al gestore code.

   Questo comando esegue la migrazione del gestore code necessaria e consente al gestore code di essere pronto per l'uso.

L'installazione che un gestore code è associato limita tale gestore code in modo che possa essere gestito solo dai comandi di tale installazione. Esistono tre eccezioni chiave:

- **setmqm** modifica l'installazione associata al gestore code. Questo comando deve essere immesso dall'installazione che si desidera associare al gestore code, non dall'installazione a cui è attualmente associato il gestore code. Il nome di installazione specificato dal comando **setmqm** deve corrispondere all'installazione da cui viene emesso il comando.
- **strmqm** in genere deve essere emesso dall'installazione associata al gestore code. Tuttavia, quando un gestore code V7.0.1 o versioni precedenti viene avviato su un'installazione di V7.1 o versioni successive per la prima volta, è possibile utilizzare **strmqm** . In tal caso **strmqm** avvia il gestore code e lo associa all'installazione da cui viene emesso il comando.
- **dspmq** visualizza informazioni su tutti i gestori code su un sistema, non solo su quelli associati alla stessa installazione del comando **dspmq** . Il comando `dspmq -o installation` visualizza informazioni sui gestori code associati a quali installazioni.

Associazione gestore code in ambienti HA

Per gli ambienti HA, il comando **addmqinf** associa automaticamente il gestore code all'installazione da cui viene emesso il comando **addmqinf** . Finché il comando **strmqm** viene immesso dalla stessa installazione del comando **addmqinf** , non è necessaria alcuna ulteriore configurazione. Per avviare il gestore code utilizzando un'installazione differente, è necessario prima modificare l'installazione associata mediante il comando **setmqm** .

Gestori code associati alle installazioni eliminate

Se l'installazione a cui è associato un gestore code è stata eliminata o se le informazioni sullo stato del gestore code non sono disponibili, il comando **setmqm** non riesce ad associare il gestore code ad un'altra installazione. In questa situazione, effettuare quanto segue:

1. Utilizzare il comando **dspmqinst** per visualizzare le altre installazioni sul sistema.
2. Modificare manualmente il campo `InstallationName` della sezione `QueueManager` in mqs.ini per specificare un'altra installazione.
3. Utilizzare il comando **dltmqm** da tale installazione per eliminare il gestore code.

Concetti correlati

“Ricerca di installazioni di IBM WebSphere MQ su un sistema” a pagina 19
Se si dispone di più installazioni IBM WebSphere MQ su un sistema, è possibile verificare quali versioni sono installate e dove si trovano.

“File di configurazione IBM WebSphere MQ , mqs.ini” a pagina 425
Il file di configurazione IBM WebSphere MQ , mqs.ini, contiene informazioni relative a tutti i gestori code sul nodo. Viene creato automaticamente durante l'installazione.

Attività correlate

Scelta di un'installazione primaria

Riferimenti correlati

setmqm

strmqm

dspmq
dspmqinst

Ricerca di installazioni di IBM WebSphere MQ su un sistema

Se si dispone di più installazioni IBM WebSphere MQ su un sistema, è possibile verificare quali versioni sono installate e dove si trovano.

È possibile utilizzare i seguenti metodi per individuare le installazioni di IBM WebSphere MQ sul proprio sistema:

- Utilizzare il comando **dspmqver**. Questo comando non fornisce i dettagli di tutte le installazioni su un sistema se viene emesso da un'installazione Version 7.0.1 .
- Utilizzare gli strumenti di installazione della piattaforma per eseguire una query su dove è stato installato IBM WebSphere MQ . Quindi, utilizzare il comando **dspmqver** da un'installazione Version 7.1 o successiva. I seguenti comandi sono esempi di comandi che è possibile utilizzare per eseguire una query su dove è stato installato IBM WebSphere MQ :
  - Sui sistemi AIX , è possibile utilizzare il comando **lslpp** :

    ```
    lslpp -R ALL -l mqm.base.runtime
    ```

  - Sui sistemi HP-UX , è possibile utilizzare il comando **swlist** :

    ```
    swlist -a location -a revision -l product MQSERIES
    ```

  - Sui sistemi Linux , è possibile utilizzare il comando **rpm** :

    ```
    rpm -qa --qf "%{NAME}-%{VERSION}-%{RELEASE}\t%{INSTPREFIXES}\n" | grep MQSeriesRuntime
    ```

  - Sui sistemi Solaris , è possibile utilizzare i comandi **pkginfo** e **pkgparam** :
    1. Elencare i package installati immettendo il seguente comando:

       ```
       pkginfo | grep -w mqm
       ```

    2. Per ogni pacchetto elencato, immettere il seguente comando:

       ```
       pkgparam pkgname BASEDIR
       ```

  - Su sistemi Windows , è possibile utilizzare il comando **wmic** . Questo comando potrebbe installare il client wmic:

    ```
    wmic product where "(Name like '%MQ%') AND (not Name like '%bitSupport')" get Name,
    Version, InstallLocation
    ```

- Su sistemi UNIX and Linux , immettere il seguente comando per individuare dove è stato installato IBM WebSphere MQ :

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

  Utilizzare quindi il comando **dspmqver** da un'installazione Version 7.1 o successiva.
- Per visualizzare i dettagli delle installazioni sul sistema, su Windowsa 32 bit, immettere il seguente comando:

  ```
  reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebSphere MQ\Installation" /s
  ```

- Su Windowsa 64 bit, immettere il seguente comando:

  ```
  reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IBM\WebSphere MQ\Installation" /s
  ```

Nota: il comando **reg.exe** visualizzerà solo le informazioni per le installazioni Version 7.1 o successive.

Concetti correlati
più installazioni
Riferimenti correlati
dspmqver
dspmqinst

Creazione e gestione di gestori code

Prima di poter utilizzare messaggi e code, è necessario creare e avviare almeno un gestore code e i relativi oggetti associati.

Creazione di un gestore code

Un gestore code gestisce le risorse associate ad esso, in particolare le code di sua proprietà. Fornisce servizi di accodamento alle applicazioni per chiamate e comandi MQI (Message Queuing Interface) per creare, modificare, visualizzare ed eliminare oggetti IBM WebSphere MQ .

Per creare un gestore code, utilizzare il comando di controllo IBM WebSphere MQ **crtmqm** (descritto in **crtmqm**). Il comando **crtmqm** crea automaticamente gli oggetti predefiniti richiesti e gli oggetti di sistema (descritti in Oggetti predefiniti di sistema). Gli oggetti predefiniti formano la base di tutte le definizioni di oggetto che si creano; gli oggetti di sistema sono richiesti per l'operazione del gestore code. Una volta creato un gestore code e i suoi oggetti, utilizzare il comando `strmqm` per avviarlo.

Nota: IBM WebSphere MQ non supporta i nomi macchina che contengono spazi. Se si installa IBM WebSphere MQ su un computer con un nome macchina che contiene spazi, non è possibile creare alcun gestore code.

Acceso

Prima di creare un gestore code, è necessario considerare diversi punti (soprattutto in ambiente di produzione). Utilizzare il seguente elenco di controllo:

L'installazione associata al gestore code
Il comando **crtmqm** associa automaticamente un gestore code all'installazione da cui è stato immesso il comando **crtmqm** . Per i comandi che operano su un gestore code, è necessario immettere il comando dall'installazione associata al gestore code. È possibile modificare l'installazione associata di un gestore code utilizzando il comando setmqm . Si noti che il programma di installazione di Windows non aggiunge l'utente che esegue l'installazione al gruppo mqm, per ulteriori dettagli, consultare Autorità per amministrare IBM WebSphere MQ sui sistemi UNIX, Linux e Windows.

Convenzioni di denominazione
Utilizzare nomi in MAIUSCOLO per poter comunicare con gestori code di qualsiasi piattaforma. Tenere presente che i nomi vengono assegnati esattamente come vengono immessi. Per evitare l'inconveniente di un sacco di digitazione, non utilizzare nomi inutilmente lunghi.

Specificare un nome gestore code univoco
Quando si crea un gestore code, assicurarsi che nessun altro gestore code abbia lo stesso nome *ovunque* nella rete. I nomi dei gestori code non vengono controllati quando viene creato il gestore code e i nomi che non sono univoci non consentono di creare canali per l'accodamento distribuito.

Un modo per garantire l'univocità consiste nel far precedere ogni nome di gestore code con il proprio nome nodo univoco. Ad esempio, se un nodo è denominato `ACCOUNTS`, è possibile denominare il proprio gestore code `ACCOUNTS.SATURN.QUEUE.MANAGER`, dove `SATURN` identifica un determinato gestore code e `QUEUE.MANAGER` è un'estensione che è possibile assegnare a tutti i gestori code. In alternativa, è possibile omettere questa opzione, ma tenere presente che `ACCOUNTS.SATURN` e `ACCOUNTS.SATURN.QUEUE.MANAGER` sono *diversi* nomi di gestore code.

Se si sta utilizzando IBM WebSphere MQ per la comunicazione con altre aziende, è anche possibile includere il proprio nome aziendale come prefisso. Questo non è fatto negli esempi, perché li rende più difficili da seguire.

Nota: I nomi dei gestori code nei comandi di controllo sono sensibili al maiuscolo / minuscolo. Ciò significa che è consentito creare due gestori code con i nomi `jupiter.queue.manager` e `JUPITER.queue.manager`. Tuttavia, è meglio evitare tali complicazioni.

Limita numero di gestori code

È possibile creare il numero di gestori code consentito dalle risorse. Tuttavia, poiché ciascun gestore code richiede le proprie risorse, è generalmente meglio avere un gestore code con 100 code su un nodo piuttosto che dieci gestori code con dieci code ciascuno.

Nei sistemi di produzione, molti processori possono essere utilizzati con un singolo gestore code, ma le macchine server più grandi potrebbero essere eseguite in modo più efficace con più gestori code.

Specificare un gestore code predefinito

Ogni nodo deve disporre di un gestore code predefinito, anche se è possibile configurare IBM WebSphere MQ su un nodo senza un gestore code. Il gestore code predefinito è il gestore code a cui si connettono le applicazioni se non specificano un nome gestore code in una chiamata `MQCONN` . È anche il gestore code che elabora i comandi MQSC quando si richiama il comando `runmqsc` senza specificare il nome del gestore code.

Se si specifica un gestore code come predefinito, *sostituisce* qualsiasi specifica del gestore code predefinito esistente per il nodo.

La modifica della gestione della coda predefinita può influire su altri utenti o applicazioni. La modifica non ha alcun effetto sulle applicazioni attualmente connesse, perché possono utilizzare l'handle dalla loro chiamata di connessione originale in qualsiasi ulteriore chiamata MQI. Questo handle garantisce che le chiamate siano dirette allo stesso gestore code. Tutte le applicazioni che si collegano *dopo* aver modificato il gestore code predefinito si connettono al nuovo gestore code predefinito. Questo potrebbe essere ciò che si intende, ma è necessario tenerne conto prima di modificare il valore predefinito.

La creazione di un gestore code predefinito è descritta in “Creazione di un gestore code predefinito” a pagina 23.

Specificare una coda di messaggi non instradabili

La coda di messaggi non instradati è una coda locale in cui i messaggi vengono inseriti se non possono essere instradati alla destinazione desiderata.

È importante disporre di una coda messaggi non recapitabili su ciascun gestore code della rete in uso. Se non se ne definisce una, gli errori che si verificano nei programmi applicativi potrebbero comportare la chiusura dei canali e le risposte ai comandi di gestione potrebbero non essere ricevute.

Ad esempio, se un'applicazione tenta di inserire un messaggio in una coda su un altro gestore code, ma fornisce il nome coda errato, il canale viene arrestato e il messaggio rimane nella coda di trasmissione. Altre applicazioni non possono quindi utilizzare questo canale per i loro messaggi.

I canali non vengono influenzati se i gestori code hanno code di messaggi non recapitabili. Il messaggio non consegnato viene inserito nella coda di messaggi non recapitabili all'estremità ricevente, lasciando il canale e la relativa coda di trasmissione disponibili.

Quando si crea un gestore code, utilizzare l'indicatore -u per specificare il nome della coda di messaggi non recapitabili. È anche possibile utilizzare un comando MQSC per modificare gli attributi di un gestore code già definito per specificare la coda di messaggi non instradabili da utilizzare. Consultare Gestione dei gestori code per un esempio del comando MQSC ALTER.

Specificare una coda di trasmissione predefinita

Una coda di trasmissione è una coda locale in cui i messaggi in transito verso un gestore code remoto sono accodati prima della trasmissione. La coda di trasmissione predefinita è la coda utilizzata quando non viene definita esplicitamente nessuna coda. A ciascun gestore code è possibile assegnare una coda di trasmissione predefinita.

Quando si crea un gestore code, utilizzare l'indicatore -d per specificare il nome della coda di trasmissione predefinita. Ciò non crea effettivamente la coda; è necessario farlo esplicitamente in un secondo momento. Per ulteriori informazioni, consultare Gestione delle code locali .

Specificare i parametri di registrazione richiesti

È possibile specificare i parametri di registrazione nel comando `crtmqm` , incluso il tipo di registrazione, il percorso e la dimensione dei file di log.

In un ambiente di sviluppo, i parametri di registrazione predefiniti devono essere adeguati. Tuttavia, è possibile modificare i valori predefiniti se, ad esempio:

- Si dispone di una configurazione di sistema di basso livello che non può supportare log di grandi dimensioni.
- Si prevede che un numero elevato di messaggi lunghi si trovino contemporaneamente nelle code.
- Si prevedono molti messaggi persistenti che passano attraverso il gestore code.

Dopo aver impostato i parametri di registrazione, alcuni di essi possono essere modificati solo eliminando il gestore code e ricreandolo con lo stesso nome ma con parametri di registrazione differenti.

Per ulteriori informazioni sui parametri di registrazione, consultare "Disponibilità, ripristino e riavvio" a pagina 314.

Solo per sistemi IBM WebSphere MQ per UNIX

È possibile creare la directory del gestore code `/var/mqm/qmgrs/<qmgr>`, anche su un filesystem locale separato, prima di utilizzare il comando `crtmqm` . Quando si utilizza `crtmqm`, se la directory `/var/mqm/qmgrs/<qmgr>` esiste, è vuota ed è di proprietà di mqm, viene utilizzata per i dati del gestore code. Se la directory non è di proprietà di mqm, la creazione ha esito negativo con un messaggio First Failure Support Technology (FFST). Se la directory non è vuota, viene creata una nuova directory.

Concetti correlati

"Configurazione" a pagina 5
Creare uno o più gestori code su uno o più computer e configurarli sui sistemi di sviluppo, test e produzione per elaborare i messaggi che contengono i dati di business.

"Backup dei file di configurazione dopo la creazione di un gestore code" a pagina 25
Le informazioni di configurazione IBM WebSphere MQ sono memorizzate nei file di configurazione sui sistemi Windows, UNIX and Linux .

"Avvio di un gestore code" a pagina 25
Quando si crea un gestore code, è necessario avviarlo per consentirgli di elaborare comandi o chiamate MQI.

"Arresto di un gestore code" a pagina 26
Esistono tre modi per arrestare un gestore code: un arresto inattivo e un arresto immediato e un arresto preventivo.

"Riavvio di un gestore code" a pagina 27
È possibile utilizzare il comando **strmqm** per riavviare un gestore code o, su sistemi IBM WebSphere MQ for Windows e IBM WebSphere MQ per Linux (piattaformex86 e x86-64), riavviare un gestore code da Esplora risorse di IBM WebSphere MQ .

"Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code" a pagina 422
Modificare il comportamento di IBM WebSphere MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione.

Oggetti di sistema e predefiniti

Attività correlate

"Impostazione di un gestore code esistente come predefinito" a pagina 24
È possibile rendere un gestore code esistente il gestore code predefinito. Il modo in cui si fa questo dipende dalla piattaforma che si sta utilizzando.

"Eliminazione di un gestore code" a pagina 27
È possibile eliminare un gestore code utilizzando il comando **dltmqm** oppure utilizzando WebSphere MQ Explorer.

distributed Creazione di un gestore code predefinito

Il gestore code predefinito è il gestore code a cui si connettono le applicazioni se non specificano un nome gestore code in una chiamata MQCONN. È anche il gestore code che elabora i comandi MQSC quando si richiama il comando **runmqsc** senza specificare il nome di un gestore code. Per creare un gestore code, utilizzare il IBM WebSphere MQ comando di controllo **crtmqm**.

Prima di iniziare

Prima di creare un gestore code predefinito, leggere le considerazioni descritte in "Creazione e gestione di gestori code" a pagina 20.

UNIX Quando si utilizza **crtmqm** per creare un gestore code su UNIX and Linux, se la directory `/var/mqm/qmgrs/<qmgr>` esiste già, è di proprietà di mqm ed è vuota, viene utilizzata per i dati del gestore code. Se la directory non è di proprietà di mqm, la creazione del gestore code ha esito negativo con un messaggio First Failure Support Technology (FFST). Se la directory non è vuota, viene creata una nuova directory per i dati del gestore code.

Questa considerazione si applica anche quando la directory `/var/mqm/qmgrs/<qmgr>` esiste già su un file system locale separato.

Informazioni su questa attività

Quando si crea un gestore code utilizzando il comando **crtmqm** , il comando crea automaticamente gli oggetti predefiniti richiesti e gli oggetti di sistema. Gli oggetti predefiniti formano la base di tutte le definizioni di oggetto che si creano e gli oggetti di sistema sono richiesti per l'operazione del gestore code.

Includendo i parametri rilevanti nel comando, è anche possibile definire, ad esempio, il nome della coda di trasmissione predefinita che deve essere utilizzata dal gestore code e il nome della coda di messaggi non recapitabili.

Windows Su Windows, è possibile utilizzare l'opzione **sax** del comando **crtmqm** per avviare più istanze del gestore code.

Per ulteriori informazioni sul comando **crtmqm** e la sua sintassi, consultare **crtmqm**.

Procedura

- Per creare un gestore code predefinito, utilizzare il comando **crtmqm** con l'indicatore **-q** .

  Il seguente esempio del comando **crtmqm** crea un gestore code predefinito denominato `SATURN.QUEUE.MANAGER`:

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

  dove:

  -q
  Indica che questo gestore code è il gestore code predefinito.

  -d MY.DEFAULT.XMIT.QUEUE
  Indica il nome della coda di trasmissione predefinita che deve essere utilizzata da questo gestore code.

  Nota: IBM WebSphere MQ non crea una coda di trasmissione predefinita per l'utente; è necessario definirla personalmente.

  -u SYSTEM.DEAD.LETTER.QUEUE
  È il nome della coda di messaggi non instradabili predefinita creata da IBM WebSphere MQ durante l'installazione.

SATURN.QUEUE.MANAGER
È il nome di questo gestore code. Deve essere l'ultimo parametro specificato nel comando `crtmqm` .

Operazioni successive

Una volta creato il gestore code e i suoi oggetti, utilizzare il comando **strmqm** per avviare il gestore code.

Concetti correlati

“Backup dei file di configurazione dopo la creazione di un gestore code” a pagina 25
Le informazioni di configurazione IBM WebSphere MQ sono memorizzate nei file di configurazione sui sistemi Windows, UNIX and Linux .

Uso dei gestori code

Gestione delle code locali

Riferimenti correlati

Oggetti di sistema e predefiniti

Impostazione di un gestore code esistente come predefinito

È possibile rendere un gestore code esistente il gestore code predefinito. Il modo in cui si fa questo dipende dalla piattaforma che si sta utilizzando.

WebSphere MQ per sistemi Windows e WebSphere MQ per Linux (piattaformex86 e x86-64)

Informazioni su questa attività

Utilizzare le seguenti istruzioni per rendere un gestore code esistente il gestore code di default sui sistemi WebSphere MQ per Windows e WebSphere MQ per Linux (piattaformex86 e x86-64):

Procedura

1. Aprire Esplora risorse di IBM WebSphere MQ .
2. Fare clic con il tasto destro del mouse su `IBM WebSphere MQ`, quindi selezionare `Properties...`. Viene visualizzato il pannello Proprietà per WebSphere WebSphere MQ .
3. Immettere il nome del gestore code predefinito nel relativo campo.
4. Fai clic su OK.

Sistemi UNIX and Linux

Informazioni su questa attività

Quando si crea un gestore code predefinito, il relativo nome viene inserito nell'attributo `Name` della sezione `DefaultQueueManager` nel file di configurazione WebSphere MQ (mqs.ini). La stanza e il relativo contenuto vengono creati automaticamente se non esistono.

Procedura

- Per impostare un gestore code esistente come predefinito, modificare il nome del gestore code nell'attributo `Name` con il nome del nuovo gestore code predefinito. È possibile eseguire questa operazione manualmente, utilizzando un editor di testo.
- Se non si dispone di un gestore code predefinito sul nodo e si desidera rendere predefinito un gestore code esistente, creare la stanza *`DefaultQueueManager`* con il nome richiesto.
- Se si imposta accidentalmente un altro gestore code come predefinito e si desidera ripristinare il gestore code predefinito originale, modificare la sezione `DefaultQueueManager` in mqs.ini, sostituendo il gestore code predefinito indesiderato con quello desiderato.

Operazioni successive

Consultare “Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code” a pagina 422 per informazioni sui file di configurazione.

Backup dei file di configurazione dopo la creazione di un gestore code

Le informazioni di configurazione IBM WebSphere MQ sono memorizzate nei file di configurazione sui sistemi Windows, UNIX and Linux .

Su sistemi Windows e Linux (x86 e x86-64) utilizzare IBM WebSphere MQ Explorer per apportare modifiche ai file di configurazione.

Sui sistemi Windows è anche possibile utilizzare il comando `amqmdain` per apportare modifiche ai file di configurazione. Consultare, amqmdain

Esistono due tipi di file di configurazione:

- Quando si installa il prodotto, viene creato il file di configurazione IBM WebSphere MQ (mqs.ini). Contiene un elenco di gestori code che viene aggiornato ogni volta che si crea o si elimina un gestore code. Esiste un file mqs.ini per nodo.
- Quando si crea un nuovo gestore code, viene creato automaticamente un nuovo file di configurazione del gestore code (qm.ini). Contiene i parametri di configurazione per il gestore code.

Dopo aver creato un gestore code, eseguire il backup dei propri file di configurazione. Quindi, se si crea un altro gestore code che causa problemi, è possibile ripristinare i backup una volta rimossa l'origine del problema. Come regola generale, eseguire il backup dei file di configurazione ogni volta che si crea un nuovo gestore code.

Per ulteriori informazioni sui file di configurazione, consultare “Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code” a pagina 422.

Avvio di un gestore code

Quando si crea un gestore code, è necessario avviarlo per consentirgli di elaborare comandi o chiamate MQI.

Per avviare un gestore code, utilizzare il comando **strmqm** .

Nota: È necessario utilizzare il comando **strmqm** dall'installazione associata al gestore code che si sta utilizzando. È possibile scoprire a quale installazione è associato un gestore code utilizzando il comando `dspmq -o installation` .

Ad esempio, per avviare un gestore code `QMB` , immettere il seguente comando:

```
strmqm QMB
```

Su WebSphere MQ per sistemi Windows e WebSphere MQ per Linux (piattaformex86 e x86-64), è possibile avviare un gestore code nel modo seguente:

1. Aprire Esplora risorse di IBM WebSphere MQ .
2. Selezionare il gestore code dalla vista Navigator .
3. Fare clic su `Start`. Il gestore code viene avviato.

Se l'avvio del gestore code impiega più di pochi secondi, WebSphere MQ emette messaggi informativi che descrivono in modo intermittente l'avanzamento dell'avvio.

Il comando `strmqm` non restituisce il controllo fino a quando il gestore code non viene avviato ed è pronto ad accettare le richieste di connessione.

Avvio automatico di un gestore code

In WebSphere MQ per Windows , è possibile avviare automaticamente un gestore code quando il sistema viene avviato utilizzando IBM WebSphere MQ Explorer. Per ulteriori informazioni, consultare Amministrazione utilizzando IBM WebSphere MQ Explorer.

Arresto di un gestore code

Esistono tre modi per arrestare un gestore code: un arresto inattivo e un arresto immediato e un arresto preventivo.

Utilizzare il comando **endmqm** per arrestare un gestore code.

Nota: È necessario utilizzare il comando **endmqm** dall'installazione associata al gestore code che si sta utilizzando. È possibile scoprire a quale installazione è associato un gestore code utilizzando il comando `dspmq -o installation` .

Ad esempio, per arrestare un gestore code denominato QMB, immettere il seguente comando:

```
endmqm QMB
```

Su WebSphere MQ per sistemi Windows e WebSphere MQ per sistemi Linux (x86 e x86-64), è possibile arrestare un gestore code nel modo seguente:

1. Aprire Esplora risorse di IBM WebSphere MQ .
2. Selezionare il gestore code dalla vista Navigator .
3. Fare clic su `Stop...`. Viene visualizzato il pannello Fine gestore code.
4. Selezionare Controllato o Immediato.
5. Fare clic su OK. Il gestore code viene arrestato.

arresto inattivo

Per impostazione predefinita, il comando **endmqm** esegue un arresto inattivo del gestore code specificato. Il completamento di questa operazione potrebbe richiedere un po' di tempo. Una chiusura sospesa attende che tutte le applicazioni connesse si disconnettano.

Utilizzare questo tipo di arresto per notificare le applicazioni da arrestare. Se si immette:

```
endmqm -c QMB
```

non viene indicato quando tutte le applicazioni sono state arrestate. Un comando `endmqm -c QMB` è equivalente a un comando `endmqm QMB` .

Tuttavia, se si immette:

```
endmqm -w QMB
```

il comando attende che tutte le applicazioni siano state arrestate e che il gestore code sia terminato.

arresto immediato

Per un arresto immediato, tutte le chiamate MQI correnti possono essere completate, ma le nuove chiamate non riescono. Questo tipo di arresto non attende la disconnessione delle applicazioni dal gestore code.

Per un arresto immediato, immettere:

```
endmqm -i QMB
```

arresto preventivo

Nota: Non utilizzare questo metodo a meno che tutti gli altri tentativi di arresto del gestore code tramite il comando **endmqm** non abbiano avuto esito negativo. Questo metodo può avere conseguenze imprevedibili per le applicazioni collegate.

Se un arresto immediato non funziona, è necessario ricorrere a un arresto *preventivo* , specificando l'indicatore `-p` . Ad esempio:

```
endmqm -p QMB
```

Questo arresta immediatamente il gestore code. Se questo metodo non funziona ancora, fare riferimento a Arresto manuale di un gestore code per una soluzione alternativa.

Per una descrizione dettagliata del comando **endmqm** e delle relative opzioni, vedere endmqm.

In caso di problemi durante la chiusura di un gestore code

I problemi di chiusura di un gestore code sono spesso causati dalle applicazioni. Ad esempio, quando le applicazioni:

- Non controllare correttamente i codici di ritorno MQI
- Non richiedere la notifica di un quiesce
- Terminare senza disconnettersi dal gestore code (eseguendo una chiamata `MQDISC`)

Se si verifica un problema quando si arresta il gestore code, è possibile interrompere il comando **endmqm** utilizzando Ctrl-C. È quindi possibile immettere un altro comando **endmqm** , ma questa volta con un indicatore che specifica il tipo di arresto richiesto.

Riavvio di un gestore code

È possibile utilizzare il comando **strmqm** per riavviare un gestore code o, su sistemi IBM WebSphere MQ for Windows e IBM WebSphere MQ per Linux (piattaformex86 e x86-64), riavviare un gestore code da Esplora risorse di IBM WebSphere MQ .

Per riavviare un gestore code, immettere:

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

Su sistemi IBM WebSphere MQ for Windows e IBM WebSphere MQ per Linux (piattaformex86 e x86-64), è possibile riavviare un gestore code nello stesso modo in cui viene avviato, come segue:

1. Aprire Esplora risorse di IBM WebSphere MQ .
2. Selezionare il gestore code dalla vista Navigator .
3. Fare clic su `Start`. Il gestore code viene riavviato.

Se il riavvio del gestore code impiega più di alcuni secondi, IBM WebSphere MQ emette messaggi informativi che descrivono in modo intermittente l'avanzamento dell'avvio.

Eliminazione di un gestore code

È possibile eliminare un gestore code utilizzando il comando **dltmqm** oppure utilizzando WebSphere MQ Explorer.

Prima di iniziare

Chiudere il gestore code.

Procedura

- Emetti il seguente comando: `dltmqm QMB`

Nota: È necessario utilizzare il comando **dltmqm** dall'installazione associata al gestore code che si sta utilizzando. È possibile scoprire a quale installazione è associato un gestore code utilizzando il comando `dspmq -o installation` .

Passi per l'eliminazione di un gestore code

Informazioni su questa attività

Su WebSphere MQ per Windows e WebSphere MQ per sistemi Linux (x86 e x86-64), è possibile eliminare un gestore code nel modo seguente:

Procedura

1. Aprire WebSphere MQ Explorer.
2. Nella vista Navigator , selezionare il gestore code.
3. Se il gestore code non è arrestato, arrestarlo.
   a) Fare clic con il pulsante destro del mouse sul gestore code.
   b) Fare clic su **Arresta**.
4. Fare clic con il pulsante destro del mouse sul gestore code.
5. Fare clic su **Elimina**.

Risultati

Il gestore code è stato eliminato.

Attenzione:

- L'eliminazione di un gestore code è un passo drastico, poiché si eliminano anche le risorse associate al gestore code, incluse tutte le code e i relativi messaggi e tutte le definizioni di oggetti. Se si utilizza il comando **dltmqm** , non viene visualizzata alcuna richiesta che consenta di cambiare idea; quando si preme il tasto Invio, tutte le risorse associate vengono perse.
- In WebSphere MQ per Windows, l'eliminazione di un gestore code rimuove anche il gestore code dall'elenco di avvio automatico (descritto in “Avvio di un gestore code” a pagina 25). Quando il comando è stato completato, viene visualizzato un messaggio `WebSphere MQ queue manager ending` ; non viene indicato che il gestore code è stato eliminato.
- L'eliminazione di un gestore code del cluster non lo rimuove dal cluster. Per ulteriori informazioni, consultare la nota nella descrizione di **dltmqm** .

Per una descrizione del comando **dltmqm** e delle relative opzioni, consultare dltmqm. Assicurarsi che solo gli amministratori attendibili abbiano l'autorità per utilizzare questo comando. Per informazioni sulla sicurezza, consultare Impostazione della sicurezza su Windows, UNIX and Linux systems .

Connessione di applicazioni mediante l'accodamento distribuito

Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra le installazioni WebSphere MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

Prima di leggere questa sezione è utile avere una conoscenza dei canali, delle code e degli altri concetti introdotti in Concetti di intercomunicazione .

Utilizzare le informazioni contenute nei seguenti link per connettere le applicazioni utilizzando l'accodamento distribuito:

- “Come inviare un messaggio a un altro gestore code” a pagina 51
- “Attivazione dei canali” a pagina 68
- “Sicurezza dei messaggi” a pagina 66
- “Tecniche di messaggistica distribuita IBM WebSphere MQ” a pagina 29

- “Introduzione alla gestione delle code distribuite” a pagina 48
- 

“Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 74

Concetti correlati

“Configurazione delle connessioni tra client e server” a pagina 100
Per configurare i collegamenti di comunicazione tra WebSphere MQ i client e i server MQI, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del collegamento, avviare un listener e definire canali.

“Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code” a pagina 422
Modificare il comportamento di IBM WebSphere MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione.

Attività correlate

“Configurazione di un cluster di gestore code” a pagina 161
Utilizzare i link in questo argomento per scoprire come funzionano i cluster, come progettare una configurazione cluster e per ottenere un esempio di come impostare un cluster semplice.

Tecniche di messaggistica distribuita IBM WebSphere MQ

Gli argomenti secondari in questa sezione descrivono le tecniche che sono di uso durante la pianificazione dei canali. Questi argomenti secondari descrivono le tecniche per pianificare come collegare i gestori code e gestire il flusso di messaggi tra le applicazioni.

Per esempi di pianificazione del canale di messaggi, consultare:

- Esempio di pianificazione del canale di messaggi per piattaforme distribuite

Concetti correlati

“Connessione di applicazioni mediante l'accodamento distribuito” a pagina 28
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra le installazioni WebSphere MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

Canali

Introduzione all'accodamento dei messaggi

Concetti di intercomunicazione

Riferimenti correlati

Informazioni di configurazione di esempio

controllo del flusso di messaggi

Il controllo del flusso di messaggi è un'attività che implica l'impostazione e la manutenzione delle serie di messaggi tra gestori code. È importante per gli instradamenti che attraversano più gestori code. Questa sezione descrive come utilizzare code, definizioni di code alias e canali di messaggi sul sistema per ottenere il controllo del flusso di messaggi.

Il flusso di messaggi viene controllato utilizzando una serie di tecniche introdotte in “Connessione di applicazioni mediante l'accodamento distribuito” a pagina 28. Se il gestore code si trova in un cluster, il flusso di messaggi viene controllato utilizzando tecniche differenti, come descritto in “controllo del flusso di messaggi” a pagina 29.

È possibile utilizzare i seguenti oggetti per ottenere il controllo del flusso di messaggi:

- Code di trasmissione
- Canali dei messaggi
- Definizione di coda remota
- Definizione alias del gestore code
- Definizione alias coda di risposta

Il gestore code e gli oggetti coda sono descritti in Oggetti . I canali di messaggi sono descritti in Componenti di accodamento distribuiti . Le tecniche seguenti utilizzano questi oggetti per creare flussi di messaggi nel sistema:

- Inserimento di messaggi nelle code remote
- Instradamento mediante particolari code di trasmissione
- ricezione di messaggi
- Passaggio di messaggi attraverso il sistema
- Separazione dei flussi di messaggi
- Passaggio di un flusso di messaggi a un'altra destinazione
- Risoluzione del nome della coda di risposta in un nome alias

Nota

Tutti i concetti descritti in questa sezione sono rilevanti per tutti i nodi in una rete e includono le estremità di invio e ricezione dei canali di messaggi. Per questo motivo, nella maggior parte degli esempi viene illustrato un solo nodo. L'eccezione si verifica quando l'esempio richiede una cooperazione esplicita da parte dell'amministratore all'altra estremità di un canale di messaggi.

Prima di procedere con le tecniche individuali, è utile ricapitolare i concetti di risoluzione dei nomi e i tre modi di utilizzare le definizioni di coda remota. Vedere Concetti di intercomunicazione.

Concetti correlati

“Nomi coda nell'intestazione di trasmissione” a pagina 30
I nomi delle code di destinazione viaggiano con il messaggio nell'intestazione di trasmissione fino a quando non viene raggiunta la coda di destinazione.

“Come creare il gestore code e gli alias di risposta” a pagina 30
Questo argomento illustra i tre modi in cui è possibile creare una definizione di coda remota.

Nomi coda nell'intestazione di trasmissione

I nomi delle code di destinazione viaggiano con il messaggio nell'intestazione di trasmissione fino a quando non viene raggiunta la coda di destinazione.

Il nome della coda utilizzato dall'applicazione, il nome della coda logica, viene risolto dal gestore code nel nome coda di destinazione. In altre parole, il nome della coda fisica. Questo nome della coda di destinazione viaggia con il messaggio in un'area dati separata, l'intestazione di trasmissione, fino a quando non viene raggiunta la coda di destinazione. L'intestazione di trasmissione viene quindi svuotata.

Modificare la parte del gestore code di questo nome coda quando si creano classi parallele di servizio. Ricordarsi di restituire il nome del gestore code al nome originale quando è stata raggiunta la fine della deviazione della classe di servizio.

Come creare il gestore code e gli alias di risposta

Questo argomento illustra i tre modi in cui è possibile creare una definizione di coda remota.

L'oggetto di definizione della coda remota viene utilizzato in tre modi diversi. Tabella 3 a pagina 31 spiega come definire ciascuno dei tre modi:

- Utilizzo di una definizione di coda remota per ridefinire un nome di coda locale.

  L'applicazione fornisce solo il nome coda quando si apre una coda e questo nome coda è il nome della definizione della coda remota.

  La definizione della coda remota contiene i nomi della coda di destinazione e del gestore code. Facoltativamente, la definizione può contenere il nome della coda di trasmissione da utilizzare. Se non viene fornito alcun nome della coda di trasmissione, il gestore code utilizza il nome del gestore code, ricavato dalla definizione della coda remota, per il nome della coda di trasmissione. Se una coda di

trasmissione con questo nome non è definita, ma è definita una coda di trasmissione predefinita, viene utilizzata la coda di trasmissione predefinita.

- Utilizzo di una definizione di coda remota per ridefinire un nome gestore code.

  L'applicazione o il programma del canale, fornisce un nome coda insieme al nome del gestore code remoto quando si apre la coda.

  Se è stata fornita una definizione di coda remota con lo stesso nome del gestore code e il nome della coda è stato lasciato vuoto, il gestore code sostituisce il nome del gestore code nella chiamata aperta con il nome del gestore code nella definizione.

  Inoltre, la definizione può contenere il nome della coda di trasmissione da utilizzare. Se non viene fornito alcun nome della coda di trasmissione, il gestore code prende il nome del gestore code, preso dalla definizione della coda remota, per il nome della coda di trasmissione. Se una coda di trasmissione con questo nome non è definita, ma è definita una coda di trasmissione predefinita, viene utilizzata la coda di trasmissione predefinita.
- Utilizzo di una definizione di coda remota per ridefinire un nome di coda di risposta.

  Ogni volta che un'applicazione inserisce un messaggio in una coda, può fornire il nome di una coda di risposta per i messaggi di risposta, ma con il nome del gestore code vuoto.

  Se si fornisce una definizione di coda remota con lo stesso nome della coda di risposta, il gestore code locale sostituisce il nome della coda di risposta con il nome della coda dalla propria definizione.

  È possibile fornire un nome gestore code nella definizione, ma non un nome coda di trasmissione.

Tabella 3. Tre modi di utilizzare l'oggetto di definizione della coda remota

Utilizzo	**Nome del gestore code**	**Nome coda**	**Nome coda di trasmissione**
1. Definizione coda remota (su chiamata OPEN)			
Fornito nella chiamata	QM locale o vuoto	(*) richiesto	-
Fornito nella definizione	richiesto	richiesto	facoltativo
2. Alias gestore code (su chiamata OPEN)			
Fornito nella chiamata	(*) richiesto e non QM locale	richiesto	-
Fornito nella definizione	richiesto	vuoto	facoltativo
3. Alias coda di risposta (su chiamata PUT)			
Fornito nella chiamata	vuoto	(*) richiesto	-
Fornito nella definizione	facoltativo	facoltativo	vuoto
Nota: (*) indica che questo nome è il nome dell'oggetto definizione			

Per una descrizione formale, consultare Risoluzione nome coda.

Inserimento di messaggi nelle code remote

È possibile utilizzare oggetti di definizione della coda remota per risolvere un nome coda in una coda di trasmissione in un gestore code adiacente.

In un ambiente di accodamento distribuito, una coda di trasmissione e un canale sono il punto focale per tutti i messaggi in un'ubicazione, indipendentemente dal fatto che i messaggi provengano da applicazioni nel sistema locale o da canali provenienti da un sistema adiacente. Figura 2 a pagina 32 mostra un'applicazione che posiziona i messaggi su una coda logica denominata 'QA_norm'. La risoluzione dei nomi utilizza la definizione della coda remota 'QA_norm' per selezionare la coda di trasmissione QMB. Aggiunge quindi un'intestazione di trasmissione ai messaggi che indicano 'QA_norm at QMB'.

I messaggi provenienti dal sistema adiacente su 'Channel_back' hanno un'intestazione di trasmissione con il nome della coda fisica 'QA_norm at QMB', ad esempio. Questi messaggi non vengono modificati nella coda di trasmissione QMB.

Il canale sposta i messaggi in un gestore code adiacente.

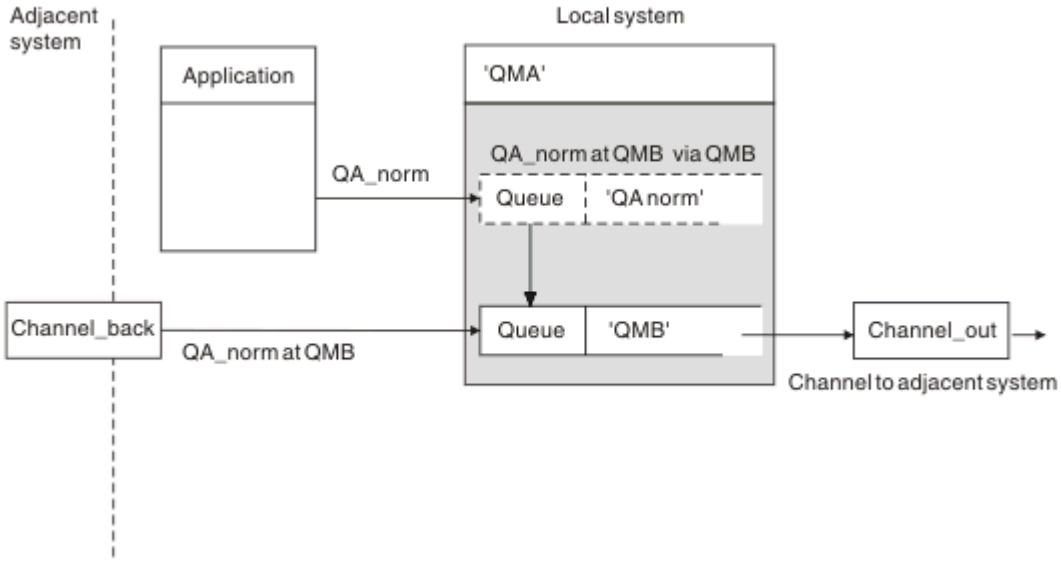


Figura 2. Una definizione di coda remota viene utilizzata per risolvere un nome coda in una coda di trasmissione in un gestore code adiacente

Se si è l'amministratore di sistema di WebSphere MQ , è necessario:

- Definire il canale di messaggi dal sistema adiacente
- Definire il canale dei messaggi per il sistema adiacente
- Crea la coda di trasmissione QMB
- Definire l'oggetto coda remota 'QA_norm' per risolvere il nome della coda utilizzato dalle applicazioni nel nome della coda di destinazione, nel nome del gestore code di destinazione e nel nome della coda di trasmissione

In un ambiente cluster, è necessario definire solo un canale ricevente del cluster sul gestore code locale. Non è necessario definire una coda di trasmissione o un oggetto coda remota. Per informazioni, consultare Cluster .

Ulteriori informazioni sulla risoluzione dei nomi

L'effetto della definizione della coda remota è definire un nome coda di destinazione fisica e un nome gestore code. Questi nomi vengono inseriti nelle intestazioni di trasmissione dei messaggi.

Per i messaggi in entrata da un sistema adiacente è già stato eseguito questo tipo di risoluzione dei nomi dal gestore code originale. Pertanto, hanno l'intestazione di trasmissione che visualizza il nome della coda di destinazione fisica e il nome del gestore code. Questi messaggi non sono influenzati dalle definizioni della coda remota.

Scelta della coda di trasmissione

È possibile utilizzare una definizione di coda remota per consentire a una diversa coda di trasmissione di inviare messaggi allo stesso gestore code adiacente.

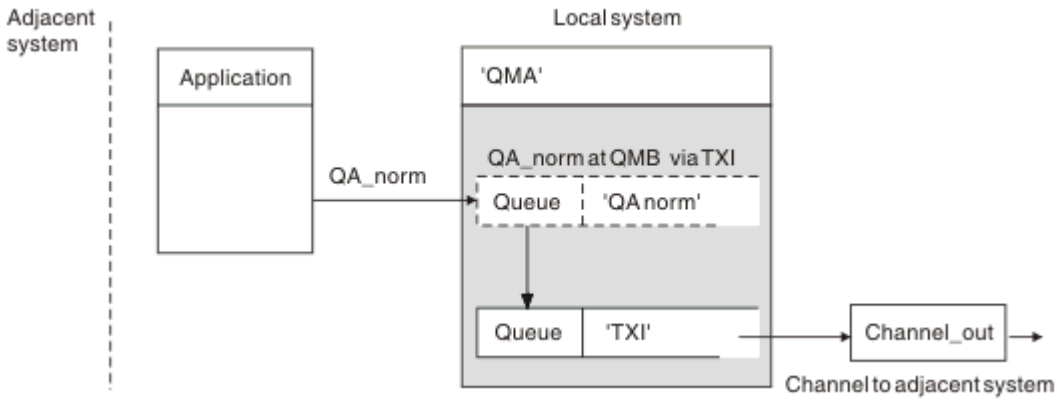


Figura 3. La definizione della coda remota consente l'utilizzo di una coda di trasmissione diversa

In un ambiente di accodamento distribuito, quando è necessario modificare un flusso di messaggi da un canale all'altro, utilizzare la stessa configurazione di sistema come mostrato in Figura 2 a pagina 32 in “Inserimento di messaggi nelle code remote” a pagina 31. Figura 3 a pagina 33 in questo argomento mostra come utilizzare la definizione della coda remota per inviare messaggi su una coda di trasmissione differente, e quindi su un canale differente, allo stesso gestore code adiacente.

Per la configurazione mostrata in Figura 3 a pagina 33, è necessario specificare l'oggetto coda remota 'QA_norm' e la coda di trasmissione 'TX1'. È necessario fornire 'QA_norm' per scegliere la coda 'QA_norm' sul Gestore code remoto, la coda di trasmissioneTX1'e il gestore code' QMB_priority '. Specificare 'TX1' nella definizione del canale adiacente al sistema.

I messaggi vengono inseriti nella coda di trasmissione 'TX1' con un'intestazione di trasmissione contenente 'QA_norm at QMB_priority' e inviati sul canale al sistema adiacente.

Il channel_back è stato lasciato fuori da questa illustrazione perché avrebbe bisogno di un alias del gestore code.

In un ambiente cluster, non è necessario definire una coda di trasmissione o una definizione di coda remota. Per ulteriori informazioni, vedere “Code cluster” a pagina 168.

ricezione di messaggi

È possibile configurare il gestore code in modo che riceva messaggi da altri gestori code. È necessario assicurarsi che non si verifichi una risoluzione del nome non intenzionale.

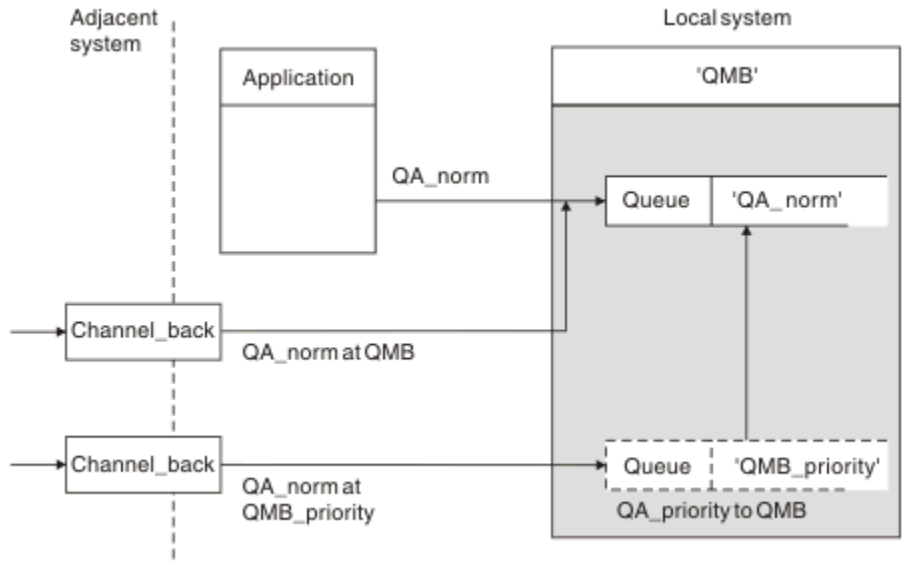


Figura 4. Ricezione diretta dei messaggi e risoluzione del nome del gestore code alias

Oltre a disporre l'invio dei messaggi, l'amministratore di sistema deve anche disporre la ricezione dei messaggi dai gestori code adiacenti. I messaggi ricevuti contengono il nome fisico del gestore code di destinazione e la coda nell'intestazione di trasmissione. Vengono trattati come messaggi da un'applicazione locale che specifica sia il nome del gestore code che il nome della coda. A causa di questo trattamento, è necessario assicurarsi che i messaggi che entrano nel sistema non abbiano una risoluzione del nome non intenzionale eseguita. Consultare Figura 4 a pagina 33 per questo scenario.

Per questa configurazione, è necessario preparare:

- Canali di messaggi per ricevere messaggi da gestori code adiacenti
- Una definizione alias del gestore code per risolvere un flusso di messaggi in entrata, 'QMB_priority', nel nome del gestore code locale, 'QMB'
- La coda locale, 'QA_norm', se non esiste

Ricezione di nomi di gestori code alias

L'utilizzo della definizione alias del gestore code in questa illustrazione non ha selezionato un gestore code di destinazione differente. I messaggi che passano attraverso questo gestore code locale e indirizzati a 'QMB_priority' sono destinati al gestore code 'QMB'. Il nome del gestore code alias viene utilizzato per creare il flusso di messaggi separato.

Passaggio di messaggi attraverso il sistema

È possibile passare i messaggi attraverso il proprio sistema in tre modi: utilizzando il nome ubicazione, utilizzando un alias per il gestore code o selezionando una coda di trasmissione.

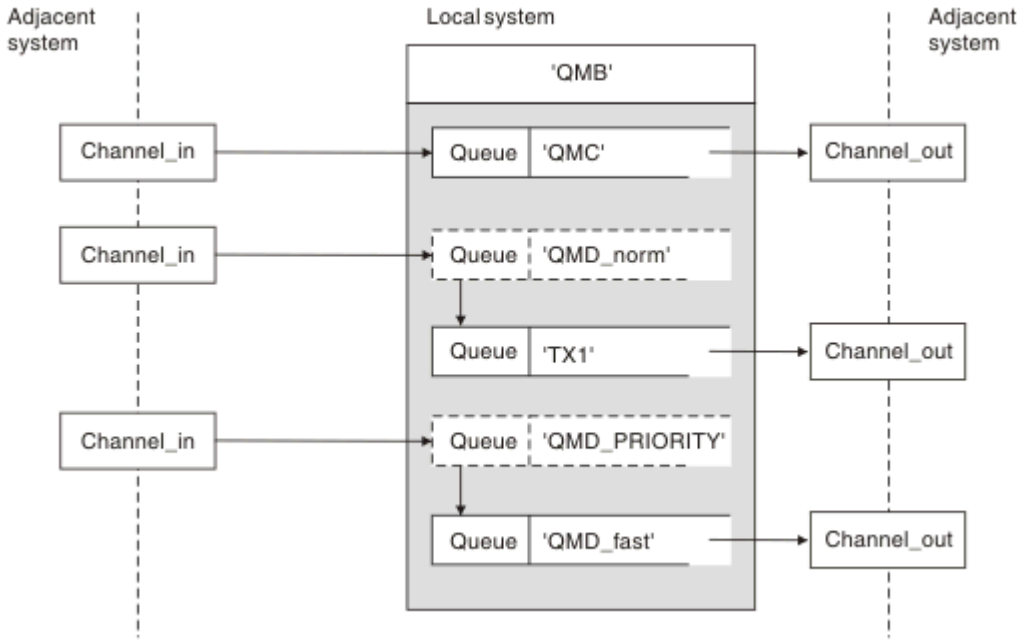


Figura 5. Tre metodi di trasmissione dei messaggi attraverso il sistema

La tecnica mostrata in Figura 4 a pagina 33 in “ricezione di messaggi” a pagina 33, ha mostrato come viene catturato un flusso alias. Figura 5 a pagina 34 illustra il modo in cui si costruiscono le reti riunendo le tecniche precedentemente descritte.

La configurazione mostra un canale che consegna tre messaggi con destinazioni differenti:

1. QB alle QMC
2. QB alle QMD_norm
3. QB alle QMD_PRIORITY

È necessario passare il primo flusso di messaggi attraverso il sistema senza modifiche. È necessario passare il secondo flusso di messaggi attraverso una coda di trasmissione e un canale differenti. Per il secondo flusso di messaggi, è necessario anche risolvere i messaggi per il nome gestore code alias QMD_norm nel gestore code QMD. Il terzo flusso di messaggi sceglie una coda di trasmissione diversa senza altre modifiche.

In un ambiente cluster, i messaggi vengono trasmessi attraverso una coda di trasmissione cluster. Di solito, una singola coda di trasmissione, SYSTEM.CLUSTER.TRANSMIT.QUEUE, trasferisce tutti i messaggi a tutti i gestori code in tutti i cluster di cui è membro il gestore code; consultare Un cluster di gestori code. È possibile definire code di trasmissione separate per tutti o per alcuni dei gestori code nei cluster di cui il gestore code è membro.

I seguenti metodi descrivono le tecniche applicabili a un ambiente di accodamento distribuito.

Utilizza questi metodi

Per queste configurazioni, è necessario preparare:

- Definizioni del canale di input
- Definizioni del canale di output
- Code di trasmissione:
  - QMC
  - TX1
  - QMD_fast
- Definizioni alias del gestore code:
  - QMD_norm con QMD_norm per QMD tramite TX1
  - QMD_PRIORITY con QMD_PRIORITY per QMD_PRIORITY tramite QMD_fast

Nota: Nessuno dei flussi di messaggi visualizzati nell'esempio modifica la coda di destinazione. Gli alias del nome gestore code forniscono la separazione dei flussi di messaggi.

Metodo 1: utilizzare il nome dell'ubicazione in entrata

Si riceveranno messaggi con un'intestazione di trasmissione contenente un altro nome di ubicazione, ad esempio QMC. La configurazione più semplice consiste nel creare una coda di trasmissione con tale nome, QMC. Il canale che servizi la coda di trasmissione distribuisce il messaggio non modificato alla destinazione successiva.

Metodo 2: utilizzare un alias per il gestore code

Il secondo metodo consiste nell'utilizzare la definizione dell'oggetto alias del Gestore code, ma specificare un nuovo nome di ubicazione, QMD, e una particolare coda di trasmissione, TX1. Questa azione:

- Termina la configurazione del flusso di messaggi alias mediante l'alias del nome gestore code QMD_norm, ossia la classe di servizio denominata QMD_norm.
- Modifica le intestazioni di trasmissione su questi messaggi da QMD_norm a QMD.

Metodo 3: selezionare una coda di trasmissione

Il terzo metodo consiste nell'avere un oggetto alias del gestore code definito con lo stesso nome dell'ubicazione di destinazione, QMD_PRIORITY. Utilizzare la definizione di alias del gestore code per selezionare una coda di trasmissione particolare, QMD_fast, e quindi un altro canale. Le intestazioni di trasmissione su questi messaggi rimangono invariate.

Separazione dei flussi di messaggi

È possibile utilizzare un alias del gestore code per creare flussi di messaggi separati per inviare messaggi allo stesso gestore code.

In un ambiente di accodamento distribuito, la necessità di separare i messaggi nello stesso gestore code in flussi di messaggi differenti può verificarsi per una serie di ragioni. Ad esempio:

- Potrebbe essere necessario fornire un flusso separato per i messaggi grandi, medi e piccoli. Questa necessità si applica anche in un ambiente di cluster e, in questo caso, è possibile creare cluster che si sovrappongono. Ci sono una serie di motivi per cui è possibile farlo, ad esempio:
  - Per consentire alle diverse organizzazioni di avere la propria amministrazione.
  - Per consentire la gestione separata delle applicazioni indipendenti.
  - Per creare una classe di servizio. Ad esempio, è possibile avere un cluster denominato STAFF che è un sottoinsieme del cluster denominato STUDENTI. Quando si inserisce un messaggio in una coda pubblicizzata nel cluster STAFF, viene utilizzato un canale limitato. Quando si inserisce un messaggio in una coda pubblicizzata nel cluster STUDENTI, è possibile utilizzare un canale generale o un canale limitato.
  - Per creare ambienti di test e di produzione.
- Potrebbe essere necessario instradare i messaggi in entrata in base a percorsi differenti dal percorso dei messaggi generati localmente.
- L'installazione potrebbe richiedere di pianificare lo spostamento dei messaggi in determinati orari (ad esempio, durante la notte) e i messaggi devono quindi essere memorizzati in code riservate fino a quando non vengono pianificati.

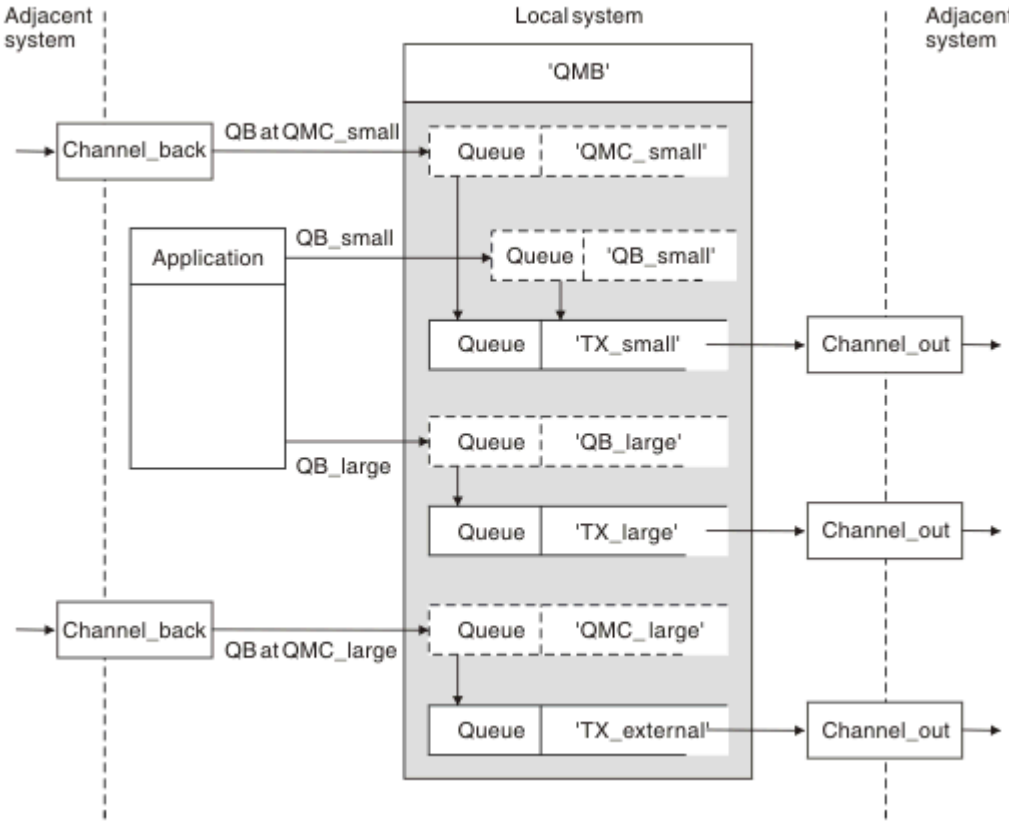


Figura 6. Separazione dei flussi di messaggi

Nell'esempio mostrato in Figura 6 a pagina 36, i due flussi in entrata sono l'alias dei nomi dei gestori code 'QMC_small' e 'QMC_large '. Fornire a questi flussi una definizione di alias del gestore code per catturare tali flussi per il gestore code locale. Si dispone di un'applicazione che si rivolge a due code remote ed

è necessario che questi flussi di messaggi siano tenuti separati. Si forniscono due definizioni di coda remota che specificano la stessa posizione, 'QMC', ma specificano code di trasmissione differenti. Questa definizione mantiene separati i flussi e non è necessario alcun elemento aggiuntivo all'estremità poiché hanno lo stesso nome gestore code di destinazione nelle intestazioni di trasmissione. L'utente fornisce:

- Le definizioni di canale in ingresso
- Le due definizioni di coda remota QB_small e QB_large
- Le due definizioni di alias del gestore code QMC_small e QMC_large
- Le tre definizioni del canale di invio
- Tre code di trasmissione: TX_small, TX_large e TX_external

Coordinamento con sistemi adiacenti

Quando si utilizza un nome alternativo del gestore code per creare un flusso di messaggi separato, è necessario coordinare questa attività con l'amministratore di sistema all'estremità remota del canale di messaggi per assicurarsi che l'alias del gestore code corrispondente sia disponibile.

Concentrare i messaggi in diverse ubicazioni

È possibile concentrare i messaggi destinati a varie ubicazioni su un singolo canale.

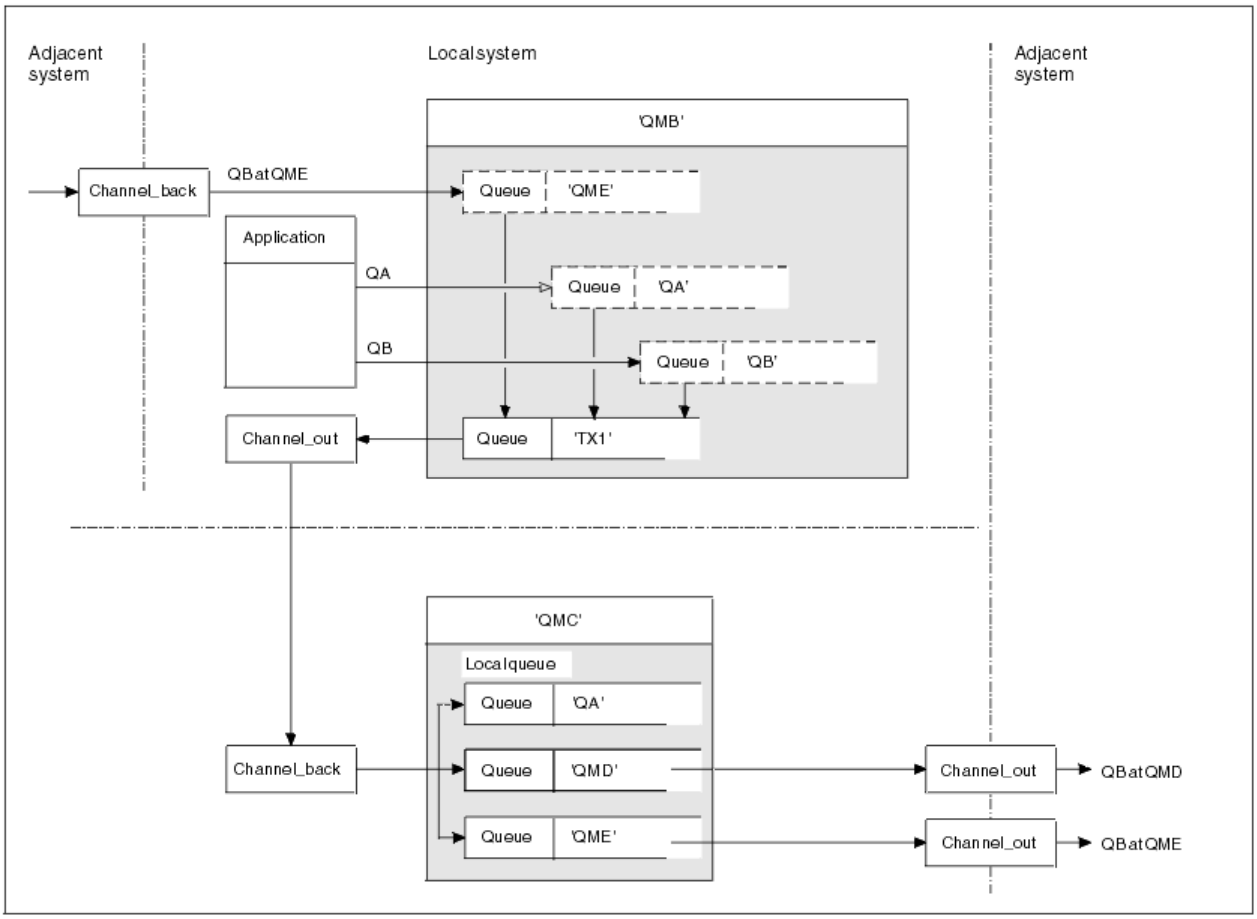


Figura 7. Combinazione dei flussi di messaggi su un canale

La Figura 7 a pagina 37 illustra una tecnica di accodamento distribuito per concentrare i messaggi destinati a varie ubicazioni su un canale. Due possibili utilizzi sono:

- Concentrazione del traffico di messaggi attraverso un gateway

- Utilizzo delle autostrade ad ampia larghezza di banda tra i nodi

In questo esempio, i messaggi provenienti da origini diverse, locali e adiacenti, con code di destinazione e gestori code differenti, vengono trasmessi attraverso la coda di trasmissione 'TX1' al gestore code QMC. Il gestore code QMC consegna i messaggi in base alle destinazioni. Uno impostato su una coda di trasmissione 'QMD' per la trasmissione in avanti al gestore code QMD. Un altro è impostato su una coda di trasmissione 'QME' per la trasmissione successiva al gestore code QME. Altri messaggi vengono inseriti nella coda locale 'QA'.

È necessario fornire:

- Definizioni canale
- Coda di trasmissione TX1
- Definizioni coda remota:
  - QA con 'QA su QMC tramite TX1'
  - QB con 'QB a QMD tramite TX1'
- Definizione alias gestore code:
  - QME con 'QME tramite TX1'

L'amministratore complementare che sta configurando QMC deve fornire:

- Ricezione della definizione di canale con lo stesso nome canale
- QMD coda di trasmissione con definizione canale di invio associata
- QME coda di trasmissione con definizione canale di invio associata
- QA oggetto coda locale.

Deviazione dei flussi di messaggi in un'altra destinazione

È possibile ridefinire la destinazione di alcuni messaggi utilizzando gli alias del gestore code e le code di trasmissione.

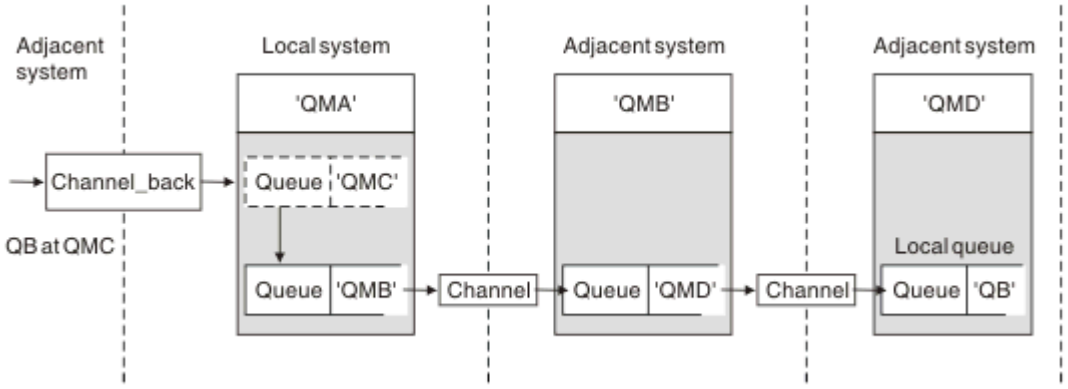


Figura 8. Deviazione dei flussi di messaggi in un'altra destinazione

Figura 8 a pagina 38 illustra come ridefinire la destinazione di determinati messaggi. I messaggi in entrata in QMA sono destinati a 'QB in QMC'. Normalmente arrivano a QMA e vengono posizionati su una coda di trasmissione chiamata QMC che è stata parte di un canale a QMC. QMA deve deviare i messaggi su QMD, ma è in grado di raggiungere QMD solo su QMB. Questo metodo è utile quando è necessario spostare un servizio da un'ubicazione all'altra e consentire ai sottoscrittori di continuare a inviare messaggi su base temporanea fino a quando non si sono adattati al nuovo indirizzo.

Il metodo di reinstradamento dei messaggi in entrata destinati per un determinato gestore code a un gestore code differente utilizza:

- Un alias del gestore code per modificare il gestore code di destinazione in un altro gestore code e per selezionare una coda di trasmissione per il sistema adiacente

- Una coda di trasmissione per servire il gestore code adiacente
- Una coda di trasmissione sul gestore code adiacente per l'instradamento verso il gestore code di destinazione

È necessario fornire:

- Definizione Channel_back
- QMC definizione oggetto alias del gestore code con QB da QMD a QMB
- Definizione Channel_out
- La coda di trasmissione associata QMB

L'amministratore complementare che sta configurando QMB deve fornire:

- La definizione channel_back corrispondente
- La coda di trasmissione, QMD
- La definizione canale associata a QMD

È possibile utilizzare gli alias all'interno di un ambiente cluster. Per informazioni, consultare “Cluster e alias del gestore code” a pagina 263.

Invio di messaggi a un elenco di distribuzione

È possibile utilizzare una singola chiamata MQPUT per fare in modo che un'applicazione invii un messaggio a diverse destinazioni.

In WebSphere MQ su tutte le piattaforme ad eccezione di z/OS, un'applicazione può inviare un messaggio a diverse destinazioni con una singola chiamata MQPUT. È possibile eseguire questa operazione sia in un ambiente di accodamento distribuito che in un ambiente cluster. È necessario definire le destinazioni in un elenco di distribuzione, come descritto in Elenchi di distribuzione.

Non tutti i gestori code supportano gli elenchi di distribuzione. Quando un MCA stabilisce una connessione con un partner, determina se il partner supporta gli elenchi di distribuzione e imposta di conseguenza un indicatore sulla coda di trasmissione. Se un'applicazione tenta di inviare un messaggio destinato ad un elenco di distribuzione ma il partner non supporta gli elenchi di distribuzione, l'MCA mittente intercetta il messaggio e lo inserisce nella coda di trasmissione una volta per ciascuna destinazione prevista.

Un MCA di ricezione garantisce che i messaggi inviati a un elenco di distribuzione vengano ricevuti in modo sicuro in tutte le destinazioni previste. Se qualche destinazione ha esito negativo, l'MCA stabilisce quali destinazioni hanno avuto esito negativo. Può quindi generare report di eccezioni e provare a inviare nuovamente i messaggi.

Coda di risposta

È possibile creare un loop di elaborazione coda remota completo utilizzando una coda di risposta.

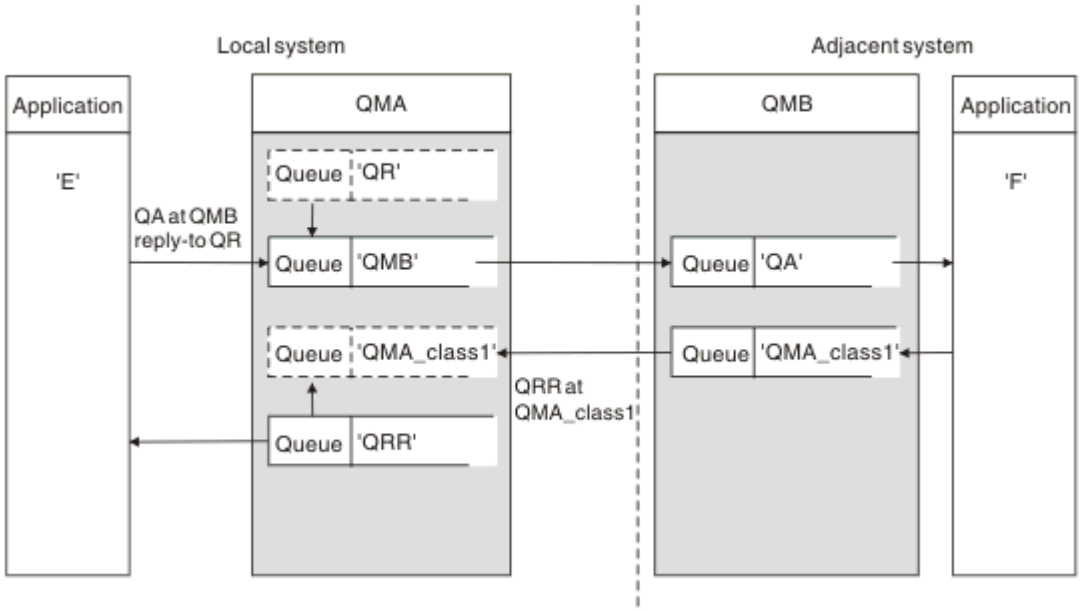


Figura 9. Sostituzione del nome della coda di risposta durante la chiamata PUT

Un loop di elaborazione della coda remota completo che utilizza una coda di risposta viene visualizzato in Figura 9 a pagina 40. Questo loop si applica sia in un ambiente di accodamento distribuito che in un ambiente cluster. I dettagli sono come mostrato in Tabella 7 a pagina 47.

L'applicazione apre QA a QMB e inserisce i messaggi su tale coda. Ai messaggi viene fornito un nome coda di risposta QR, senza specificare il nome del gestore code. QMA del gestore code trova l'oggetto coda di risposta QR ed estrae da esso il nome alias di QRR e il nome gestore code QMA_class1. Questi nomi vengono inseriti nei campi di risposta dei messaggi.

I messaggi di risposta dalle applicazioni in QMB vengono indirizzati a QRR in QMA_class1. La definizione del nome alias del gestore code QMA_class1 viene utilizzata dal gestore code per trasmettere i messaggi a se stesso e alla coda QRR.

Questo scenario illustra il modo in cui le applicazioni possono scegliere una classe di servizio per i messaggi di risposta. La classe è implementata dalla coda di trasmissione QMA_class1 in QMB, insieme alla definizione dell'alias del gestore code, QMA_class1 in QMA. In questo modo, è possibile modificare la coda di risposta dell'applicazione in modo che i flussi siano segregati senza coinvolgere l'applicazione. L'applicazione sceglie sempre QR per questa particolare classe di servizi. È possibile modificare la classe di servizi con la definizione della coda di risposta QR.

È necessario creare:

- QR definizione coda di risposta
- QMB oggetto coda di trasmissione
- Definizione Channel_out
- Definizione Channel_back
- Definizione alias gestore code QMA_class1
- Oggetto coda locale QRR, se non esiste

L'amministratore complementare sul sistema adiacente deve creare:

- Definizione di canale di ricezione
- Oggetto coda di trasmissione QMA_class1
- Canale di invio associato
- QA oggetto coda locale.

I programmi applicativi utilizzano:

- Nome coda di risposta a QR nelle chiamate di inserimento
- Nome coda QRR nelle chiamate get

In questo modo, è possibile modificare la classe di servizio come necessario, senza coinvolgere l'applicazione. È possibile modificare l'alias di risposta 'QR', insieme alla coda di trasmissione 'QMA_class1' e all'alias del gestore code 'QMA_class1'.

Se non viene trovato alcun oggetto alias di risposta quando il messaggio viene inserito nella coda, il nome del gestore code locale viene inserito nel campo del nome del gestore code di risposta vuoto. Il nome della coda di risposta rimane invariato.

Limitazione risoluzione nome

Poiché la risoluzione del nome è stata eseguita per la coda di risposta in 'QMA' quando è stato inserito il messaggio originale, non è consentita alcuna ulteriore risoluzione del nome in 'QMB'. Il messaggio viene inserito con il nome fisico della coda reply - to dall'applicazione che risponde.

Le applicazioni devono essere consapevoli che il nome che utilizzano per la coda di risposta è diverso dal nome della coda effettiva in cui si trovano i messaggi di ritorno.

Ad esempio, quando due classi di servizio vengono fornite per l'utilizzo di applicazioni con nomi alias coda reply - to 'C1_alias' e 'C2_alias', le applicazioni utilizzano questi nomi come nomi coda reply - to nelle chiamate di inserimento messaggi. Tuttavia, le applicazioni in realtà prevedono che i messaggi vengano visualizzati nelle code 'C1' per 'C1_alias' e 'C2' per 'C2_alias'.

Tuttavia, un'applicazione è in grado di effettuare una chiamata di interrogazione sulla coda alias di risposta per controllare il nome della coda reale che deve utilizzare per ottenere i messaggi di risposta.

Concetti correlati

“Come creare il gestore code e gli alias di risposta” a pagina 30
Questo argomento illustra i tre modi in cui è possibile creare una definizione di coda remota.

“Esempio di alias della coda reply - to” a pagina 41
Questo esempio illustra l'utilizzo di un alias reply - to per selezionare un instradamento differente (coda di trasmissione) per i messaggi restituiti. L'utilizzo di questa funzionalità richiede la modifica del nome della coda di risposta in collaborazione con le applicazioni.

“Funzionamento dell'esempio” a pagina 43
Una spiegazione dell'esempio e del modo in cui il gestore code utilizza l'alias della coda di risposta.

“Procedura dettagliata per l'alias della coda di risposta” a pagina 44
Una procedura dettagliata del processo da un'applicazione che immette un messaggio su una coda remota alla stessa applicazione che rimuove il messaggio di risposta dalla coda di risposta alias.

Esempio di alias della coda reply - to

Questo esempio illustra l'utilizzo di un alias reply - to per selezionare un instradamento differente (coda di trasmissione) per i messaggi restituiti. L'utilizzo di questa funzionalità richiede la modifica del nome della coda di risposta in collaborazione con le applicazioni.

Come mostrato in Figura 10 a pagina 42, l'instradamento di ritorno deve essere disponibile per i messaggi di risposta, inclusi la coda di trasmissione, il canale e l'alias del gestore code.

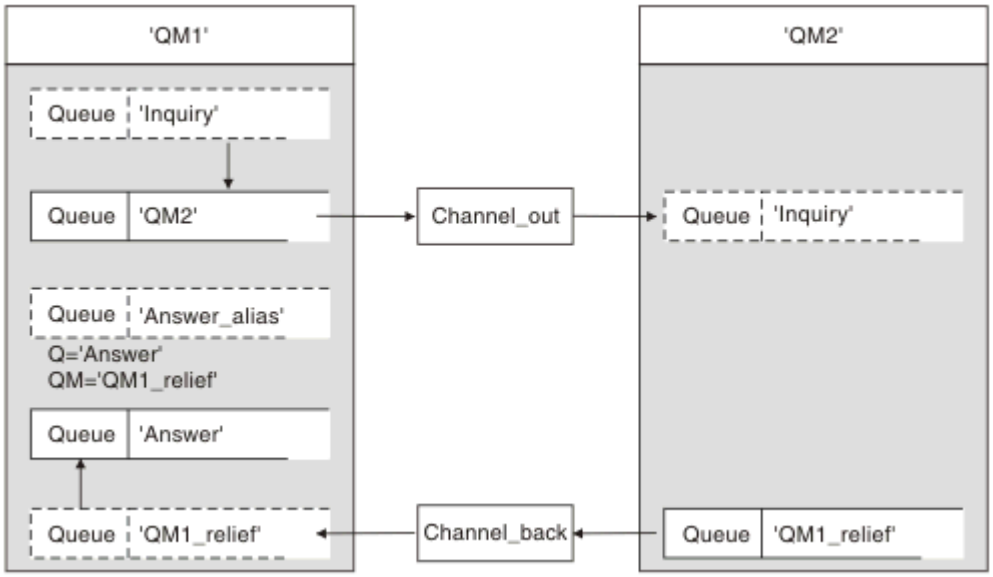


Figura 10. Esempio di alias della coda reply - to

Questo esempio è per le applicazioni del richiedente in 'QM1' che inviano messaggi alle applicazioni server in 'QM2'. I messaggi sul server devono essere restituiti tramite un canale alternativo utilizzando la coda di trasmissione 'QM1_relief' (il canale di ritorno predefinito viene servito con una coda di trasmissione 'QM1').

L'alias della coda di risposta è un utilizzo particolare della definizione della coda remota denominata 'Answer_alias'. Le applicazioni in QM1 includono questo nome, 'Answer_alias', nel campo di risposta di tutti i messaggi che inseriscono nella coda 'Inquiry'.

La definizione della coda di risposta 'Answer_alias' è definita come 'Risposta a QM1_relief'. Le applicazioni in QM1 prevedono che le loro risposte vengano visualizzate nella coda locale denominata 'Risposta'.

Le applicazioni server in QM2 utilizzano il campo di risposta dei messaggi ricevuti per ottenere i nomi della coda e del gestore code per i messaggi di risposta al richiedente in QM1.

Definizioni utilizzate in questo esempio in QM1

L'amministratore di sistema di WebSphere MQ all'indirizzo QM1 deve garantire che la coda di risposta 'Risposta' sia creata insieme agli altri oggetti. Il nome dell'alias del gestore code, contrassegnato con un '*', deve essere in accordo con il nome del gestore code nella definizione dell'alias della coda di risposta, contrassegnato anche con un '*'.

Oggetto	**Definizione**	
Coda di trasmissione locale	QM2	
Definizione di coda remota	Nome oggetto	Interrogazione
	Nome gestore code remoto	QM2
	Nome coda remota	Interrogazione
	Nome coda di trasmissione	QM2 (PREDEFINITO)
Alias gestore code	Nome oggetto	QM1_relief *
	Nome del gestore code	QM1
	Nome coda	(vuoto)
Alias coda di risposta	Nome oggetto	Alias_risposta
	Nome gestore code remoto	QM1_relief *

Oggetto	Definizione	
	Nome coda remota	Risposta

Inserisci definizione in QM1

Le applicazioni compilano i campi di risposta con il nome alias della coda di risposta e lasciano vuoto il campo del nome del gestore code.

Campo	Contenuto
Nome coda	Interrogazione
Nome del gestore code	(vuoto)
Nome delle repliche alla coda	Alias_risposta
Gestore code di risposta	(vuoto)

Definizioni utilizzate in questo esempio in QM2

L'amministratore del sistema WebSphere MQ in QM2 deve assicurarsi che la coda locale esista per i messaggi in entrata e che la coda di trasmissione correttamente denominata sia disponibile per i messaggi di risposta.

Oggetto	Definizione
Coda locale	Interrogazione
Coda di trasmissione	QM1_relief

Inserire la definizione in QM2

Le applicazioni in QM2 richiamano il nome della coda di risposta e il nome del gestore code dal messaggio originale e li utilizzano durante l'inserimento del messaggio di risposta nella coda di risposta.

Campo	Contenuto
Nome coda	Risposta
Nome del gestore code	QM1_relief

Funzionamento dell'esempio

Una spiegazione dell'esempio e del modo in cui il gestore code utilizza l'alias della coda di risposta.

In questo esempio, le applicazioni del richiedente in QM1 utilizzano sempre 'Answer_alias' come coda di risposta nel relativo campo della chiamata put. Richiamano sempre i messaggi dalla coda denominata 'Risposta'.

Le definizioni degli alias della coda di risposta sono disponibili per l'utilizzo da parte dell'amministratore di sistema QM1 per modificare il nome della coda di risposta 'Risposta' e dell'instradamento di ritorno 'QM1_relief'.

La modifica del nome della coda 'Risposta' di solito non è utile perché le applicazioni QM1 si aspettano le risposte in questa coda. Tuttavia, l'amministratore di sistema QM1 è in grado di modificare il percorso di ritorno (classe di servizio), se necessario.

Modalità con cui il gestore code utilizza l'alias della coda di risposta

Il gestore code QM1 richiama le definizioni dall'alias della coda di risposta quando il nome della coda di risposta, incluso nella chiamata di inserimento dall'applicazione, è uguale all'alias della coda di risposta e la parte del gestore code è vuota.

Il gestore code sostituisce il nome della coda di risposta nella chiamata di inserimento con il nome della coda dalla definizione. Sostituisce il nome del gestore code vuoto nella chiamata di inserimento con il nome del gestore code dalla definizione.

Questi nomi vengono portati con il messaggio nel descrittore del messaggio.

Tabella 4. Alias coda di risposta

Nome campo	**Inserisci chiamata**	**Intestazione trasmissione**
Nome delle repliche alla coda	Alias_risposta	Risposta
Nome gestore code di risposta	(vuoto)	QM1_relief

Procedura dettagliata per l'alias della coda di risposta

Una procedura dettagliata del processo da un'applicazione che immette un messaggio su una coda remota alla stessa applicazione che rimuove il messaggio di risposta dalla coda di risposta alias.

Per completare questo esempio, guardiamo il processo.

1. L'applicazione apre una coda denominata 'Inquiry' e vi inserisce i messaggi. L'applicazione imposta i campi reply - to del descrittore del messaggio su:

Nome delle repliche alla coda	**Alias_risposta**
Nome gestore code di risposta	(vuoto)

2. Il gestore code 'QM1' risponde al nome del gestore code vuoto controllando la definizione di una coda remota con il nome 'Answer_alias'. In caso contrario, il gestore code inserisce il proprio nome, 'QM1', nel campo del gestore code di risposta del descrittore del messaggio.
3. Se il gestore code trova una definizione di coda remota con il nome 'Answer_alias', estrae il nome coda e i nomi gestore code dalla definizione (nome coda = 'Risposta' e nome gestore code = 'QM1_relief'). Quindi, li inserisce nei campi reply - to del descrittore del messaggio.
4. Il gestore code 'QM1' utilizza la definizione della coda remota 'Inquiry' per stabilire che la coda di destinazione prevista si trova sul gestore code 'QM2' e che il messaggio viene inserito nella coda di trasmissione 'QM2'. 'QM2' è il nome della coda di trasmissione predefinita per i messaggi destinati alle code sul gestore code 'QM2'.
5. Quando il gestore code 'QM1' inserisce il messaggio nella coda di trasmissione, aggiunge un'intestazione di trasmissione al messaggio. Questa intestazione contiene il nome della coda di destinazione, 'Inquiry', e il gestore code di destinazione, 'QM2'.
6. Il messaggio arriva al gestore code 'QM2' e viene inserito nella coda locale 'Inquiry'.
7. Un'applicazione richiama il messaggio da questa coda ed elabora il messaggio. L'applicazione prepara un messaggio di risposta e inserisce questo messaggio di risposta nel nome della coda di risposta dal descrittore del messaggio originale:

Nome delle repliche alla coda	**Risposta**
Nome gestore code di risposta	QM1_relief

8. Il gestore code 'QM2' esegue il comando put. Rilevando che il nome del gestore code 'QM1_relief' è un gestore code remoto, posiziona il messaggio sulla coda di trasmissione con lo stesso nome, 'QM1_relief'. Al messaggio viene fornita un'intestazione di trasmissione contenente il nome della coda di destinazione, 'Risposta', e il gestore code di destinazione, 'QM1_relief'.
9. Il messaggio viene trasferito al gestore codeQM1'. Il gestore code, riconosce che il nome del gestore code 'QM1_relief' è un alias, estrae dalla definizione alias 'QM1_relief' il nome del gestore code fisico 'QM1'.
10. Il gestore code 'QM1' inserisce il messaggio nel nome della coda contenuto nell'intestazione di trasmissione, 'Risposta'.
11. L'applicazione estrae il messaggio di risposta dalla coda 'Risposta'.

Considerazioni sulla rete

In un ambiente di accodamento distribuito, poiché le destinazioni dei messaggi vengono indirizzate solo con un nome coda e un nome gestore code, si applicano alcune regole.

1. Dove viene fornito il nome del gestore code e il nome è diverso dal nome del gestore code locale:
   - Una coda di trasmissione deve avere lo stesso nome. Questa coda di trasmissione deve far parte di un canale di messaggi che sposta i messaggi in un altro gestore code oppure
   - È necessario che esista una definizione dell'alias del gestore code per risolvere il nome del gestore code nello stesso nome o in un altro nome del gestore code e nella coda di trasmissione facoltativa oppure
   - Se il nome della coda di trasmissione non può essere risolto ed è stata definita una coda di trasmissione predefinita, viene utilizzata la coda di trasmissione predefinita.
2. Dove viene fornito solo il nome della coda, una coda di qualsiasi tipo ma con lo stesso nome deve essere disponibile sul gestore code locale. Questa coda può essere una definizione di coda remota che si risolve in: una coda di trasmissione a un gestore code adiacente, un nome gestore code e una coda di trasmissione facoltativa.

Per vedere come funziona in un ambiente cluster, consultare gli argomenti appropriati nella sezione Funzionamento dei cluster della documentazione del prodotto.

Si consideri lo scenario di un canale di messaggi che sposta i messaggi da un gestore code ad un altro in un ambiente di accodamento distribuito.

I messaggi spostati sono stati originati da qualsiasi altro gestore code nella rete e potrebbero arrivare alcuni messaggi con un nome gestore code sconosciuto come destinazione. Questo problema può verificarsi quando un nome gestore code è stato modificato o è stato rimosso dal sistema, ad esempio.

Il programma del canale riconosce questa situazione quando non riesce a trovare una coda di trasmissione per questi messaggi e inserisce i messaggi nella coda dei messaggi non recapitati (messaggi non recapitati). È tua responsabilità cercare questi messaggi e fare in modo che vengano inoltrati alla destinazione corretta. In alternativa, restituirli all'originatore, dove l'originatore può essere accertato.

I report di eccezione vengono generati in queste circostanze, se i messaggi di report sono stati richiesti nel messaggio originale.

Convenzione di risoluzione dei nomi

La risoluzione dei nomi che modifica l'identità della coda di destinazione (ossia, la modifica del nome da logico a fisico), si verifica solo una volta e solo sul gestore code di origine.

L'utilizzo successivo delle varie possibilità alias deve essere utilizzato solo quando si separano e si combinano i flussi di messaggi.

Instradamento di ritorno

I messaggi possono contenere un indirizzo di ritorno nel formato del nome di una coda e di un gestore code. Questo modulo di indirizzo di ritorno può essere utilizzato sia in un ambiente di accodamento distribuito che in un ambiente cluster.

Questo indirizzo viene normalmente specificato dall'applicazione che crea il messaggio. Può essere modificato da qualsiasi applicazione che gestisce il messaggio, incluse le applicazioni di uscita utente.

Indipendentemente dall'origine di questo indirizzo, qualsiasi applicazione che gestisce il messaggio potrebbe scegliere di utilizzare questo indirizzo per restituire i messaggi di risposta, di stato o di report all'applicazione di origine.

Il modo in cui vengono instradati questi messaggi di risposta non è diverso dal modo in cui viene instradato il messaggio originale. È necessario tenere presente che i flussi di messaggi creati per altri gestori code richiedono flussi di ritorno corrispondenti.

Conflitti di nomi fisici

Il nome della coda di risposta di destinazione è stato risolto in un nome di coda fisica sul gestore code originale. Non deve essere risolto nuovamente nel gestore code di risposta.

È una probabile possibilità per i problemi di conflitto dei nomi che possono essere evitati solo da un accordo a livello di rete sui nomi delle code fisiche e logiche.

Gestione delle traduzioni dei nomi delle code

Quando si crea una definizione dell'alias del gestore code o una definizione della coda remota, la risoluzione del nome viene eseguita per ogni messaggio che porta quel nome. Questa situazione deve essere gestita.

Questa descrizione viene fornita per progettisti di applicazioni e pianificatori di canali interessati a un singolo sistema che dispone di canali di messaggi per sistemi adiacenti. Prende una visione locale di pianificazione e controllo del canale.

Quando si crea una definizione dell'alias del gestore code o una definizione della coda remota, la risoluzione del nome viene eseguita per ogni messaggio che contiene tale nome, indipendentemente dall'origine del messaggio. Per sovrintendere a questa situazione, che potrebbe coinvolgere un numero elevato di code in una rete di gestori code, è necessario tenere le seguenti tabelle:

- I nomi delle code di origine e dei gestori code di origine rispetto ai nomi delle code risolti, ai nomi dei gestori code risolti e ai nomi delle code di trasmissione risolti, con il metodo di risoluzione
- I nomi delle code di origine rispetto a:
  - Nomi delle code di destinazione risolte
  - Nomi dei gestori code di destinazione risolti
  - Code di trasmissione
  - Nomi dei canali di messaggi
  - Nomi di sistema adiacenti
  - Nomi coda di risposta

Nota: L'utilizzo del termine *origine* in questo contesto fa riferimento al nome della coda o al nome del gestore code fornito dall'applicazione o a un programma del canale durante l'apertura di una coda per l'inserimento di messaggi.

Un esempio di ciascuna di queste tabelle viene mostrato in Tabella 5 a pagina 46, Tabella 6 a pagina 47e Tabella 7 a pagina 47.

I nomi in queste tabelle sono derivati dagli esempi in questa sezione e questa tabella non è intesa come un esempio pratico di risoluzione dei nomi di coda in un nodo.

Tabella 5. Risoluzione nome coda nel gestore code QMA

Coda di origine specificata quando la coda è aperta	Gestore code di origine specificato quando la coda è aperta	Nome coda risolto	Nome del gestore code risolto	Nome coda di trasmissione risolta	Tipo di risoluzione
QA_norm	-	QA_norm	QMB	QMB	Coda remota
(qualsiasi)	QMB	-	-	QMB	(nessuno)
QA_norm	-	QA_norm	QMB	TX1	Coda remota
QB	MMC	QB	MMD	QMB	Alias gestore code

Tabella 6. Risoluzione del nome coda nel gestore code QMB

Coda di origine specificata quando la coda è aperta	Gestore code di origine specificato quando la coda è aperta	Nome coda risolto	Nome del gestore code risolto	Nome coda di trasmissione risolta	Tipo di risoluzione
QA_norm	-	QA_norm	QMB	-	(nessuno)
QA_norm	QMB	QA_norm	QMB	-	(nessuno)
QA_norm	PRIORITÀ_QM	QA_norm	QMB	-	Alias gestore code
(qualsiasi)	MMC	(qualsiasi)	MMC	MMC	(nessuno)
(qualsiasi)	QMD_norma	(qualsiasi)	QMD_norma	TX1	Alias gestore code
(qualsiasi)	QMD_PRIORITY	(qualsiasi)	QMD_PRIORITY	QMD_veloce	Alias gestore code
(qualsiasi)	QMC_piccolo	(qualsiasi)	QMC_piccolo	TX_piccolo	Alias gestore code
(qualsiasi)	QMC_grande	(qualsiasi)	QMC_grande	TX_esterno	Alias gestore code
QB_piccolo	MMC	QB_piccolo	MMC	TX_piccolo	Coda remota
QB_grande	MMC	QB_grande	MMC	TX_grande	Coda remota
(qualsiasi)	DME	(qualsiasi)	DME	TX1	Alias gestore code
QA	MMC	QA	MMC	TX1	Coda remota
QB	MMD	QB	MMD	TX1	Coda remota

Tabella 7. Conversione del nome della coda di risposta nel gestore code QMA

Progettazione dell'applicazione		Definizione alias di risposta	
QMGR locale	**Nome coda per i messaggi**	**Nome alias coda di risposta**	**Ridefinito in**
QMA	RQ	Q.	QRR a QMA_class1

Numerazione sequenza messaggi canale

Il canale utilizza i numeri di sequenza per assicurare che i messaggi vengano consegnati, consegnati senza duplicazione e memorizzati nello stesso ordine in cui sono stati presi dalla coda di trasmissione.

Il numero di sequenza viene creato all'estremità di invio del canale e viene incrementato di uno prima di essere utilizzato, il che significa che il numero di sequenza corrente è il numero dell'ultimo messaggio inviato. Queste informazioni possono essere visualizzate utilizzando DISPLAY CHSTATUS (vedere Guida di riferimento a MQSC). Il numero di sequenza e un identificativo denominato LUWID vengono memorizzati nella memoria persistente per l'ultimo messaggio trasferito in batch. Questi valori vengono utilizzati durante l'avvio del canale per garantire che entrambe le estremità del collegamento concordino su quali messaggi sono stati trasferiti correttamente.

Richiamo sequenziale dei messaggi

Se un'applicazione inserisce una sequenza di messaggi nella stessa coda di destinazione, tali messaggi possono essere richiamati in sequenza da un'applicazione ***singola*** con una sequenza di operazioni MQGET, se sono soddisfatte le seguenti condizioni:

- Tutte le richieste di inserimento sono state effettuate dalla stessa applicazione.

- Tutte le richieste di inserimento provenivano dalla stessa unità di lavoro oppure tutte le richieste di inserimento sono state effettuate al di fuori di un'unità di lavoro.
- Tutti i messaggi hanno la stessa priorità.
- I messaggi hanno tutti la stessa persistenza.
- Per l'accodamento remoto, la configurazione è tale che può esistere solo un percorso dall'applicazione che effettua la richiesta di inserimento, attraverso il gestore code, attraverso l'intercomunicazione, al gestore code di destinazione e alla coda di destinazione.
- I messaggi non vengono inseriti in una coda di messaggi non instradabili (ad esempio, se una coda è temporaneamente piena).
- L'applicazione che riceve il messaggio non modifica deliberatamente l'ordine di richiamo, ad esempio specificando un particolare *MsgId* o *CorrelId* o utilizzando le priorità del messaggio.
- Solo un'applicazione sta eseguendo operazioni get per richiamare i messaggi dalla coda di destinazione. Se è presente più di un'applicazione, queste applicazioni devono essere progettate per ottenere tutti i messaggi in ogni sequenza inseriti da un'applicazione di invio.

Nota: I messaggi provenienti da altre attività e unità di lavoro potrebbero essere intervallati dalla sequenza, anche quando la sequenza è stata inserita all'interno di una singola unità di lavoro.

Se queste condizioni non possono essere soddisfatte e l'ordine dei messaggi sulla coda di destinazione è importante, l'applicazione può essere codificata per utilizzare il proprio numero di sequenza dei messaggi come parte del messaggio per assicurare l'ordine dei messaggi.

Sequenza di richiamo dei messaggi veloci e non persistenti

I messaggi non persistenti su un canale veloce potrebbero superare i messaggi persistenti sullo stesso canale e quindi arrivare fuori sequenza. L'MCA ricevente inserisce immediatamente i messaggi non persistenti nella coda di destinazione e li rende visibili. I messaggi persistenti non saranno visibili fino al punto di sincronizzazione successivo.

Test di loopback

Il *test di loopback* è una tecnica su piattaforme non z/OS che consente di verificare un link di comunicazione senza collegarlo effettivamente a un'altra macchina.

Si imposta una connessione tra due gestori code come se fossero su macchine separate, ma si verifica la connessione eseguendo un loop su un altro processo sulla stessa macchina. Questa tecnica significa che è possibile verificare il codice di comunicazione senza richiedere una rete attiva.

Il modo in cui si fa ciò dipende da quali prodotti e protocolli si stanno utilizzando.

Su sistemi Windows , è possibile utilizzare l'adattatore "loopback".

Per ulteriori informazioni, fare riferimento alla documentazione dei prodotti in uso.

Traccia del percorso e registrazione dell'attività

È possibile confermare l'instradamento di un messaggio attraverso una serie di gestori code in due modi.

È possibile utilizzare l'applicazione di instradamento di visualizzazione di WebSphere MQ , disponibile tramite il comando di controllo `dspmqrte`, oppure è possibile utilizzare la registrazione attività. Entrambi questi argomenti sono descritti in Riferimento del monitoraggio.

Introduzione alla gestione delle code distribuite

DQM (Distributed Queue Management) viene utilizzato per definire e controllare le comunicazioni tra gestori code.

Gestione code distribuite:

- Consente di definire e controllare i canali di comunicazione tra i gestori code

- Fornisce un servizio del canale dei messaggi per spostare i messaggi da un tipo di *coda locale*, nota come coda di trasmissione, a link di comunicazioni su un sistema locale e da link di comunicazioni a code locali su un gestore code di destinazione
- Fornisce funzioni per monitorare il funzionamento dei canali e diagnosticare i problemi, utilizzando pannelli, comandi e programmi

Le definizioni dei canali associano i nomi dei canali alle code di trasmissione, agli identificatori dei collegamenti di comunicazione e agli attributi dei canali. Le definizioni di canale sono implementate in modi diversi su piattaforme diverse. L'invio e la ricezione di messaggi è controllata da programmi noti come *agent MCA (message channel agent)* , che utilizzano le definizioni di canale per avviare e controllare le comunicazioni.

Gli MCA a loro volta sono controllati dallo stesso DQM. La struttura è dipendente dalla piattaforma, ma in genere include listener e controlli trigger, insieme a comandi e pannelli dell'operatore.

Un *canale di messaggi* è un pipe unidirezionale per spostare i messaggi da un gestore code a un altro. Quindi un canale di messaggi ha due endpoint, rappresentati da una coppia di MCA. Ogni endpoint ha una definizione della sua fine del canale di messaggi. Ad esempio, un'estremità definirebbe un mittente, l'altra un destinatario.

Per i dettagli su come definire i canali, consultare:

- 

“Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 74

Per esempi di pianificazione del canale di messaggi, consultare:

- 

Esempio di pianificazione del canale di messaggi per piattaforme distribuite

Per informazioni sulle uscite canale, vedere Programmi di uscita canale per canali di messaggistica.

Concetti correlati

“Invio e ricezione di messaggi” a pagina 50
La seguente figura mostra il modello di gestione della coda distribuita, dettagliando le relazioni tra entità quando vengono trasmessi i messaggi. Mostra anche il flusso per il controllo.

“Funzione di controllo canale” a pagina 54
La funzione di controllo del canale consente di definire, monitorare e controllare i canali.

“Cosa succede quando un messaggio non può essere consegnato?” a pagina 67
Quando un messaggio non può essere consegnato, l'MCA può elaborarlo in diversi modi. Può riprovare, può tornare al mittente o può inserirlo nella coda di messaggi non recapitabili.

“File di inizializzazione e di configurazione” a pagina 71
La gestione dei dati di inizializzazione del canale dipende dalla piattaforma WebSphere MQ .

“Conversione dati per i messaggi” a pagina 72
I messaggi WebSphere MQ potrebbero richiedere la conversione dei dati quando vengono inviati tra le code su gestori code differenti.

“Scrittura dei propri agent del canale dei messaggi” a pagina 72
WebSphere MQ consente di scrivere i propri programmi MCA (message channel agent) o di installarne uno da un fornitore di software indipendente.

“Altre cose da considerare per la gestione della coda distribuita” a pagina 73
Altri argomenti da considerare quando si prepara WebSphere MQ per la gestione delle code distribuite. Questo argomento riguarda la coda di messaggi non recapitati, le code in uso, le estensioni di sistema e i programmi di uscita utente e i canali e listener in esecuzione come applicazioni attendibili.

Riferimenti correlati

Informazioni di configurazione di esempio

Invio e ricezione di messaggi

La seguente figura mostra il modello di gestione della coda distribuita, dettagliando le relazioni tra entità quando vengono trasmessi i messaggi. Mostra anche il flusso per il controllo.

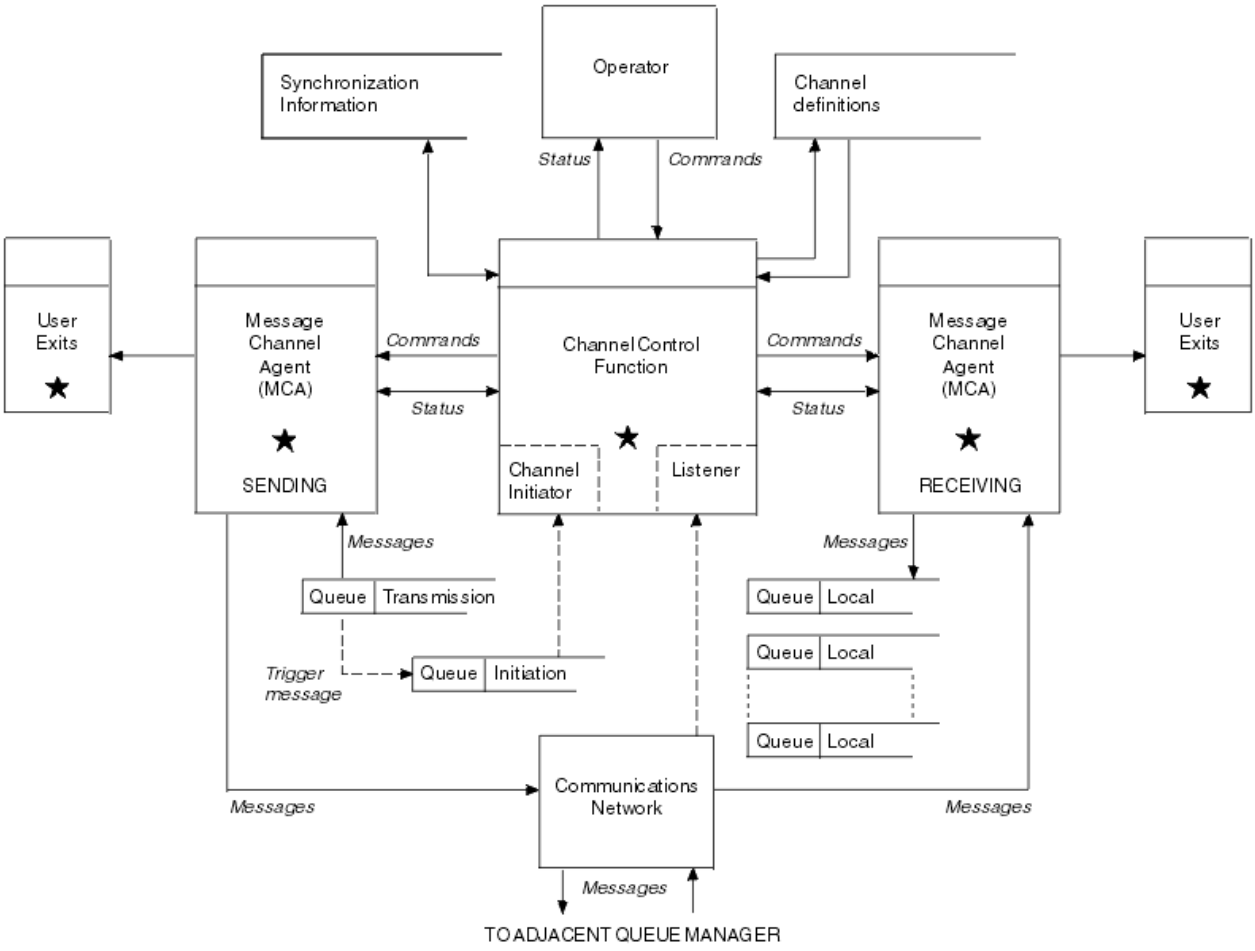


Figura 11. Modello di gestione code distribuite

Nota:

1. Esiste un MCA per canale, a seconda della piattaforma. Potrebbero essere presenti una o più funzioni di controllo del canale per un particolare gestore code.
2. L'implementazione degli MCA e delle funzioni di controllo del canale è altamente dipendente dalla piattaforma. Possono essere programmi o processi o thread, e possono essere una singola entità o molte che comprendono diverse parti indipendenti o collegate.
3. Tutti i componenti contrassegnati con un asterisco possono utilizzare MQI.

Parametri canale

Un MCA riceve i suoi parametri in uno dei seguenti modi:

- Se avviato da un comando, il nome del canale viene passato in un'area dati. L'MCA legge quindi la definizione del canale direttamente per ottenere i suoi attributi.
- Per i canali mittente e in alcuni casi server, l'MCA può essere avviato automaticamente dal trigger del gestore code. Il nome del canale viene richiamato dalla definizione del processo trigger, dove applicabile, e viene passato all'MCA. La restante elaborazione è la stessa descritta in precedenza. I canali server devono essere impostati per essere attivati solo se sono completi, ovvero, specificano un CONNAME a cui connettersi.

- Se avviato in remoto da un mittente, un server, un richiedente o una connessione client, il nome del canale viene trasmesso nei dati iniziali dall'agent del canale dei messaggi partner. MCA legge la definizione di canale direttamente per ottenere i suoi attributi.

Alcuni attributi non definiti nella definizione del canale sono anch'essi negoziabili:

Suddividi messaggi
Se un'estremità non supporta i messaggi suddivisi, i messaggi suddivisi non vengono inviati.

Capacità di conversione
Se un'estremità non può eseguire la conversione della codepage o la conversione della codifica numerica necessarie, l'altra estremità deve gestirla. Se nessuna delle due estremità lo supporta, quando necessario, il canale non può essere avviato.

Supporto elenco di distribuzione
Se un'estremità non supporta gli elenchi di distribuzione, l'MCA partner imposta un indicatore nella propria coda di trasmissione in modo che sappia intercettare i messaggi destinati a più destinazioni.

Stato del canale e numeri di sequenza

I programmi dell'agent del canale dei messaggi conservano i record del numero di sequenza corrente e del numero dell'unità di lavoro logica per ciascun canale e dello stato generale del canale. Alcune piattaforme consentono di visualizzare queste informazioni di stato per facilitare il controllo dei canali.

Come inviare un messaggio a un altro gestore code

In questa sezione viene descritto il modo più semplice per inviare un messaggio tra i gestori code, inclusi i prerequisiti e le autorizzazioni richieste. Altri metodi possono essere utilizzati anche per l'invio di messaggi a un gestore code remoto.

Prima di inviare un messaggio da un gestore code a un altro, è necessario effettuare le seguenti operazioni:

1. Verificare che il protocollo di comunicazione scelto sia disponibile.
2. Avviare i gestori code.
3. Avviare gli iniziatori di canali.
4. Avviare i listener.

È inoltre necessario disporre dell'autorizzazione di sicurezza WebSphere MQ corretta per creare gli oggetti richiesti.

Per inviare messaggi da un gestore code a un altro:

- Definire i seguenti oggetti sul gestore code di origine:
  - Canale di trasmissione
  - Definizione di coda remota
  - Coda di iniziazione (facoltativo)
  - Coda di trasmissione
  - Coda di messaggi non recapitabili
- Definire i seguenti oggetti sul gestore code di destinazione:
  - Canale di ricezione
  - Coda di destinazione
  - Coda di messaggi non recapitabili

È possibile utilizzare diversi metodi per definire questi oggetti, a seconda della piattaforma WebSphere MQ :

- Su tutte le piattaforme, è possibile utilizzare i comandi WebSphere MQ script commands (MQSC) descritti in I comandi MQSC i comandi PCF (programmable command format) descritti in Automating administration tasks o WebSphere MQ Explorer.

Per ulteriori informazioni sulla creazione dei componenti per l'invio di messaggi a un altro gestore code, consultare i seguenti argomenti secondari:

Concetti correlati

"Creazione e gestione di gestori code" a pagina 20
Prima di poter utilizzare messaggi e code, è necessario creare e avviare almeno un gestore code e i relativi oggetti associati.

"Tecniche di messaggistica distribuita IBM WebSphere MQ" a pagina 29
Gli argomenti secondari in questa sezione descrivono le tecniche che sono di uso durante la pianificazione dei canali. Questi argomenti secondari descrivono le tecniche per pianificare come collegare i gestori code e gestire il flusso di messaggi tra le applicazioni.

"Introduzione alla gestione delle code distribuite" a pagina 48
DQM (Distributed Queue Management) viene utilizzato per definire e controllare le comunicazioni tra gestori code.

"Attivazione dei canali" a pagina 68
WebSphere MQ fornisce una funzione per avviare automaticamente un'applicazione quando vengono soddisfatte determinate condizioni su una coda. Questa funzione viene chiamata attivazione.

"Sicurezza dei messaggi" a pagina 66
Oltre alle tipiche funzioni di ripristino di WebSphere MQ, la gestione delle code distribuite garantisce che i messaggi vengano consegnati correttamente utilizzando una procedura del punto di sincronizzazione coordinata tra le due estremità del canale dei messaggi. Se questa procedura rileva un errore, chiude il canale in modo da poter esaminare il problema e mantiene i messaggi in modo sicuro nella coda di trasmissione fino a quando il canale non viene riavviato.

"Monitoraggio e controllo dei canali su UNIX, Linux, and Windows" a pagina 74
Per DQM è necessario creare, monitorare e controllare i canali per i gestori code remoti. È possibile controllare i canali utilizzando comandi, programmi, IBM WebSphere MQ Explorer, file per le definizioni dei canali e un'area di memoria per le informazioni di sincronizzazione.

"Configurazione delle connessioni tra client e server" a pagina 100
Per configurare i collegamenti di comunicazione tra WebSphere MQ i client e i server MQI, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del collegamento, avviare un listener e definire canali.

Attività correlate

"Configurazione di un cluster di gestore code" a pagina 161
Utilizzare i link in questo argomento per scoprire come funzionano i cluster, come progettare una configurazione cluster e per ottenere un esempio di come impostare un cluster semplice.

Definizione dei canali

Per inviare i messaggi da un gestore code a un altro, è necessario definire due canali. È necessario definirne uno sul gestore code di origine e uno sul gestore code di destinazione.

Sul gestore code di origine

Definire un canale con un tipo di canale SENDER. È necessario specificare quanto segue:

- Il nome della coda di trasmissione da utilizzare (attributo XMITQ).
- Il nome della connessione del sistema partner (l'attributo CONNAME).
- Il nome del protocollo di comunicazione che si sta utilizzando (attributo TRPTYPE). Su WebSphere MQ per z/OS, il protocollo deve essere TCP o LU6.2. Su altre piattaforme, non è necessario specificarlo. È possibile lasciarlo per selezionare il valore dalla propria definizione di canale predefinita.

I dettagli di tutti gli attributi del canale sono forniti in Attributi canale .

Sul gestore code di destinazione

Definire un canale con un tipo di canale RECEIVER e lo stesso nome del canale mittente.

Specificare il nome del protocollo di comunicazioni che si sta utilizzando (attributo TRPTYPE). Su WebSphere MQ per z/OS, il protocollo deve essere TCP o LU6.2. Su altre piattaforme, non è necessario specificarlo. È possibile lasciarlo per selezionare il valore dalla propria definizione di canale predefinita.

Le definizioni del canale ricevente possono essere generiche. Ciò significa che se si dispone di diversi gestori code che comunicano con lo stesso destinatario, i canali di invio possono tutti specificare lo stesso nome per il destinatario e una definizione di destinatario si applica a tutti.

Nota: Il valore del parametro TRPTYPE viene ignorato dall'agent del canale dei messaggi che risponde. Ad esempio, un TRPTYPE di TCP sulla definizione del canale mittente inizia correttamente con un TRPTYPE LU62 sulla definizione del canale ricevente come partner.

Una volta definito il canale, è possibile verificarlo utilizzando il comando PING CHANNEL. Questo comando invia un messaggio speciale dal canale mittente al canale ricevente e verifica che venga restituito.

Definizione delle code

Per inviare messaggi da un gestore code a un altro, è necessario definire fino a sei code. È necessario definire fino a quattro code sul gestore code di origine e fino a due code sul gestore code di destinazione.

Sul gestore code di origine

- Definizione di coda remota

  In questa definizione, specificare quanto segue:

  Nome gestore code remoto
  Il nome del gestore code di destinazione.

  Nome coda remota
  Il nome della coda di destinazione sul gestore code di destinazione.

  Nome coda di trasmissione
  Il nome della coda di trasmissione. Non è necessario specificare questo nome della coda di trasmissione. In caso contrario, viene utilizzata una coda di trasmissione con lo stesso nome del gestore code di destinazione. Se non esiste, viene utilizzata la coda di trasmissione predefinita. Si consiglia di fornire alla coda di trasmissione lo stesso nome del gestore code di destinazione in modo che la coda venga trovata per impostazione predefinita.

- Definizione della coda di avvio

  Richiesto su z/OSe facoltativo su altre piattaforme. Prendere in considerazione la denominazione della coda di iniziazione SYSTEM.CHANNEL.INITQ. su altre piattaforme.

- Definizione della coda di trasmissione

  Una coda locale con l'attributo USAGE impostato su XMITQ.

- Definizione coda di messaggi non instradabili

  Definire una coda di messaggi non recapitabili in cui scrivere i messaggi non recapitati.

Sul gestore code di destinazione

- Definizione coda locale

  La coda di destinazione. Il nome di questa coda deve essere uguale a quello specificato nel campo del nome della coda remota della definizione della coda remota sul gestore code di origine.

- Definizione coda di messaggi non instradabili

  Definire una coda di messaggi non recapitabili in cui scrivere i messaggi non recapitati.

Concetti correlati

“Creazione di una coda di trasmissione” a pagina 54

Prima che un canale (diverso da un canale richiedente) possa essere avviato, la coda di trasmissione deve essere definita come descritto in questa sezione. La coda di trasmissione deve essere denominata nella definizione di canale.

Creazione di una coda di trasmissione
Prima che un canale (diverso da un canale richiedente) possa essere avviato, la coda di trasmissione deve essere definita come descritto in questa sezione. La coda di trasmissione deve essere denominata nella definizione di canale.

Definire una coda locale con l'attributo USAGE impostato su XMITQ per ogni canale di invio messaggi. Se si desidera utilizzare una coda di trasmissione specifica nelle definizioni della coda remota, creare una coda remota come mostrato.

Per creare una coda di trasmissione, utilizzare WebSphere MQ Commands (MQSC), come mostrato nei seguenti esempi:

Crea esempio di coda di trasmissione

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

Crea esempio di coda remota

```
DEFINE QREMOTE(PAYROLL) DESCR('Remote queue for QM2') +
XMITQ(QM2) RNAME(PAYROLL) RQMNAME(QM2)
```

Considerare la possibilità di denominare la coda di trasmissione come nome del gestore code sul sistema remoto, come mostrato negli esempi.

Avvio del canale
Quando si inseriscono i messaggi nella coda remota definita nel gestore code di origine, questi vengono memorizzati nella coda di trasmissione fino a quando il canale non viene avviato. Una volta avviato il canale, i messaggi vengono consegnati alla coda di destinazione sul gestore code remoto.

Avviare il canale sul gestore code di invio utilizzando il comando START CHANNEL. Quando si avvia il canale di invio, il canale di ricezione viene avviato automaticamente (dal listener) e i messaggi vengono inviati alla coda di destinazione. Entrambe le estremità del canale dei messaggi devono essere in esecuzione per poter trasferire i messaggi.

Poiché le due estremità del canale si trovano su gestori code differenti, è possibile che siano state definite con attributi differenti. Per risolvere eventuali differenze, esiste una negoziazione di dati iniziale tra le due estremità quando il canale viene avviato. In generale, le due estremità del canale operano con gli attributi che richiedono meno risorse. Ciò consente ai sistemi più grandi di contenere le risorse minori dei sistemi più piccoli all'altra estremità del canale dei messaggi.

L'MCA mittente suddivide i messaggi di grandi dimensioni prima di inviarli attraverso il canale. Vengono riassemblati sul gestore code remoto. Ciò non è evidente per l'utente.

Un MCA può trasferire messaggi utilizzando più thread. Questo processo, denominato *pipelining* , consente all'MCA di trasferire i messaggi in modo più efficiente, con meno stati di attesa. Pipelining migliora le prestazioni del canale.

Funzione di controllo canale

La funzione di controllo del canale consente di definire, monitorare e controllare i canali.

I comandi vengono emessi tramite pannelli, programmi o da una riga comandi alla funzione di controllo del canale. L'interfaccia del pannello visualizza anche lo stato del canale e i dati di definizione del canale. È possibile utilizzare i formati dei comandi programmabili o i comandi WebSphere MQ (MQSC) e i comandi di controllo descritti in “Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 74.

I comandi rientrano nei seguenti gruppi:

- Amministrazione canale
- Controllo canale

- Monitoraggio stato canale

I comandi di gestione dei canali gestiscono le definizioni dei canali. Essi consentono di:

- Crea una definizione di canale
- Copia una definizione di canale
- Modifica di una definizione di canale
- Elimina una definizione di canale

I comandi di controllo del canale gestiscono il funzionamento dei canali. Essi consentono di:

- Avvia un canale
- Arresta un canale
- Risincronizza con il partner (in alcune implementazioni)
- Reimpostare i numeri di sequenza dei messaggi
- Risoluzione di un batch di messaggi in dubbio
- Ping; invia una comunicazione di verifica attraverso il canale

Il monitoraggio dei canali visualizza lo stato dei canali, ad esempio:

- Impostazioni canale correnti
- Se il canale è attivo o inattivo
- Se il canale è terminato in uno stato sincronizzato

Per ulteriori informazioni sulla definizione, il controllo e il monitoraggio dei canali, consultare i topic secondari riportati di seguito:

Preparazione dei canali

Prima di tentare di avviare un canale messaggi o un canale MQI, è necessario preparare il canale. È necessario verificare che tutti gli attributi delle definizioni di canale locale e remoto sia corretti e compatibili.

Attributi canale descrive le definizioni e gli attributi del canale.

Anche se si impostano le definizioni di canale esplicite, le negoziazioni del canale eseguite all'avvio di un canale potrebbero sovrascrivere uno o l'altro dei valori definiti. Questo comportamento è normale, e non apparente per l'utente, ed è stato organizzato in questo modo in modo che le definizioni altrimenti incompatibili possano funzionare insieme.

Definizione automatica dei canali riceventi e di connessione server

In WebSphere MQ su tutte le piattaforme, ad eccezione di z/OS, se non esiste una definizione di canale appropriata, per un canale ricevente o di connessione server che ha la definizione automatica abilitata, viene creata automaticamente una definizione. La definizione viene creata utilizzando:

1. La definizione di canale modello appropriata, SYSTEM.AUTO.RECEIVERo SYSTEM.AUTO.SVRCONN. Le definizioni del canale modello per la definizione automatica sono le stesse dei valori predefiniti del sistema, SYSTEM.DEF.RECEIVERe SYSTEM.DEF.SVRCONN, ad eccezione del campo della descrizione, che è "Auto - definito da" seguito da 49 spazi. L'amministratore di sistema può scegliere di modificare qualsiasi parte delle definizioni di canale modello fornite.
2. Informazioni dal sistema partner. I valori del partner vengono utilizzati per il nome del canale e per il valore di wrap del numero di sequenza.
3. Un programma di uscita canale, che è possibile utilizzare per modificare i valori creati dalla definizione automatica. Vedere Programma di uscita di definizione automatica del canale.

La descrizione viene quindi controllata per determinare se è stata modificata da un'uscita di definizione automatica o perché la definizione del modello è stata modificata. Se i primi 44 caratteri sono ancora "Definito automaticamente da" seguito da 29 spazi vuoti, il nome gestore code viene aggiunto. Se gli ultimi 20 caratteri sono ancora tutti vuoti, vengono aggiunti l'ora e la data locali.

Quando la definizione è stata creata e memorizzata, l'avvio del canale procede come se la definizione fosse sempre esistita. La dimensione batch, la dimensione di trasmissione e la dimensione del messaggio vengono negoziate con il partner.

Definizione di altri oggetti

Prima di poter avviare un canale di messaggi, entrambe le estremità devono essere definite (o abilitate per la definizione automatica) sui relativi gestori code. La coda di trasmissione che deve servire deve essere definita per il gestore code all'estremità di invio. Il collegamento di comunicazione deve essere definito e disponibile. Potrebbe essere necessario preparare altri oggetti WebSphere MQ , come le definizioni di code remote, le definizioni di alias del gestore code e le definizioni di alias della coda reply - to, per implementare gli scenari descritti in “Connessione di applicazioni mediante l'accodamento distribuito” a pagina 28.

Per informazioni sulla definizione dei canali MQI, consultare “Definizione di canali MQI” a pagina 113.

Più canali di messaggi per coda di trasmissione

È possibile definire più di un canale per coda di trasmissione, ma solo uno di questi canali può essere attivo alla volta. Considerare questa opzione per il provisioning di instradamenti alternativi tra gestori code per il bilanciamento del traffico e collegare l'azione correttiva di errore. Una coda di trasmissione non può essere utilizzata da un altro canale se il canale precedente per utilizzarla è terminato lasciando un batch di messaggi in dubbio all'estremità di invio. Per ulteriori informazioni, vedere “Canali in dubbio” a pagina 65.

Avvio di un canale

È possibile che un canale inizi a trasmettere i messaggi in uno dei quattro modi. Può essere:

- Avviato da un operatore (non da canali ricevente, ricevente del cluster o di connessione server).
- Attivato dalla coda di trasmissione. Questo metodo si applica solo ai canali mittente e ai canali server completi (quei canali che specificano un CONNAME). È necessario preparare gli oggetti necessari per attivare i canali.
- Avviato da un programma applicativo (non canali ricevente, ricevente cluster o di connessione server).
- Avviato in remoto dalla rete da un canale mittente, mittente cluster, richiedente, server o connessione client. I canali riceventi, riceventi del cluster e, possibilmente, i canali server e richiedenti vengono avviati in questo modo, così come i canali di connessione server. I canali stessi devono essere già avviati (cioè abilitati).

Nota: Poiché un canale è 'avviato ', non trasmette necessariamente i messaggi. Invece, potrebbe essere 'abilitato' per avviare la trasmissione quando si verifica uno dei quattro eventi precedentemente descritti. L'abilitazione e la disabilitazione di un canale si ottiene utilizzando i comandi operatore START e STOP.

Stati del canale

Un canale può essere in uno dei tanti stati in qualsiasi momento. Alcuni stati hanno anche sottostati. Da un determinato stato un canale può spostarsi in altri stati.

La Figura 12 a pagina 57 mostra la gerarchia di tutti i possibili stati del canale e gli stati secondari che si applicano a ciascuno degli stati del canale.

Figura 13 a pagina 58 mostra i link tra gli stati del canale. Questi collegamenti si applicano a tutti i tipi di canali di messaggi e di canali di connessione server.

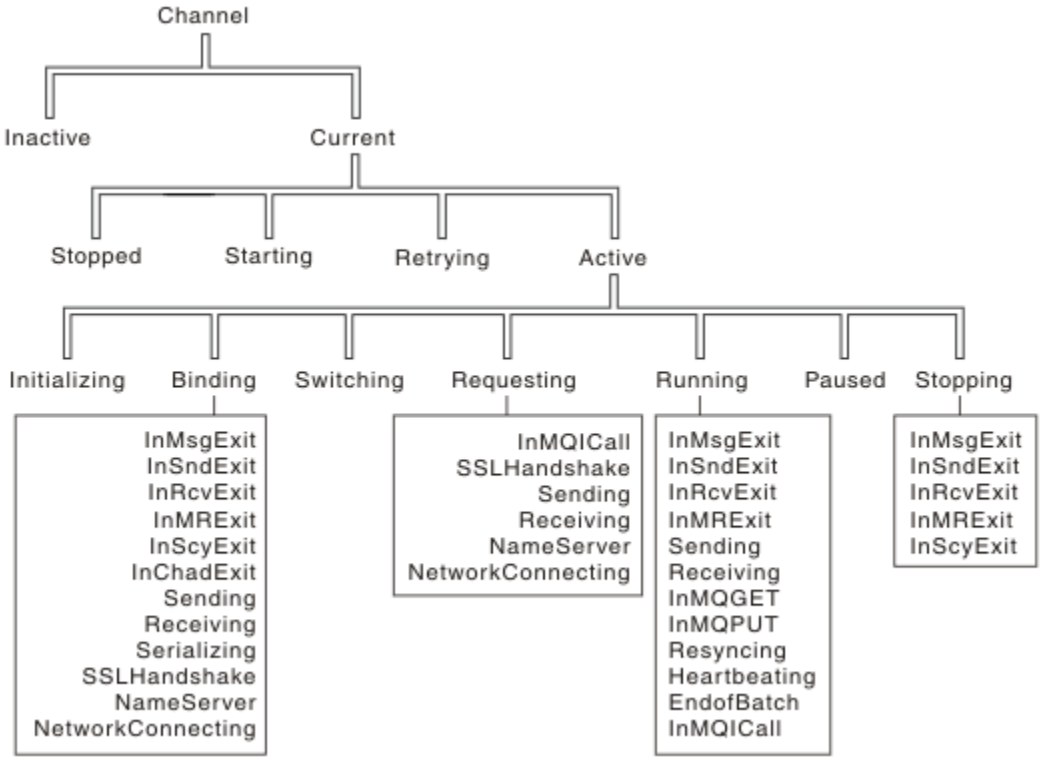


Figura 12. Stati e sottostati del canale

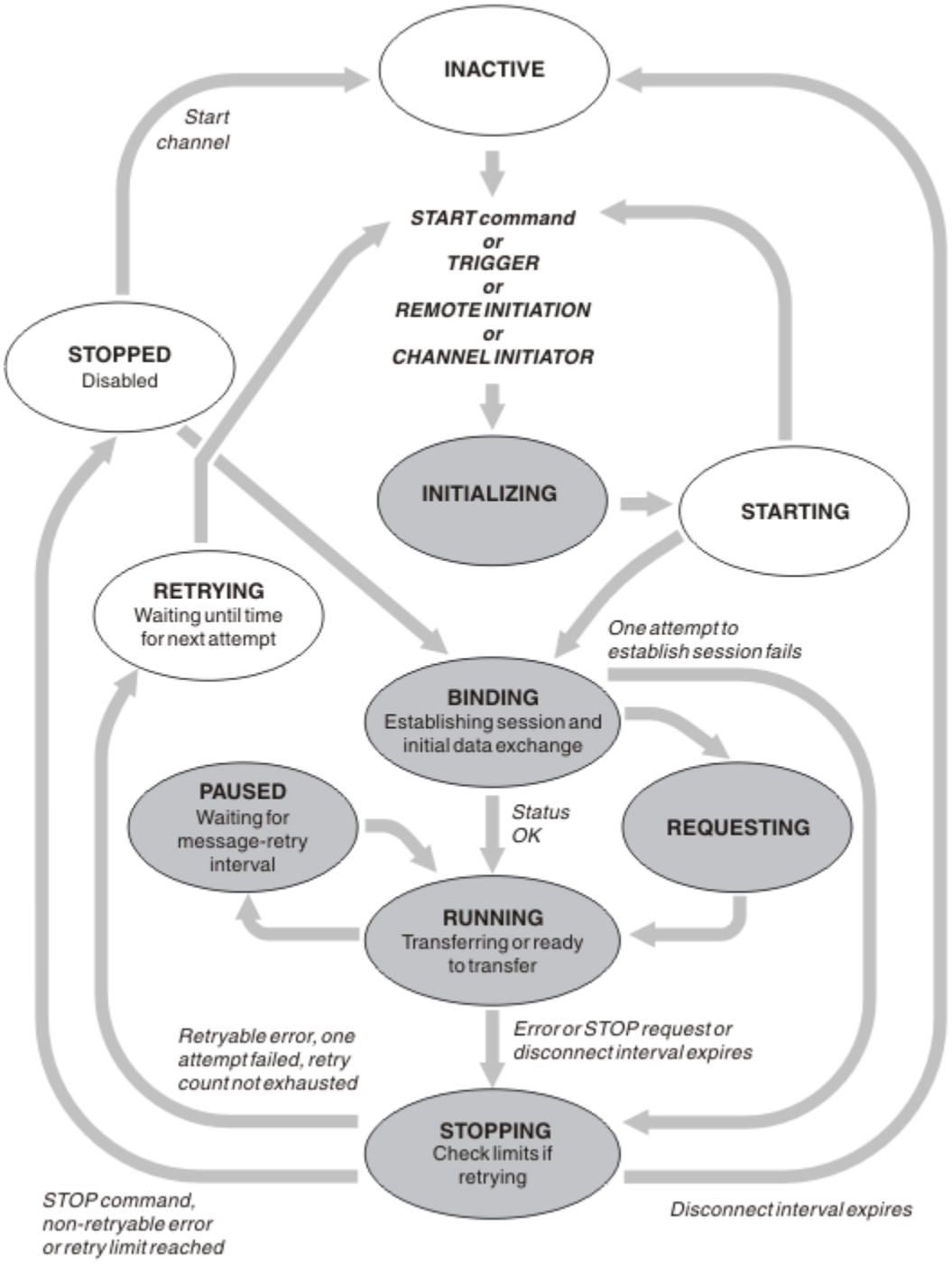


Figura 13. Flussi tra stati del canale

Corrente e attivo

Un canale è *corrente* se si trova in uno stato diverso da inattivo. Un canale corrente è *attivo* a meno che non si trovi nello stato NUOVO TENTATIVO, ARRESTATO o IN fase di avvio. Quando un canale è attivo, sta consumando una risorsa e un processo o un thread è in esecuzione. I sette possibili stati di un canale attivo (INITIALIZING, BINDING, SWITCHING, RICHIEDENTE, RUNNING, PAUSED o STOPPING) sono evidenziati in Figura 13 a pagina 58.

Un canale attivo può anche visualizzare uno stato secondario che fornisce maggiori dettagli su cosa sta facendo esattamente il canale. I sottostati per ciascuno stato sono mostrati in Figura 12 a pagina 57.

Corrente e attivo
Il canale è "corrente" se si trova in uno stato diverso da inattivo. Un canale corrente è "attivo" a meno che non si trovi nello stato NUOVO TENTATIVO, ARRESTATO o IN fase di avvio.

Se un canale è "attivo" potrebbe anche mostrare un sottostato che fornisce maggiori dettagli su cosa sta facendo esattamente il canale.

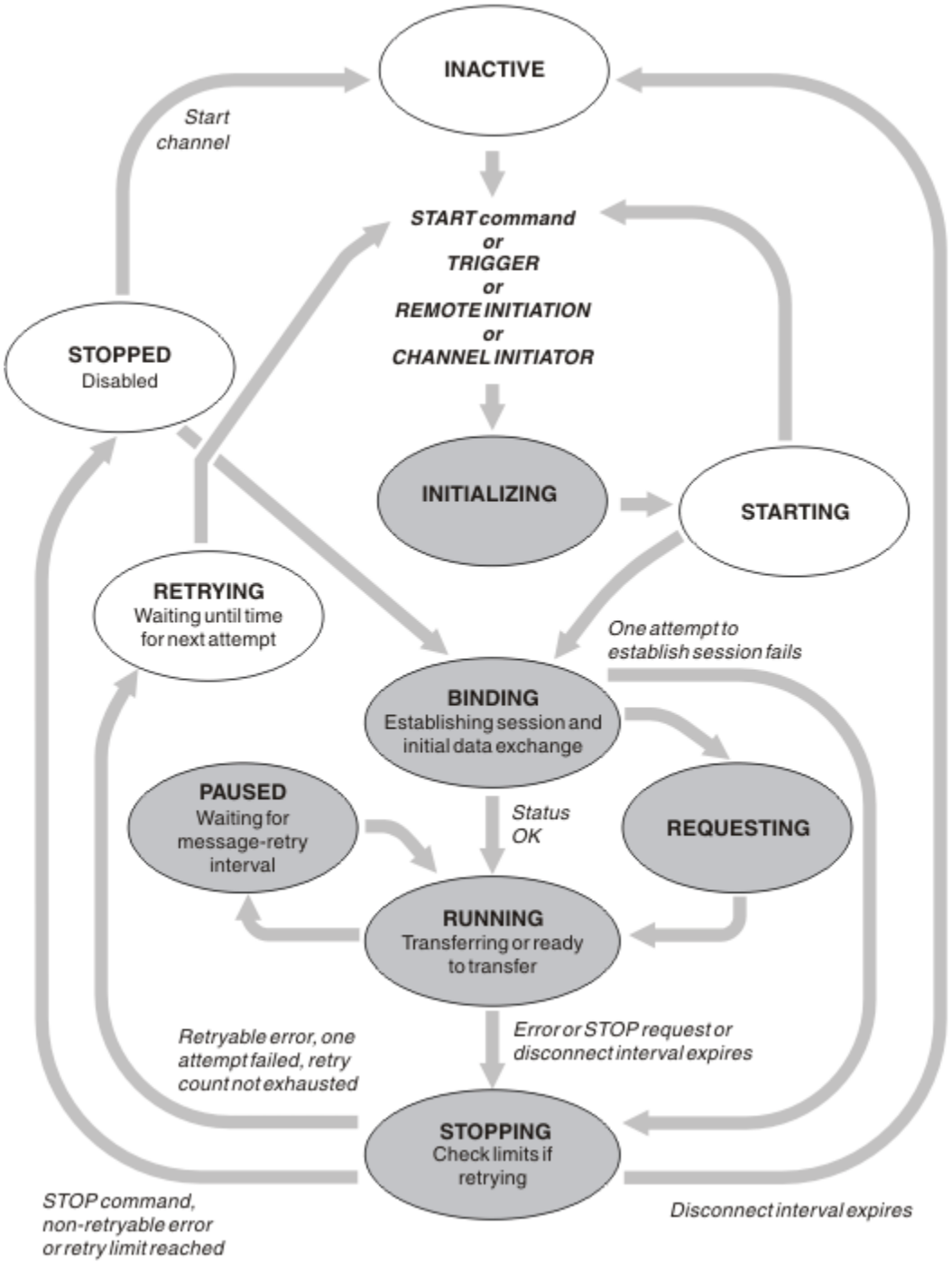


Figura 14. Flussi tra stati del canale

Nota:

1. Quando un canale si trova in uno dei sei stati evidenziati in Figura 14 a pagina 59 (INITIALIZING, BINDING, RICHIEDENTE, IN ESECUZIONE, PAUSED o STOPPING), sta consumando una risorsa e un processo o un thread è in esecuzione; il canale è *attivo*.

2. Quando un canale si trova nello stato ARRESTATO, la sessione potrebbe essere attiva perché lo stato successivo non è ancora noto.

Specifica del numero massimo di canali correnti

È possibile specificare il numero massimo di canali che possono essere correnti contemporaneamente. Questo numero è il numero di canali che hanno voci nella tabella di stato del canale, inclusi i canali che stanno ritentando e i canali che sono arrestati. Specificare questa opzione utilizzando il file di configurazione del gestore code per sistemi UNIX and Linux o WebSphere MQ Explorer. Per ulteriori informazioni sui valori impostati utilizzando il file di inizializzazione o di configurazione, consultare Stanza del file di configurazione per l'accodamento distribuito. Per ulteriori informazioni sulla specifica del numero massimo di canali, consultare Amministrazione IBM WebSphere MQ per WebSphere MQ per sistemi UNIX and Linux e Sistemi Windows.

Nota:

1. I canali di connessione server sono inclusi in questo numero.
2. Un canale deve essere corrente prima di diventare attivo. Se un canale viene avviato, ma non può diventare corrente, l'avvio ha esito negativo.

Specifica del numero massimo di canali attivi

È anche possibile specificare il numero massimo di canali attivi per evitare che il sistema venga sovraccaricato da molti canali di avvio. Se si utilizza questo metodo, impostare l'attributo dell'intervallo di disconnessione su un valore basso per consentire l'avvio dei canali in attesa non appena terminano gli altri canali.

Ogni volta che un canale che tenta nuovamente di stabilire una connessione con il partner, deve diventare un canale attivo. Se il tentativo non riesce, rimane un canale corrente che non è attivo, fino a quando non è il momento per il successivo tentativo. Il numero di volte in cui un canale tenta nuovamente e la frequenza è determinata dagli attributi del numero di tentativi e dell'intervallo di tentativi. Esistono valori brevi e lunghi per entrambi questi attributi. Per ulteriori informazioni, consultare Attributi del canale .

Quando un canale deve diventare un canale attivo (perché è stato emesso un comando START, perché è stato attivato o perché è il momento di un nuovo tentativo), ma non è in grado di farlo perché il numero di canali attivi è già al valore massimo, il canale attende che uno degli slot attivi venga liberato da un'altra istanza del canale che cessa di essere attivo. Se, tuttavia, un canale viene avviato perché è stato avviato in remoto e non ci sono slot attivi disponibili per tale canale in quel momento, l'avvio remoto viene rifiutato.

Ogni volta che un canale, diverso da un canale richiedente, tenta di diventare attivo, passa allo stato STARTING. Questo stato si verifica anche se c'è uno slot attivo immediatamente disponibile, anche se è solo nello stato STARTING per un breve periodo di tempo. Tuttavia, se il canale deve attendere un alloggiamento attivo, è in stato AVVIO mentre è in attesa.

I canali del richiedente non passano allo stato STARTING. Se un canale richiedente non può essere avviato perché il numero di canali attivi è già al limite, il canale termina in modo anomalo.

Ogni volta che un canale, diverso da un canale richiedente, non è in grado di ottenere uno slot attivo e quindi ne attende uno, viene scritto un messaggio nel log e viene generato un evento. Quando uno slot viene successivamente liberato e il canale è in grado di acquisirlo, vengono generati un altro evento e un altro messaggio. Nessuno di questi eventi e messaggi viene generato se il canale è in grado di acquisire immediatamente uno slot.

Se si immette un comando STOP CHANNEL mentre il canale è in attesa di diventare attivo, il canale passa allo stato STOPPED. Viene generato un evento Arrestato dal canale.

I canali di connessione server sono compresi nel numero massimo di canali attivi.

Per ulteriori informazioni sulla specifica del numero massimo di canali attivi, consultare Amministrazione IBM WebSphere MQ per WebSphere MQ per sistemi UNIX and Linux e Sistemi Windows.

Errori canale
Gli errori sui canali causano l'arresto di ulteriori trasmissioni da parte del canale. Se il canale è un mittente o un server, passa allo stato RETRY perché è possibile che il problema si risolva da solo. Se non è possibile passare allo stato RETRY, il canale passa allo stato STOPPED.

Per i canali di invio, la coda di trasmissione associata è impostato su GET (DISABLED) e l'attivazione è disattivata. (Un comando STOP con STATUS (STOPPED) prende il lato che lo ha emesso nello stato STOPPED; solo la scadenza dell'intervallo di disconnessione o un comando STOP con STATUS (INACTIVE) lo rende terminato normalmente e diventa inattivo.) I canali che si trovano nello stato STOPPED necessitano dell'intervento dell'operatore prima di poter essere riavviati (consultare “Riavvio dei canali arrestati” a pagina 64).

Nota: Per sistemi UNIX, Linux e Windows , è necessario che un iniziatore di canali sia in esecuzione per ritentare. Se l'iniziatore di canali non è disponibile, il canale diventa inattivo e deve essere riavviato manualmente. Se si sta utilizzando uno script per avviare il canale, assicurarsi che l'iniziatore del canale sia in esecuzione prima di provare ad eseguire lo script.

Conteggio tentativi lunghi (LONGRTY) descrive come funziona il nuovo tentativo. Se l'errore viene cancellato, il canale viene riavviato automaticamente e la coda di trasmissione viene riabilitata. Se il limite di tentativi viene raggiunto senza la cancellazione dell'errore, il canale passa allo stato ARRESTATO. Un canale arrestato deve essere riavviato manualmente dall'operatore. Se l'errore è ancora presente, non riprovare. Quando viene avviata correttamente, la coda di trasmissione viene riabilitata.

Se l'iniziatore del canale gestore code si arresta mentre un canale è in stato REENTAMENTO o ARRESTATO, lo stato del canale viene ricordato quando l'iniziatore del canale viene riavviato. Tuttavia, lo stato del canale per il tipo di canale SVRCONN viene reimpostato se l' gestore code si arresta mentre il canale è in stato STOPPED.

Se un canale non è in grado di inserire un messaggio nella coda di destinazione perché tale coda è piena o non è consentita, il canale può ritentare l'operazione un certo numero di volte (specificato nell'attributo conteggio tentativi messaggi) in un intervallo di tempo (specificato nell'attributo intervallo tentativi messaggi). In alternativa, è possibile scrivere la propria uscita di nuovo tentativo di messaggio che determina le circostanze che causano un nuovo tentativo e il numero di tentativi effettuati. Il canale passa allo stato PAUSED durante l'attesa del completamento dell'intervallo di tentativi del messaggio.

Consultare Attributi del canale per informazioni relative agli attributi del canale e Programmi di uscita del canale per i canali di messaggistica per informazioni relative all'uscita del nuovo tentativo di messaggio.

Limiti del canale di connessione server
È possibile impostare i limiti del canale di connessione server per evitare che le applicazioni client esauriscano le risorse del canale del gestore code, **MAXINST**, e per impedire che una singola applicazione client esaurisca la capacità del canale di connessione server, **MAXINSTC**.

Un numero massimo totale di canali può essere attivo in qualsiasi momento su un singolo gestore code. Il numero totale di istanze del canale di connessione server è incluso nel numero massimo di canali attivi.

Se non si specifica il numero massimo di istanze simultanee di un canale di connessione server che è possibile avviare, è possibile che una singola applicazione client, che si connette a un singolo canale di connessione server, esaurisca il numero massimo di canali attivi disponibili. Quando viene raggiunto il numero massimo di canali attivi, impedisce l'avvio di altri canali sul gestore code. Per evitare questa situazione, è necessario limitare il numero di istanze simultanee di un singolo canale di connessione server che è possibile avviare, indipendentemente dal client che le ha avviate.

Se il valore del limite viene ridotto al di sotto del numero di istanze attualmente in esecuzione del canale di connessione del server, anche a zero, i canali in esecuzione non vengono interessati. Le nuove istanze non possono essere avviate fino a quando non cessa l'esecuzione di istanze esistenti sufficienti in modo che il numero di istanze attualmente in esecuzione sia inferiore al valore del limite.

Inoltre, molti canali di connessione client diversi possono connettersi a un canale di connessione server individuale. Il limite sul numero di istanze simultanee di un singolo canale di connessione server che è possibile avviare, indipendentemente dal client che le ha avviate, impedisce a qualsiasi client di esaurire la capacità massima del canale attivo del gestore code. Se non si limita anche il numero di istanze

simultanee di un singolo canale di connessione server che può essere avviato da un singolo client, è possibile che una singola applicazione client malfunzionante apra un numero di connessioni tale da esaurire la capacità del canale assegnata a un singolo canale di connessione server e quindi impedisca ad altri client che devono utilizzare il canale di connettersi ad esso. Per evitare questa situazione, è necessario limitare il numero di istanze simultanee di un singolo canale di connessione server che può essere avviato da un singolo client.

Se il valore del limite del singolo client viene ridotto al di sotto del numero di istanze del canale di connessione server attualmente in esecuzione da singoli client, anche a zero, i canali in esecuzione non vengono interessati. Tuttavia, le nuove istanze del canale di connessione server non possono essere avviate da un singolo client che supera il nuovo limite fino a quando non cessa l'esecuzione di un numero sufficiente di istanze esistenti da tale client, in modo che il numero di istanze attualmente in esecuzione sia inferiore al valore di questo parametro.

Verifica che l'altra estremità del canale sia ancora disponibile

È possibile utilizzare l'intervallo di heartbeat, l'intervallo keep alive e il timeout di ricezione per verificare che l'altra estremità del canale sia disponibile.

Segnali di stato

È possibile utilizzare l'attributo del canale dell'intervallo heartbeat per specificare che i flussi devono essere passati dall'MCA di invio quando non vi sono messaggi nella coda di trasmissione, come descritto in Intervallo heartbeat (HBINT).

Tenere attivo

Nei sistemi WebSphere MQ per UNIX, Linuxe Windows , se si utilizza TCP come protocollo di trasporto, è possibile impostare `keepalive=yes`. Se si specifica questa opzione, TCP controlla periodicamente che l'altra estremità della connessione sia ancora disponibile. Non è così, il canale viene terminato. Questa opzione è descritta in Intervallo keepalive (KAINT).

Se si dispone di canali non affidabili che riportano errori TCP, l'utilizzo dell'opzione **Keepalive** indica che è più probabile che i canali vengano ripristinati.

È possibile specificare intervalli di tempo per controllare il comportamento dell'opzione **Keepalive** . Quando si modifica l'intervallo di tempo, vengono interessati solo i canali TCP/IP avviati dopo la modifica. Assicurarsi che il valore scelto per l'intervallo di tempo sia inferiore al valore dell'intervallo di disconnessione per il canale.

Per ulteriori informazioni sull'utilizzo dell'opzione **Keepalive** , consultare il parametro KAINT nel comando DEFINE CHANNEL .

Timeout ricezione

Se si utilizza TCP come protocollo di trasporto, anche l'estremità di ricezione di una connessione del canale non MQI inattiva viene chiusa se non vengono ricevuti dati per un periodo di tempo. Questo periodo, il valore *timeout di ricezione* , è determinato in base al valore HBINT (heartbeat interval).

Nei sistemi WebSphere MQ per UNIX, Linuxe Windows , il valore *timeout di ricezione* è impostato come segue:

1. Per un numero iniziale di flussi, prima di qualsiasi negoziazione, il valore *timeout di ricezione* è il doppio del valore HBINT dalla definizione del canale.
2. Dopo che i canali negoziano un valore HBINT, se HBINT è impostato su meno di 60 secondi, il valore di *timeout di ricezione* è impostato sul doppio di questo valore. Se HBINT è impostato su 60 o più secondi, il valore di *timeout di ricezione* è impostato su 60 secondi maggiore del valore di HBINT.

Nota:

1. Se uno dei valori è zero, non si verifica alcun timeout.

2. Per le connessioni che non supportano gli heartbeat, il valore HBINT viene negoziato a zero nel passo 2 e quindi non vi è alcun timeout, quindi è necessario utilizzare TCP/IP KEEPALIVE.
3. Per le connessioni client che utilizzano conversazioni condivise, gli heartbeat possono fluire attraverso il canale (da entrambe le estremità) tutto il tempo, non solo quando un MQGET è in sospeso.
4. Per le connessioni client in cui le conversazioni di condivisione non sono in uso, gli heartbeat vengono trasferiti dal server solo quando il client emette una chiamata MQGET con attesa. Pertanto, non si consiglia di impostare l'intervallo heartbeat troppo piccolo per i canali client. Ad esempio, se l'heartbeat è impostato su 10 secondi, una chiamata MQCMIT non riesce (con MQRC_CONNECTION_BROKEN) se il commit impiega più di 20 secondi perché non sono stati trasmessi dati durante questo periodo di tempo. Ciò può accadere con grandi unità di lavoro. Tuttavia, non si verifica se vengono scelti i valori appropriati per l'intervallo di heartbeat poiché solo MQGET con attesa richiede periodi di tempo significativi.

   Se SHARECNV non è zero, il client utilizza una connessione full duplex, il che significa che il client può (e fa) heartbeat durante tutte le chiamate MQI
5. Nei canali WebSphere MQ Versione 7 Client, gli heartbeat possono fluire sia dal lato server che da quello client. Il timeout su entrambe le estremità è basato su 2*HBINT per HBINTs di meno di 60 secondi e HBINT+60 per HBINTs di più di 60 secondi.
6. L'annullamento della connessione dopo il doppio dell'intervallo heartbeat è valido perché un flusso di dati o heartbeat è previsto almeno ad ogni intervallo heartbeat. L'impostazione dell'intervallo heartbeat troppo piccolo, tuttavia, può causare problemi, soprattutto se si utilizzano le uscite del canale. Ad esempio, se il valore HBINT è un secondo e viene utilizzata un'uscita di invio o ricezione, l'estremità di ricezione attende solo 2 secondi prima di annullare il canale. Se l'MCA sta eseguendo un'attività come la codifica del messaggio, questo valore potrebbe essere troppo breve.

Adozione di un MCA

La funzione Adotta MCA consente a IBM WebSphere MQ Explorer di annullare un canale ricevente e avviarne uno nuovo al suo posto.

Se un canale subisce un errore di comunicazione, il canale ricevente potrebbe essere lasciato in uno stato di 'ricezione comunicazioni '. Quando le comunicazioni vengono ristabilite, il canale mittente tenta di riconnettersi. Se il gestore code remoto rileva che il canale ricevente è già in esecuzione, non consente l'avvio di un'altra versione dello stesso canale ricevente. Questo problema richiede l'intervento dell'utente per risolvere il problema o l'utilizzo del keepalive del sistema.

La funzione di adozione MCA risolve automaticamente il problema. Consente a IBM WebSphere MQ Explorer di annullare un canale ricevente e di avviarne uno nuovo al suo posto.

La funzione può essere impostata con varie opzioni. distributed Per le piattaforme distribuite, consultare Amministrazione.

Arresto e disattivazione dei canali

Questo argomento spiega come arrestare e disattivare un canale prima della scadenza dell'intervallo di tempo di disconnessione.

I canali di messaggi sono progettati per essere connessioni di lunga durata tra gestori code con terminazione ordinata controllata solo dall'attributo dell'intervallo di disconnessione del canale. Questo meccanismo funziona a meno che l'operatore non debba terminare il canale prima della scadenza dell'intervallo di tempo di disconnessione. Questa necessità può verificarsi nelle situazioni seguenti:

- Disattivazione del sistema
- Conservazione delle risorse
- Azione unilaterale a un'estremità di un canale

In questo caso, è possibile arrestare il canale. È possibile eseguire questa operazione utilizzando:

- comando STOP CHANNEL MQSC
- comando Arresta canale PCF

- IBM WebSphere MQ Explorer

Esistono tre opzioni per arrestare i canali utilizzando questi comandi:

QUIESCE
L'opzione QUIESCE tenta di terminare il batch corrente di messaggi prima di arrestare il canale.

Forza
L'opzione FORCE tenta di arrestare il canale immediatamente e potrebbe richiedere la risincronizzazione del canale quando viene riavviato poiché il canale potrebbe essere lasciato in dubbio.

TERMINATE
L'opzione TERMINATE tenta di arrestare immediatamente il canale e termina il thread o il processo del canale.

Tutte queste opzioni lasciano il canale nello stato ARRESTATO, richiedendo l'intervento dell'operatore per riavviarlo.

L'arresto del canale all'estremità di invio è effettivo ma richiede l'intervento dell'operatore per il riavvio. All'estremità di ricezione del canale, le cose sono molto più difficili perché l'MCA è in attesa di dati dal lato di invio e non c'è modo di avviare una terminazione *ordinata* del canale dal lato di ricezione; il comando di arresto è in sospeso fino a quando l'MCA non ritorna dall'attesa dei dati.

Di conseguenza ci sono tre modi consigliati di utilizzare i canali, a seconda delle caratteristiche operative richieste:

- Se vuoi che i tuoi canali siano di lunga durata, tieni presente che ci può essere una terminazione ordinata solo dall'estremità di invio. Quando i canali vengono interrotti, ossia arrestati, è richiesto l'intervento dell'operatore (un comando START CHANNEL) per riavviarli.
- Se si desidera che i canali siano attivi solo quando vi sono messaggi da trasmettere, impostare l'intervallo di disconnessione su un valore abbastanza basso. L'impostazione predefinita è alta e quindi non è consigliata per i canali in cui è richiesto questo livello di controllo. Poiché è difficile interrompere il canale ricevente, l'opzione più economica è quella di disconnettere e riconnettere automaticamente il canale in base alle esigenze del workload. Per la maggior parte dei canali, l'impostazione appropriata dell'intervallo di disconnessione può essere stabilita in modo euristico.
- È possibile utilizzare l'attributo heartbeat - interval per fare in modo che l'MCA mittente invii un flusso heartbeat all'MCA ricevente durante i periodi in cui non ha messaggi da inviare. Questa azione rilascia l'MCA ricevente dal relativo stato di attesa e le fornisce l'opportunità di sospendere il canale senza attendere la scadenza dell'intervallo di disconnessione. Fornire all'intervallo di heartbeat un valore inferiore a quello dell'intervallo di disconnessione.

  Nota:

  1. Si consiglia di impostare l'intervallo di disconnessione su un valore basso o di utilizzare gli heartbeat per i canali del server. Questo valore basso è per consentire il caso in cui il canale richiedente termina in modo anomalo (ad esempio, perché il canale è stato annullato) quando non ci sono messaggi per il canale server da inviare. Se l'intervallo di disconnessione è impostato su un valore elevato e gli heartbeat non sono in uso, il server non rileva che il richiedente è terminato (operazione che eseguirà solo la volta successiva che tenterà di inviare un messaggio al richiedente). Mentre il server è ancora in esecuzione, mantiene la coda di trasmissione aperta per l'input esclusivo al fine di ottenere ulteriori messaggi che arrivano sulla coda. Se si tenta di riavviare il canale dal richiedente, la richiesta di avvio riceve un errore poiché il server ha ancora la coda di trasmissione aperta per l'input esclusivo. È necessario arrestare il canale del server e riavviare di nuovo il canale dal richiedente.

Riavvio dei canali arrestati

Quando un canale passa allo stato ARRESTATO, è necessario riavviare manualmente il canale.

Per riavviare il canale, immettere uno dei seguenti comandi:

- Comando START CHANNEL MQSC
- Il comando Avvio canale PCF
- IBM WebSphere MQ Explorer

Per i canali mittente o server, quando il canale è entrato nello stato STOPPED, la coda di trasmissione associata è stata impostata su GET (DISABLED) e il trigger è stato disattivato. Quando viene ricevuta la richiesta di avvio, questi attributi vengono reimpostati automaticamente.

Se l'iniziatore di canali (su piattaforme distribuite) si arresta mentre un canale è in stato RETENTOR o STOPPED, lo stato del canale viene ricordato quando l'iniziatore di canali viene riavviato. Tuttavia, lo stato del canale per il tipo di canale SVRCONN viene reimpostato se l'iniziatore del canale si arresta mentre il canale si trova nello stato ARRESTATO.

Canali in dubbio

Un canale in dubbio è un canale in dubbio con un canale remoto su cui sono stati inviati e ricevuti i messaggi.

Notare la distinzione tra questo e un gestore code che è in dubbio su quali messaggi devono essere sottoposti a commit in una coda.

È possibile ridurre la possibilità che un canale venga messo in dubbio utilizzando il parametro del canale Batch Heartbeat (BATCHHB). Quando viene specificato un valore per questo parametro, un canale mittente controlla che il canale remoto sia ancora attivo prima di intraprendere qualsiasi ulteriore azione. Se non viene ricevuta alcuna risposta, il canale ricevente viene considerato non più attivo. I messaggi possono essere sottoposti a rollback e reinstradati e il canale mittente non viene messo in dubbio. Ciò riduce il tempo durante il quale il canale potrebbe essere messo in dubbio rispetto al periodo tra il canale mittente che verifica che il canale ricevente sia ancora attivo e che il canale ricevente abbia ricevuto i messaggi inviati. Consultare Attributi del canale per ulteriori informazioni sul parametro heartbeat batch.

I problemi del canale in dubbio vengono generalmente risolti automaticamente. Anche quando la comunicazione viene persa e un canale viene messo in dubbio con un batch di messaggi al mittente con stato di ricezione sconosciuto, la situazione viene risolta quando la comunicazione viene ristabilita. Il numero di sequenza e i record LUWID vengono conservati per questo scopo. Il canale è in dubbio fino a quando non sono state scambiate le informazioni LUWID e solo un batch di messaggi può essere in dubbio per il canale.

È possibile, quando necessario, risincronizzare manualmente il canale. Il termine *manuale* include l'uso di operatori o programmi che contengono i comandi di gestione del sistema WebSphere MQ . Il processo di risincronizzazione manuale funziona come segue. Questa descrizione utilizza i comandi MQSC, ma è anche possibile utilizzare gli equivalenti PCF.

1. Utilizzare il comando DISPLAY CHSTATUS per trovare l'ultimo LUWID (logical unit of work ID) con commit per ***ciascun lato*** del canale. Effettuare questa operazione utilizzando i comandi riportati di seguito:
   - Per il lato in dubbio del canale:

     ```
     DISPLAY CHSTATUS(name) SAVED CURLUWID
     ```

     È possibile utilizzare i parametri CONNAME e XMITQ per identificare ulteriormente il canale.
   - Per il lato ricevente del canale:

     ```
     DISPLAY CHSTATUS(name) SAVED LSTLUWID
     ```

     È possibile utilizzare il parametro CONNAME per identificare ulteriormente il canale.

   I comandi sono diversi perché solo il lato mittente del canale può essere in dubbio. Il lato ricevente non è mai in dubbio.

   In WebSphere MQ per IBM i, il comando DISPLAY CHSTATUS può essere eseguito da un file utilizzando il comando STRMQMMQSC o il comando CL Work with MQM Channel Status, WRKMQMCHST
2. Se i due LUWID sono gli stessi, il lato ricevente ha eseguito il commit dell'unità di lavoro che il mittente considera in dubbio. Il lato mittente può ora rimuovere i messaggi in dubbio dalla coda di trasmissione e riabilitarli. Questa operazione viene eseguita con il seguente comando RESOLVE del canale:

```
RESOLVE CHANNEL(name) ACTION(COMMIT)
```

3. Se i due LUWID sono diversi, il lato ricevente non ha eseguito il commit dell'unità di lavoro che il mittente considera in dubbio. Il lato mittente deve conservare i messaggi in dubbio sulla coda di trasmissione e inviarli nuovamente. Questa operazione viene eseguita con il seguente comando RESOLVE del canale:

```
RESOLVE CHANNEL(name) ACTION(BACKOUT)
```

Una volta completato questo processo, il canale non è più in dubbio. La coda di trasmissione può ora essere utilizzata da un altro canale, se necessario.

Determinazione del problema

Ci sono due aspetti distinti per la determinazione dei problemi: i problemi rilevati quando un comando viene inoltrato e i problemi rilevati durante il funzionamento dei canali.

Convalida del comando

I comandi e i dati del pannello devono essere privi di errori prima di essere accettati per l'elaborazione. Tutti gli errori rilevati dalla convalida vengono immediatamente notificati all'utente dai messaggi di errore.

La diagnosi del problema inizia con l'interpretazione di questi messaggi di errore e l'esecuzione di un'azione correttiva.

Problemi di elaborazione

I problemi rilevati durante il normale funzionamento dei canali vengono notificati alla console di sistema o al log di sistema. La diagnosi del problema inizia con la raccolta di tutte le informazioni rilevanti dal file di log e continua con l'analisi per identificare il problema.

I messaggi di conferma e di errore vengono restituiti al terminale che ha avviato i comandi, quando possibile.

WebSphere MQ produce dati statistici e di contabilità, che è possibile utilizzare per identificare le tendenze di utilizzo e prestazioni. distributed Su piattaforme distribuite, queste informazioni vengono prodotte come record PCF, consultare Tipo di dati della struttura per i dettagli.

Messaggi e codici

Per i messaggi e i codici che consentono la diagnosi primaria del problema, consultare Messaggi diagnostici e codici di errore.

Sicurezza dei messaggi

Oltre alle tipiche funzioni di ripristino di WebSphere MQ, la gestione delle code distribuite garantisce che i messaggi vengano consegnati correttamente utilizzando una procedura del punto di sincronizzazione coordinata tra le due estremità del canale dei messaggi. Se questa procedura rileva un errore, chiude il canale in modo da poter esaminare il problema e mantiene i messaggi in modo sicuro nella coda di trasmissione fino a quando il canale non viene riavviato.

La procedura del punto di sincronizzazione ha un ulteriore vantaggio in quanto tenta di recuperare una situazione *in dubbio* all'avvio del canale. (*In dubbio* è lo stato di un'unità di recupero per cui è stato richiesto un punto di sincronizzazione ma il risultato della richiesta non è ancora noto.) A questa funzione sono associate anche le due funzioni:

1. Risolvi con commit o backout
2. Reimposta il numero di sequenza

L'uso di queste funzioni si verifica solo in circostanze eccezionali perché il canale si ripristina automaticamente nella maggior parte dei casi.

Messaggi veloci, non persistenti

L'attributo del canale NPMSPEED (velocità dei messaggi non persistenti) può essere utilizzato per specificare che i messaggi non persistenti sul canale devono essere consegnati più rapidamente. Per ulteriori informazioni su questo attributo, consultare Velocità messaggio non persistente (NPMSPEED).

Se un canale termina mentre i messaggi veloci e non persistenti sono in transito, i messaggi potrebbero andare persi e spetta all'applicazione organizzarne il ripristino, se necessario.

Se il canale ricevente non può inserire il messaggio nella sua coda di destinazione, viene collocato nella coda di messaggi non recapitabili, se ne è stato definito uno. In caso contrario, il messaggio viene eliminato.

Nota: Se l'altra estremità del canale non supporta l'opzione, il canale viene eseguito alla velocità normale.

Messaggi non recapitati

Per informazioni su cosa accade quando un messaggio non può essere consegnato, consultare “Cosa succede quando un messaggio non può essere consegnato?” a pagina 67.

Cosa succede quando un messaggio non può essere consegnato?

Quando un messaggio non può essere consegnato, l'MCA può elaborarlo in diversi modi. Può riprovare, può tornare al mittente o può inserirlo nella coda di messaggi non recapitabili.

Figura 15 a pagina 67 mostra l'elaborazione che si verifica quando un MCA non è in grado di inserire un messaggio nella coda di destinazione. (Le opzioni mostrate non si applicano a tutte le piattaforme.)

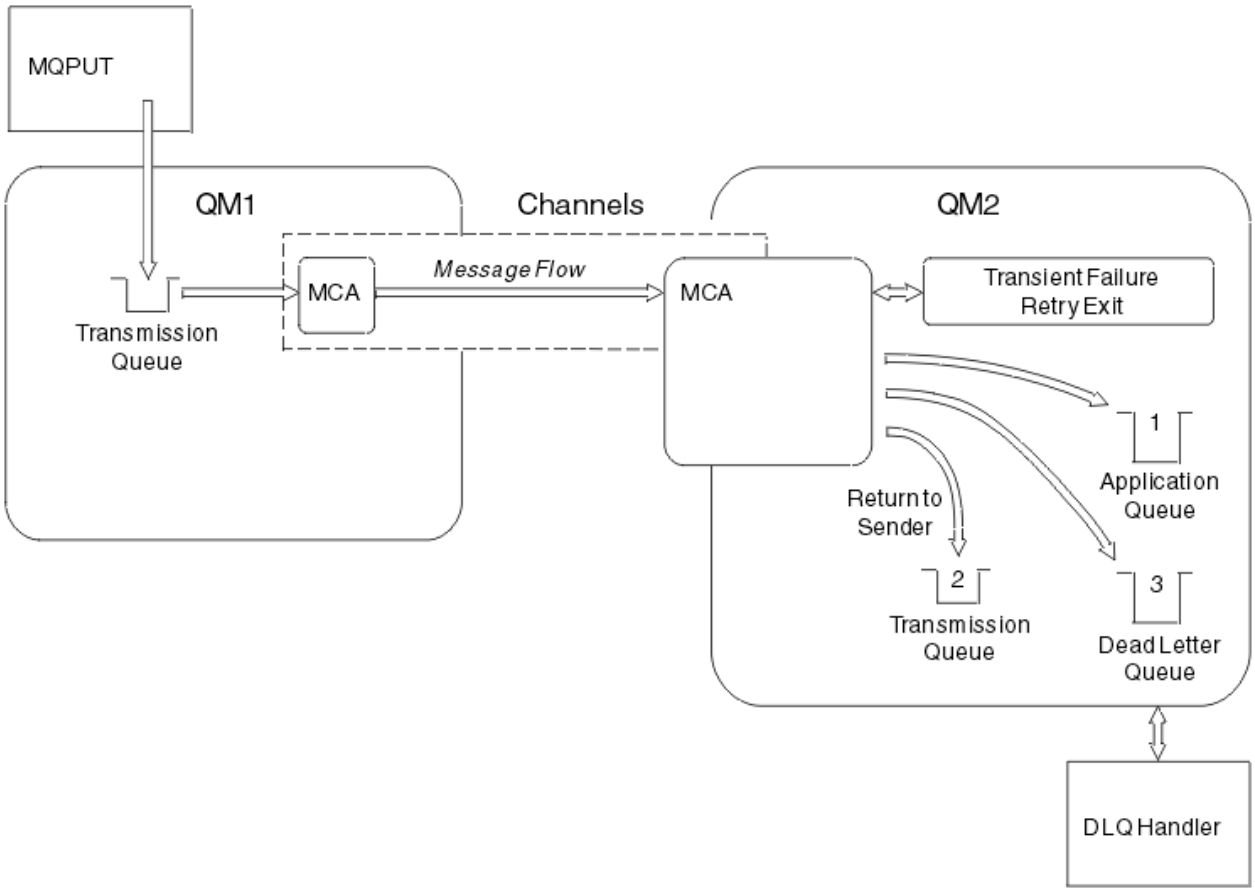


Figura 15. Cosa succede quando un messaggio non può essere consegnato

Come mostrato nella figura, l'MCA può eseguire diverse operazioni con un messaggio che non è in grado di consegnare. L'azione intrapresa è determinata dalle opzioni specificate quando il canale è definito e dalle opzioni del prospetto MQPUT per il messaggio.

1. tentativo messaggi

   Se l'MCA non è in grado di inserire un messaggio nella coda di destinazione per un motivo che potrebbe essere transitorio (ad esempio, perché la coda è piena), l'MCA può attendere e ritentare l'operazione in un secondo momento. È possibile determinare se l'MCA attende, per quanto tempo e quante volte tenta.

   - È possibile specificare un intervallo e un tempo di tentativi del messaggio per gli errori MQPUT quando si definisce il canale. Se il messaggio non può essere inserito nella coda di destinazione perché la coda è piena o non è consentita per le immissioni, l'MCA tenta l'operazione il numero di volte specificato, nell'intervallo di tempo specificato.
   - È possibile scrivere la propria uscita di messaggi - tentativi. L'uscita consente di specificare in quali condizioni si desidera che l'MCA tenti nuovamente l'operazione MQPUT o MQOPEN. Specificare il nome dell'uscita quando si definisce il canale.

2. ritorno al mittente

   Se il tentativo del messaggio ha avuto esito negativo o è stato rilevato un tipo di errore diverso, l'MCA può inviare nuovamente il messaggio al mittente. Per abilitare il ritorno al mittente, è necessario specificare le seguenti opzioni nel descrittore del messaggio quando si inserisce il messaggio nella coda originale:

   - Opzione di report MQRO_EXCEPTION_WITH_FULL_DATA
   - Opzione di report MQRO_DISCARD_MSG
   - Il nome della coda di risposta e del gestore code di risposta

   Se l'MCA non è in grado di inserire il messaggio nella coda di destinazione, genera un report di eccezioni contenente il messaggio originale e lo inserisce in una coda di trasmissione da inviare alla coda di risposta specificata nel messaggio originale. (Se la coda di risposta si trova sullo stesso gestore code dell'MCA, il messaggio viene inserito direttamente in quella coda, non in una coda di trasmissione.)

3. Coda di messaggi non recapitabili

   Se un messaggio non può essere consegnato o restituito, viene inserito nella coda di messaggi non recapitabili (DLQ). È possibile utilizzare il gestore DLQ per elaborare il messaggio. Questa elaborazione viene descritta in Gestione dei messaggi non recapitati con il gestore code di messaggi non recapitabili WebSphere MQ per IBM WebSphere MQ per sistemi UNIX, Linux. Se la coda di messaggi non instradabili non è disponibile, l'MCA di invio lascia il messaggio sulla coda di trasmissione e il canale si arresta. Su un canale veloce, i messaggi non persistenti che non possono essere scritti in una coda di messaggi non recapitabili vengono persi.

   Su IBM WebSphere MQ Version 7.0, se non è definita alcuna coda di messaggi non recapitabili locale, la coda remota non è disponibile o definita e non è presente alcuna coda di messaggi non recapitabili remota, il canale mittente va in RETRY e i messaggi vengono automaticamente sottoposti a rollback nella coda di trasmissione.

Riferimenti correlati

Utilizza coda di messaggi non instradabili (USEDLQ)

Attivazione dei canali

WebSphere MQ fornisce una funzione per avviare automaticamente un'applicazione quando vengono soddisfatte determinate condizioni su una coda. Questa funzione viene chiamata attivazione.

Questa spiegazione è intesa come una panoramica dei concetti di attivazione. Per una descrizione completa, consultare Avvio delle applicazioni WebSphere MQ utilizzando i trigger.

Per informazioni specifiche sulla piattaforma, consultare quanto segue:

- Per Windows, consultare UNIX and Linux systems, “Attivazione di canali su sistemi UNIX, Linux e Windows .” a pagina 70

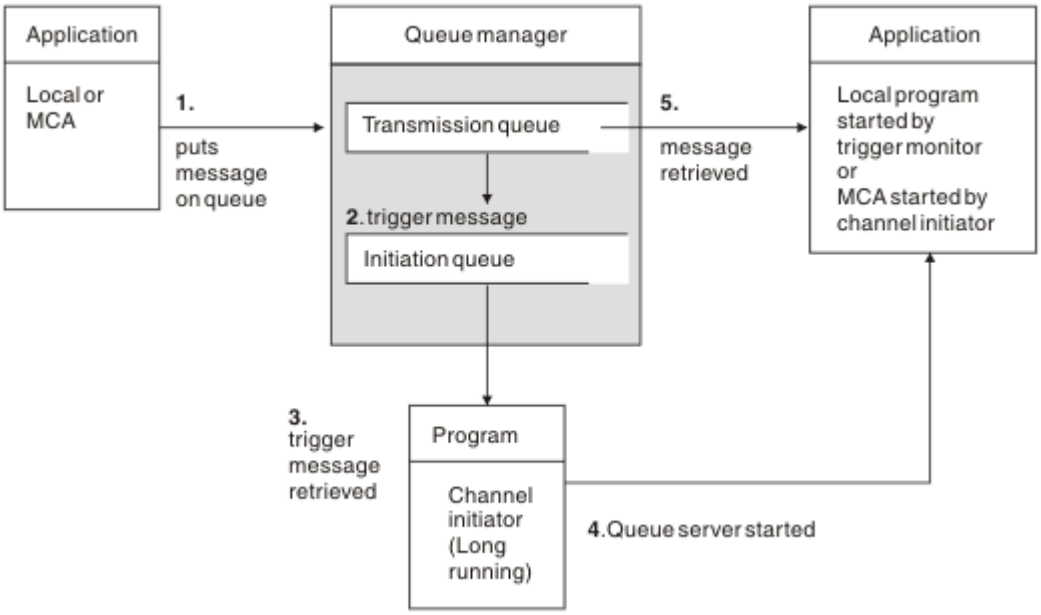


Figura 16. I concetti di attivazione

Gli oggetti richiesti per l'attivazione vengono mostrati in Figura 16 a pagina 69. Mostra la seguente sequenza di eventi:

1. Il gestore code locale inserisce un messaggio da un'applicazione o da un MCA (message channel agent) nella coda di trasmissione.
2. Quando le condizioni di attivazione sono soddisfatte, il gestore code locale inserisce un messaggio di trigger nella coda di avvio.
3. Il programma iniziatore di canali di lunga durata controlla la coda di iniziazione e richiama i messaggi quando arrivano.
4. L'iniziatore del canale elabora i messaggi del trigger in base alle informazioni contenute in essi. Queste informazioni potrebbero includere il nome del canale, nel qual caso viene avviato l'MCA corrispondente.
5. L'applicazione locale o l'MCA, dopo essere stato attivato, richiama i messaggi dalla coda di trasmissione.

Per configurare questo scenario, è necessario:

- Creare la coda di trasmissione con il nome della coda di avvio (ovvero, SYSTEM.CHANNEL.INITQ) nell'attributo corrispondente.
- Assicurarsi che la coda di avvio (SYSTEM.CHANNEL.INITQ) esiste.
- Verificare che il programma iniziatore di canali sia disponibile e in esecuzione. Il programma iniziatore di canali deve essere fornito con il nome della coda di iniziazione nel suo comando di avvio.
- Facoltativamente, creare la definizione del processo per il trigger, se non esiste, e assicurarsi che nel campo *UserData* sia contenuto il nome del canale utilizzato. Invece di creare una definizione processo, è possibile specificare il nome del canale nell'attributo *TriggerData* della coda di trasmissione. WebSphere MQ per sistemi UNIX, Linux e Windows , consentono di specificare il nome del canale come vuoto, nel qual caso viene utilizzata la prima definizione di canale disponibile con questa coda di trasmissione.
- Accertarsi che la definizione della coda di trasmissione contenga il nome della definizione di processo per servirla (se applicabile), il nome della coda di avvio e le caratteristiche di attivazione che si ritengono

più adatte. L'attributo di controllo del trigger consente di abilitare o meno il trigger, in base alle necessità.

Nota:

1. Il programma iniziatore di canali agisce come un 'controllo trigger ' che controlla la coda di iniziazione utilizzata per avviare i canali.
2. Una coda di iniziazione e un processo trigger possono essere utilizzati per attivare un numero qualsiasi di canali.
3. È possibile definire qualsiasi numero di code di iniziazione e processi trigger.
4. Si consiglia un tipo di trigger FIRST, per evitare il riempimento del sistema con l'avvio del canale.

Attivazione di canali su sistemi UNIX, Linux e Windows .

È possibile creare una definizione di processo in WebSphere MQ, definendo i processi da attivare. Utilizzare il comando MQSC DEFINE PROCESS per creare una definizione di processo che denomina il processo da attivare quando i messaggi arrivano su una coda di trasmissione. L'attributo USERDATA della definizione del processo contiene il nome del canale servito dalla coda di trasmissione.

Definire la coda locale (QM4), specificando che i messaggi trigger devono essere scritti nella coda di avvio (IQ) per attivare l'applicazione che avvia il canale (QM3.TO.QM4):

```
DEFINE QLOCAL(QM4) TRIGGER INITQ(SYSTEM.CHANNEL.INITQ) PROCESS(P1) USAGE(XMITQ)
```

Definire l'applicazione (processo P1) da avviare:

```
DEFINE PROCESS(P1) USERDATA(QM3.TO.QM4)
```

In alternativa, per i sistemi WebSphere MQ per UNIX, Linux e Windows , è possibile eliminare la necessità di una definizione di processo specificando il nome del canale nell'attributo TRIGDATA della coda di trasmissione.

Definire la coda locale (QM4). Specificare che i messaggi di trigger devono essere scritti nella coda di avvio predefinita SYSTEM.CHANNEL.INITQ, per attivare l'applicazione (processo P1) che avvia il canale (QM3.TO.QM4):

```
DEFINE QLOCAL(QM4) TRIGGER INITQ(SYSTEM.CHANNEL.INITQ)
USAGE(XMITQ) TRIGDATA(QM3.TO.QM4)
```

Se non si specifica un nome di canale, l'iniziatore del canale ricerca i file di definizione del canale finché non trova un canale associato alla coda di trasmissione denominata.

Concetti correlati

“Avvio e arresto dell'iniziatore di canali” a pagina 70
L'attivazione viene implementata utilizzando il processo dell'iniziatore di canali.

“Connessione di applicazioni mediante l'accodamento distribuito” a pagina 28
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra le installazioni WebSphere MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

Riferimenti correlati

Programmi di canale su sistemi UNIX, Linuxe Windows

Avvio e arresto dell'iniziatore di canali

L'attivazione viene implementata utilizzando il processo dell'iniziatore di canali.

Questo processo iniziatore di canali viene avviato con il comando MQSC START CHINIT. a meno che non si stia utilizzando la coda di avvio predefinita, specificare il nome della coda di avvio sul comando. Ad esempio, per utilizzare il comando START CHINIT per avviare il QI della coda per il gestore code predefinito, immettere:

```
START CHINIT INITQ(IQ)
```

Per impostazione predefinita, un iniziatore di canali viene avviato automaticamente utilizzando la coda di avvio predefinita, SYSTEM.CHANNEL.INITQ. Se si desidera avviare manualmente tutti gli iniziatori di canali, attenersi alla seguente procedura:

1. Creare e avviare il gestore code.
2. Modificare la proprietà SCHINIT del gestore code in MANUAL
3. Terminare e riavviare il gestore code

Nei sistemi Linux e Windows , un iniziatore di canali viene avviato automaticamente. Il numero di iniziatori di canali che è possibile avviare è limitato. Il valore predefinito e massimo è 3. È possibile modificare questa impostazione utilizzando MAXINITIATORS nel file qm.ini per sistemi UNIX and Linux e nel registro per sistemi Windows.

Consultare WebSphere MQ per informazioni dettagliate sul comando di esecuzione dell'iniziatore di canali **runmqchi**e sugli altri comandi di controllo.

Arresto dell'iniziatore di canali

L'iniziatore di canali predefinito viene avviato automaticamente quando si avvia un gestore code. Tutti gli iniziatori di canali vengono arrestati automaticamente quando un gestore code viene arrestato.

File di inizializzazione e di configurazione

La gestione dei dati di inizializzazione del canale dipende dalla piattaforma WebSphere MQ .

Sistemi di Windows, UNIX and Linux

Nei sistemi WebSphere MQ per Windows, UNIX and Linux , esistono *file di configurazione* per conservare le informazioni di configurazione di base sull'installazione WebSphere MQ .

Ci sono due file di configurazione: uno si applica alla macchina, l'altro a un singolo gestore code.

File di configurazione di WebSphere MQ
Questo file contiene informazioni relative a tutti i gestori code sul sistema WebSphere MQ . Il file è denominato mqs.ini. È descritto in modo completo in Amministrazione for WebSphere MQ for Windows, UNIX and Linux systems.

File di configurazione del gestore code

Questo file contiene informazioni di configurazione relative ad uno specifico gestore code. Il file è denominato qm.ini.

Viene creato durante la creazione del gestore code e può contenere le informazioni di configurazione relative a qualsiasi aspetto del gestore code. Le informazioni contenute nel file includono dettagli su come la configurazione del file di log differisce da quella predefinita nel file di configurazione WebSphere MQ .

Il file di configurazione del gestore code si trova nella root della struttura di directory occupata dal gestore code. Ad esempio, per gli attributi DefaultPath , i file di configurazione del gestore code per un gestore code denominato QMNAME sono:

Per sistemi UNIX and Linux :

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

Segue un estratto di un file qm.ini . Specifica che il listener TCP/IP deve essere in ascolto sulla porta 2500, il numero massimo di canali correnti deve essere 200 e il numero massimo di canali attivi deve essere 100.

```
TCP:
  Port=2500
CHANNELS:
  MaxChannels=200
  MaxActiveChannels=100
```

È possibile specificare un intervallo di porte TCP/IP che devono essere utilizzate da un canale in uscita. Un metodo consiste nell'utilizzare il file qm.ini per specificare l'inizio e la fine di un intervallo di valori di porta. Il seguente esempio riporta un file qm.ini che specifica un intervallo di canali:

```
TCP:
  StrPort=2500
  EndPort=3000
CHANNELS:
  MaxChannels=200
  MaxActiveChannels=100
```

Se si specifica un valore per StrPort o EndPort , è necessario specificare un valore per entrambi. Il valore di EndPort deve essere sempre maggiore del valore di StrPort.

Il canale tenta di utilizzare ogni valore di porta nell'intervallo specificato. Quando la connessione riesce, il valore della porta è la porta utilizzata dal canale.

Per sistemi Windows :

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

Per ulteriori informazioni sui file qm.ini , consultare Stanza dei file di configurazione per l'accodamento distribuito.

Conversione dati per i messaggi

I messaggi WebSphere MQ potrebbero richiedere la conversione dei dati quando vengono inviati tra le code su gestori code differenti.

Un messaggio WebSphere MQ è composto da due parti:

- Informazioni di controllo in un descrittore di messaggi
- Dati applicazione

Una delle due parti potrebbe richiedere la conversione dei dati quando viene inviata tra le code su gestori code differenti. Per informazioni sulla conversione dei dati dell'applicazione, consultare Conversione dei dati dell'applicazione.

Scrittura dei propri agent del canale dei messaggi

WebSphere MQ consente di scrivere i propri programmi MCA (message channel agent) o di installarne uno da un fornitore di software indipendente.

È possibile che si desideri scrivere i propri programmi MCA per rendere WebSphere MQ interoperativi sul proprio protocollo di comunicazione proprietario o per inviare messaggi su un protocollo che WebSphere MQ non supporta. Non è possibile scrivere il proprio MCA per interagire con un MCA fornito da WebSphere MQall'altra estremità.

Se si decide di utilizzare un MCA non fornito da WebSphere MQ, è necessario considerare i seguenti punti.

Invio e ricezione di messaggi
È necessario scrivere un'applicazione di invio che riceva i messaggi da qualsiasi posizione in cui l'applicazione li inserisce, ad esempio da una coda di trasmissione e li invia su un protocollo con cui si desidera comunicare. È inoltre necessario scrivere un'applicazione ricevente che prenda i messaggi

da questo protocollo e li inserisca nelle code di destinazione. Le applicazioni di invio e di ricezione utilizzano le chiamate MQI (message queue interface), non interfacce speciali.

È necessario assicurarsi che i messaggi vengano consegnati solo una volta. Il coordinamento del punto di sincronizzazione può essere utilizzato per facilitare questa distribuzione.

Funzione di controllo canale
È necessario fornire le proprie funzioni di amministrazione per controllare i canali. Non è possibile utilizzare le funzioni di amministrazione del canale WebSphere MQ sia per la configurazione (ad esempio, il comando DEFINE CHANNEL) che per il controllo (ad esempio, DISPLAY CHSTATUS) dei canali.

File di inizializzazione
È necessario fornire il proprio file di inizializzazione, se necessario.

Conversione dati applicazione
È probabile che si desideri consentire la conversione dei dati per i messaggi inviati a un sistema differente. In tal caso, utilizzare l'opzione MQGMO_CONVERT nella chiamata MQGET quando si richiamano i messaggi da qualsiasi posizione in cui l'applicazione li inserisce, ad esempio la coda di trasmissione.

Uscite utente
Considerare se sono necessarie uscite utente. In tal caso, è possibile utilizzare le stesse definizioni di interfaccia utilizzate da WebSphere MQ .

Triggering
Se l'applicazione inserisce i messaggi in una coda di trasmissione, è possibile impostare gli attributi della coda di trasmissione in modo che l'MCA di invio venga attivato quando i messaggi arrivano sulla coda.

Iniziatore di canali
È possibile che sia necessario fornire il proprio iniziatore di canali.

Altre cose da considerare per la gestione della coda distribuita

Altri argomenti da considerare quando si prepara WebSphere MQ per la gestione delle code distribuite. Questo argomento riguarda la coda di messaggi non recapitati, le code in uso, le estensioni di sistema e i programmi di uscita utente e i canali e listener in esecuzione come applicazioni attendibili.

Coda messaggi non recapitati

Per assicurarsi che i messaggi in arrivo sulla coda di messaggi non recapitati (nota anche come coda di messaggi non recapitabili o DLQ) vengano elaborati, creare un programma che possa essere attivato o eseguito a intervalli regolari per gestire tali messaggi. Un gestore DLQ viene fornito con WebSphere MQ su sistemi UNIX and Linux ; per ulteriori informazioni, consultare The sample DLQ handler, amqsdlq.

Code in uso

Gli MCA per i canali riceventi possono mantenere aperte le code di destinazione anche quando i messaggi non vengono trasmessi. Ciò determina la visualizzazione delle code come "in uso".

Numero massimo di canali

Consultare Stanza del file di configurazione per l'accodamento distribuito .

Estensioni di sistema e programmi di uscita utente

Viene fornita una funzionalità nella definizione del canale per consentire l'esecuzione di programmi aggiuntivi in momenti definiti durante l'elaborazione dei messaggi. Questi programmi non vengono forniti con WebSphere MQ, ma possono essere forniti da ciascuna installazione in base ai requisiti locali.

Per poter essere eseguiti, questi programmi di uscita utente devono avere nomi predefiniti e devono essere disponibili durante la chiamata ai programmi del canale. I nomi dei programmi di uscita utente sono inclusi nelle definizioni del canale messaggi.

Esiste un'interfaccia di blocco di controllo definita per la consegna del controllo a questi programmi e per la gestione della restituzione del controllo da questi programmi.

Le posizioni precise in cui vengono richiamati questi programmi e i dettagli dei nomi e dei blocchi di controllo si trovano in Programmi di uscita canale per i canali di messaggistica .

Esecuzione di canali e listener come applicazioni attendibili

Se le prestazioni sono una considerazione importante nell'ambiente e l'ambiente è stabile, è possibile eseguire i canali e i listener come attendibili, utilizzando il bind FASTPATH. Ci sono due fattori che influenzano se i canali e i listener vengono eseguiti come attendibili:

- La variabile di ambiente MQ_CONNECT_TYPE=FASTPATH o MQ_CONNECT_TYPE = STANDARD. È sensibile al maiuscolo / minuscolo. Se si specifica un valore non valido, viene ignorato.
- MQIBindType nella stanza Channels del file `qm.ini` o del file di registro. È possibile impostarlo su FASTPATH o STANDARD e non è sensibile al maiuscolo / minuscolo. L'impostazione predefinita è Standard.

È possibile utilizzare MQIBindType in associazione con la variabile di ambiente per ottenere l'effetto richiesto nel modo seguente:

MQIBindType	**Variabile di ambiente**	**Risultato**
STANDARD	NON DEFINITO	STANDARD
Percorso veloce	NON DEFINITO	Percorso veloce
STANDARD	STANDARD	STANDARD
Percorso veloce	STANDARD	STANDARD
STANDARD	Percorso veloce	STANDARD
Percorso veloce	Percorso veloce	Percorso veloce
STANDARD	CLIENT	CLIENT
Percorso veloce	CLIENT	STANDARD
STANDARD	LOCALE	STANDARD
Percorso veloce	LOCALE	STANDARD

In sintesi, ci sono solo due modi per rendere realmente affidabili i canali e i listener:

1. Specificando MQIBindType= FASTPATH in `qm.ini` o nel registro e non specificando la variabile di ambiente.
2. Specificando MQIBindType= FASTPATH in `qm.ini` o nel registro e impostando la variabile di ambiente su FASTPATH.

Considerare l'esecuzione dei listener come attendibili, poiché i listener sono processi stabili. Considerare l'esecuzione dei canali come sicuri, a meno che non si stiano utilizzando uscite di canali instabili o il comando STOP CHANNEL MODE (TERMINATE).

Monitoraggio e controllo dei canali su UNIX, Linux, and Windows

Per DQM è necessario creare, monitorare e controllare i canali per i gestori code remoti. È possibile controllare i canali utilizzando comandi, programmi, IBM WebSphere MQ Explorer, file per le definizioni dei canali e un'area di memoria per le informazioni di sincronizzazione.

È possibile utilizzare i seguenti tipi di comando:

I comandi IBM WebSphere MQ (MQSC)
È possibile utilizzare MQSC come singoli comandi in una sessione MQSC in sistemi Windows, UNIX and Linux . Per emettere comandi più complicati o multipli, è possibile creare MQSC in un file che si esegue dalla riga comandi. Per i dettagli, consultare Comandi MQSC. Questa sezione fornisce alcuni semplici esempi di utilizzo di MQSC per l'accodamento distribuito.

I comandi del canale sono un sottoinsieme di MQSC (IBM WebSphere MQ Commands). Utilizzare MQSC e i comandi di controllo per:

- Creare, copiare, visualizzare, modificare ed eliminare le definizioni di canale
- Avviare e arrestare i canali, eseguire il ping, ripristinare i numeri di sequenza dei canali e risolvere i messaggi in dubbio quando i collegamenti non possono essere ristabiliti
- Visualizza informazioni di stato sui canali

Comandi di controllo
È inoltre possibile immettere i *comandi di controllo* dalla riga comandi per alcune di tali funzioni. Per dettagli, consultare Comandi di controllo.

Comandi del formato del comando programmabile
Per dettagli, consultare Comandi PCF.

IBM WebSphere MQ Explorer
Su sistemi UNIX, Linux e Windows , è possibile utilizzare IBM WebSphere MQ Explorer. Ciò fornisce un'interfaccia di gestione grafica per eseguire le attività di gestione come alternativa all'utilizzo dei comandi di controllo o dei comandi MQSC. Le definizioni di canale vengono conservate come oggetti del gestore code.

Ogni gestore code dispone di un componente DQM per il controllo delle interconnessioni ai gestori code remoti compatibili. Un'area di memoria contiene numeri di sequenza e identificatori *LUW (logical unit of work)* . Vengono utilizzati per scopi di sincronizzazione del canale.

Per un elenco delle funzioni disponibili durante l'impostazione e il controllo dei canali di messaggi, utilizzando i diversi tipi di comando, consultare Tabella 8 a pagina 76.

Concetti correlati

“Introduzione agli oggetti” a pagina 78
I canali devono essere definiti e i relativi oggetti associati devono esistere ed essere disponibili per l'utilizzo, prima che un canale possa essere avviato. Questa sezione mostra come.

“Impostazione della comunicazione per Windows” a pagina 84
Quando un canale di gestione dell'accodamento distribuito viene avviato, tenta di utilizzare la connessione specificata nella definizione del canale. Perché ciò abbia esito positivo, è necessario che la connessione sia definita e disponibile. Questa sezione spiega come eseguire questa operazione utilizzando una delle quattro forme di comunicazione per sistemi WebSphere MQ per sistemi Windows .

“Impostazione della comunicazione sui sistemi UNIX and Linux” a pagina 94
DQM è una funzione di accodamento remoto per IBM WebSphere MQ. Fornisce programmi di controllo del canale per il gestore code che formano l'interfaccia per i collegamenti di comunicazione, controllabili dall'operatore di sistema. Le definizioni di canale gestite dalla gestione delle code distribuite utilizzano queste connessioni.

Riferimenti correlati

Programmi di canale su sistemi UNIX, Linuxe Windows

Esempio di pianificazione del canale dei messaggi per le piattaforme distribuite

Informazioni di configurazione di esempio

Attributi canale

Funzioni richieste per l'impostazione e il controllo dei canali

Potrebbe essere necessario un certo numero di funzioni IBM WebSphere MQ per impostare e controllare i canali. Le funzioni del canale sono illustrate in questo argomento.

È possibile creare una definizione di canale utilizzando i valori predefiniti forniti da IBM WebSphere MQ, specificando il nome del canale, il tipo di canale che si sta creando, il metodo di comunicazione da utilizzare, il nome coda di trasmissione e il nome connessione.

Il nome del canale deve essere lo stesso ad entrambe le estremità del canale e univoco nella rete. Tuttavia, è necessario limitare i caratteri utilizzati a quelli validi per i nomi oggetto IBM WebSphere MQ .

Per altre funzioni correlate al canale, consultare i seguenti argomenti:

- “Introduzione agli oggetti” a pagina 78
- “Creazione di oggetti associati” a pagina 78
- “Creazione di oggetti predefiniti” a pagina 79
- “Creazione di un canale” a pagina 79
- “Visualizzazione di un canale” a pagina 80
- “Visualizzazione dello stato del canale” a pagina 80
- “Controllo dei collegamenti mediante ping” a pagina 80
- “Avvio di un canale” a pagina 81
- “Arresto di un canale” a pagina 82
- “Ridenominazione di un canale” a pagina 83
- “Reimpostazione di un canale” a pagina 83
- “Risoluzione dei messaggi in dubbio su un canale” a pagina 84

Tabella 8 a pagina 76 mostra l'elenco completo delle funzioni IBM WebSphere MQ di cui potresti aver bisogno.

Tabella 8. Funzioni richieste nei sistemi UNIX, Linux, and Windows

Funzione	**Comandi di controllo**	**MQSC**	**WebSphere MQ Explorer equivalente?**
Funzioni del gestore code			
Modifica gestore code		ALTER DRG	Sì
Creare il gestore code	qmqm		Sì
Elimina gestore code	dltmqm		Sì
Visualizza gestore code		VISUALIZZA QMGR	Sì
Termina gestore code	qmfine		Sì
Ping gestore code		QMGR PING	No
Avvia gestore code	strmqm		Sì
Funzioni del server dei comandi			
Visualizza server dei comandi	vmqcsv		No
Termina server dei comandi	endmqcsv		No
Avvio server dei comandi	strmqcsv		No
Funzioni della coda			

Tabella 8. Funzioni richieste nei sistemi UNIX, Linux, and Windows (Continua)

Funzione	**Comandi di controllo**	**MQSC**	**WebSphere MQ Explorer equivalente?**
Modifica coda		ALTER QALIAS ALTER QLOCAL ALTER QMODEL ALTER QREMOTE Consultare Code ALTER .	Sì
Cancella coda		CANCELLA QLOCAL	Sì
Creazione coda		DEFINE QALIAS DEFINE QLOCAL DEFINE QMODEL DEFINE QREMOTE Consultare DEFINE queues .	Sì
Elimina coda		ELIMINARE QALIAS ELIMINARE QLOCAL ELIMINARE QMODEL ELIMINARE QREMOTE Vedere code DELETE .	Sì
Visualizza coda		VISUALIZZA CODA	Sì
Funzioni di processo			
Modifica processo		MODIFICA PROCESSO	Sì
Crea processo		DEFINE PROCESS	Sì
Elimina processo		Eliminazione processo	Sì
Visualizza processo		VISUALIZZA PROCESSO	Sì
Funzioni di canale			
Modifica canale		MODIFICA CANALE	Sì
Crea canale		Definire il canale	Sì
Elimina canale		Elimina canale	Sì
Visualizza canale		VISUALIZZA CANALE	Sì
Visualizza stato canale		VISUALIZZA CHSTATUS	Sì
Fine canale		Arresto canale	Sì
Ping canale		Ping canale	Sì

Tabella 8. Funzioni richieste nei sistemi UNIX, Linux, and Windows (Continua)

Funzione	**Comandi di controllo**	**MQSC**	**WebSphere MQ Explorer equivalente?**
Reimposta canale		Reimpostazione canale	Sì
Risoluzione canale		Risoluzione canale	Sì
Esegui canale	runmqchl	Avvio canale	Sì
Esegui iniziatore di canali	runmqchi	INIZIO STRINGA	No
Esegui listener[1]	runmqlsr	Avvia listener	No
Fine listener	endmqlsr (solo sistemi Windows , AIX, HP-UXe Solaris)		No

Nota:

1. Un listener potrebbe essere avviato automaticamente all'avvio del gestore code.

Introduzione agli oggetti

I canali devono essere definiti e i relativi oggetti associati devono esistere ed essere disponibili per l'utilizzo, prima che un canale possa essere avviato. Questa sezione mostra come.

Utilizzare i comandi WebSphere MQ (MQSC) o IBM WebSphere MQ Explorer per:

1. Definire canali di messaggi e oggetti associati
2. Monitorare e controllare i canali dei messaggi

Gli oggetti associati che potrebbe essere necessario definire sono:

- Code di trasmissione
- Definizioni di coda remota
- Definizioni alias gestore code
- Definizioni alias coda di risposta
- Code locali di risposta
- Processi per l'attivazione (MCA)
- Definizioni di canali di messaggi

Il particolare collegamento di comunicazione per ciascun canale deve essere definito e disponibile prima che un canale possa essere eseguito. Per una descrizione della modalità di definizione dei collegamenti LU 6.2, TCP/IP, NetBIOS, SPX e DECnet, consultare la specifica guida alla comunicazione per l'installazione. Consultare anche Informazioni di configurazione di esempio.

Per ulteriori informazioni sulla creazione e l'utilizzo degli oggetti, consultare i topic secondari riportati di seguito:

Creazione di oggetti associati

MQSC viene utilizzato per creare oggetti associati.

Utilizzare MQSC per creare la coda e gli oggetti alias: code di trasmissione, definizioni di code remote, definizioni di alias del gestore code, definizioni di alias della coda reply - to e code locali reply - to.

Creare anche le definizioni dei processi per l'attivazione (MCA) in modo simile.

Per un esempio che mostra come creare tutti gli oggetti richiesti, consultare Esempio di pianificazione del canale dei messaggi per le piattaforme distribuite .

Creazione di oggetti predefiniti

Gli oggetti predefiniti vengono creati automaticamente quando viene creato un gestore code. Questi oggetti sono code, canali, una definizione di processo e code di gestione. Una volta creati gli oggetti predefiniti, è possibile sostituirli in qualsiasi momento eseguendo il comando strmqm con l'opzione -c.

Quando si utilizza il comando crtmqm per creare un gestore code, il comando avvia anche un programma per creare una serie di oggetti predefiniti.

1. Ogni oggetto predefinito viene creato a turno. Il programma conserva un conteggio del numero di oggetti definiti con esito positivo, del numero di oggetti esistenti e sostituiti e del numero di tentativi non riusciti.
2. Il programma visualizza i risultati e, se si sono verificati degli errori, indirizza l'utente al log degli errori appropriato per i dettagli.

Una volta terminata l'esecuzione del programma, è possibile utilizzare il comando strmqm per avviare il gestore code.

Per ulteriori informazioni sui comandi crtmqm e strmqm, consultare Comandi di controllo .

Modifica degli oggetti predefiniti

Quando si specifica l'opzione -c, il gestore code viene avviato temporaneamente mentre gli oggetti vengono creati e viene quindi nuovamente arrestato. L'emissione di strmqm con l'opzione -c aggiorna gli oggetti di sistema esistenti con i valori predefiniti (ad esempio, l'attributo MCAUSER di una definizione di canale è impostato su spazi vuoti). È necessario utilizzare nuovamente il comando strmqm, senza l'opzione -c, se si desidera avviare il gestore code.

Se si desidera modificare gli oggetti predefiniti, è possibile creare la propria versione del vecchio file amqscoma.tst e modificarla.

Creazione di un canale

Creare ***due*** definizioni di canali, una a ciascuna estremità della connessione. Si crea la prima definizione di canale nel primo gestore code. Quindi, creare la seconda definizione di canale sul secondo gestore code, sull'altra estremità del link.

Entrambe le estremità devono essere definite utilizzando lo ***stesso nome canale*** . Le due estremità devono avere tipi di canale **compatibili** , ad esempio: Mittente e Destinatario.

Per creare una definizione di canale per un'estremità del collegamento utilizzare il comando MQSC DEFINE CHANNEL. Includere il nome del canale, il tipo di canale per questa estremità della connessione, un nome connessione, una descrizione (se richiesto), il nome della coda di trasmissione (se richiesto) e il protocollo di trasmissione. Includere anche qualsiasi altro attributo che si desidera sia diverso dai valori predefiniti di sistema per il tipo di canale richiesto, utilizzando le informazioni raccolte in precedenza.

Viene fornito un aiuto per decidere i valori degli attributi di canale in Attributi di canale.

Nota: Si consiglia di denominare tutti i canali nella rete in modo univoco. L'inclusione dei nomi dei gestori code di origine e di destinazione nel nome del canale è un buon modo per farlo.

Crea esempio di canale

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) +
DESCR('Sender channel to QM2') +
CONNAME(QM2) TRPTYPE(TCP) XMITQ(QM2) CONVERT(YES)
```

In tutti gli esempi di MQSC, il comando viene visualizzato come viene visualizzato in un file di comandi e come viene immesso in sistemi Windows o UNIX o Linux . I due metodi sono identici, tranne che per emettere un comando in modo interattivo, è necessario prima avviare una sessione MQSC. Immettere `runmqsc`, per il gestore code predefinito o `runmqsc` *qmname* dove *qmname* è il nome del gestore code richiesto. Quindi immettere qualsiasi numero di comandi, come mostrato negli esempi.

Per la portabilità, limitare la lunghezza della linea dei comandi a 72 caratteri. Utilizzare il carattere di concatenazione, +, come mostrato per continuare su più di una riga. In Windows utilizzare Ctrl - z per terminare la voce sulla riga comandi. Sui sistemi UNIX and Linux , utilizzare Ctrl - d. In alternativa, su sistemi UNIX, Linux o Windows , utilizzare il comando **end** .

Visualizzazione di un canale

Utilizzare il comando MQSC DISPLAY CHANNEL per visualizzare gli attributi di un canale.

Il parametro ALL del comando DISPLAY CHANNEL viene assunto per impostazione predefinita se non sono richiesti attributi specifici e il nome del canale specificato non è generico.

Gli attributi sono descritti in Attributi del canale.

Visualizza esempi di canale

```
DISPLAY CHANNEL(QM1.TO.QM2) TRPTYPE,CONVERT
DISPLAY CHANNEL(QM1.TO.*) TRPTYPE,CONVERT
DISPLAY CHANNEL(*) TRPTYPE,CONVERT
DISPLAY CHANNEL(QM1.TO.QMR34) ALL
```

Visualizzazione dello stato del canale

Utilizzare il comando MQSC DISPLAY CHSTATUS, specificando il nome del canale e se si desidera lo stato corrente dei canali o lo stato delle informazioni salvate.

DISPLAY CHSTATUS si applica a tutti i canali di messaggi. Non si applica a canali MQI diversi dai canali di connessione server.

Le informazioni visualizzate includono:

- Nome canale
- Nome connessione di comunicazione
- Stato in dubbio del canale (dove appropriato)
- Ultimo numero sequenza
- Nome coda di trasmissione (se appropriato)
- L'identificativo in dubbio (dove appropriato)
- L'ultimo numero di sequenza con commit
- Identificativo LUW (Logical unit of work)
- Processo ID
- ID thread (solo Windows)

Visualizza esempi di stato del canale

```
DISPLAY CHSTATUS(*) CURRENT
DISPLAY CHSTATUS(QM1.TO.*) SAVED
```

Lo stato salvato non si applica fino a quando non viene trasmesso almeno un batch di messaggi sul canale. Lo stato viene salvato anche quando un canale viene arrestato (utilizzando il comando STOP CHL) e quando il gestore code viene chiuso.

Controllo dei collegamenti mediante ping

Utilizzare il comando MQSC PING CHANNEL per scambiare un messaggio di dati fisso con l'estremità remota.

Il ping fornisce al supervisore del sistema la certezza che il collegamento sia disponibile e funzionante.

Il ping non comporta l'utilizzo di code di trasmissione e code di destinazione. Utilizza le definizioni di canale, il link di comunicazione correlato e l'impostazione di rete. Può essere utilizzato solo se il canale non è attualmente attivo.

È disponibile solo dai canali mittente e server. Il canale corrispondente viene avviato sul lato opposto del link ed esegue la negoziazione del parametro di avvio. Gli errori vengono notificati normalmente.

Il risultato dello scambio di messaggi viene presentato come `Ping complete` o come un messaggio di errore.

Ping con LU 6.2

Quando viene richiamato il ping, per impostazione predefinita nessun ID utente o password viene inoltrato all'estremità di ricezione. Se l'ID utente e la password sono richiesti, possono essere creati all'estremità iniziale nella definizione del canale. Se viene immessa una password nella definizione del canale, viene codificata da WebSphere MQ prima di essere salvata. Viene quindi decodificato prima di scorrere attraverso la conversazione.

Avvio di un canale

Utilizzare il comando MQSC START CHANNEL per i canali mittente, server e richiedente. Per consentire alle applicazioni di scambiare messaggi, è necessario avviare un programma listener per le connessioni in entrata.

START CHANNEL non è necessario quando un canale è stato configurato con l'attivazione del gestore code.

Quando avviato, l'MCA mittente legge le definizioni di canale e apre la coda di trasmissione. Viene emessa una sequenza di avvio del canale, che avvia in remoto l'MCA corrispondente del canale ricevente o server. Una volta avviati, i processi del mittente e del server attendono i messaggi in arrivo sulla coda di trasmissione e li trasmettono non appena arrivano.

Quando si utilizzano i canali di attivazione o di esecuzione come thread, assicurarsi che l'iniziatore di canali sia disponibile per monitorare la coda di avvio. L'iniziatore di canali viene avviato per impostazione predefinita come parte del gestore code.

Tuttavia, TCP e LU 6.2 forniscono altre funzioni:

- Per TCP sui sistemi UNIX and Linux , inetd può essere configurato per avviare un canale. inetd viene avviata come processo separato.
- Per LU 6.2 nei sistemi UNIX and Linux , configurare il prodotto SNA per avviare il processo responder LU 6.2 .
- Per LU 6.2 nei sistemi Windows , utilizzando SNA Server è possibile utilizzare TpStart (un programma di utilità fornito con SNA Server) per avviare un canale. TpStart viene avviato come processo separato.

L'utilizzo dell'opzione Start provoca sempre la risincronizzazione del canale, se necessario.

Perché l'inizio abbia successo:

- Le definizioni di canale, locale e remoto, devono esistere. Se non esiste una definizione di canale appropriata per un canale ricevente o di connessione server, ne viene creata automaticamente una predefinita se il canale è definito automaticamente. Vedere Programma di uscita di definizione automatica del canale.
- La coda di trasmissione deve esistere e non deve essere utilizzata da altri canali.
- Gli MCA, locali e remoti, devono esistere.
- Il collegamento di comunicazione deve essere disponibile.
- I gestori code devono essere in esecuzione, locali e remoti.
- Il canale dei messaggi non deve essere già in esecuzione.

Viene restituito un messaggio sullo schermo che conferma che la richiesta di avviare un canale è stata accettata. Per confermare che il comando di avvio ha avuto esito positivo, controllare il log degli errori oppure utilizzare DISPLAY CHSTATUS. I log degli errori sono:

Windows

MQ_INSTALLATION_PATH\qmgrs\qmname\errors\AMQERR01.LOG (per ogni gestore code denominato qmname)

MQ_INSTALLATION_PATH\qmgrs\@SYSTEM\errors\AMQERR01.LOG (per errori generali)

MQ_INSTALLATION_PATH rappresenta la directory di alto livello in cui è installato WebSphere MQ .

Nota: Sui sistemi Windows , si riceve ancora un messaggio nel registro eventi dell'applicazione dei sistemi Windows .

Sistemi UNIX and Linux

/var/mqm/qmgrs/qmname/errors/AMQERR01.LOG (per ogni gestore code denominato qmname)

/var/mqm/qmgrs/@SYSTEM/errors/AMQERR01.LOG (per errori generali)

Su sistemi Windows, UNIX and Linux , utilizzare il comando runmqlsr per avviare il processo listener WebSphere MQ . Per impostazione predefinita, le richieste in entrata per l'allegato del canale fanno sì che il processo listener avvii gli MCA come thread del processo amqrmppa.

```
runmqlsr -t tcp -m QM2
```

Per le connessioni in entrata, è necessario avviare il canale in uno dei tre seguenti modi:

1. Utilizzare il comando MQSC START CHANNEL, specificando il nome del canale, per avviare il canale come un processo o un thread, in base al parametro MCATYPE. (Se i canali vengono avviati come thread, sono thread di un iniziatore di canali.)

   ```
   START CHANNEL(QM1.TO.QM2)
   ```

2. Utilizzare il comando di controllo runmqchl per avviare un canale come processo.

   ```
   runmqchl -c QM1.TO.QM2 -m QM1
   ```

3. Utilizzare l'iniziatore del canale per attivare il canale.

Arresto di un canale

Utilizzare il comando MQSC STOP CHANNEL per richiedere al canale di arrestare l'attività. Il canale non avvia un nuovo batch di messaggi finché l'operatore non avvia nuovamente il canale.

Per informazioni sul riavvio dei canali arrestati, consultare “Riavvio dei canali arrestati” a pagina 64.

Questo comando può essere emesso su un canale di qualsiasi tipo, ad eccezione di MQCHT_CLNTCONN.

È possibile selezionare il tipo di arresto richiesto:

Esempio di arresto del quiesce

```
STOP CHANNEL(QM1.TO.QM2) MODE(QUIESCE)
```

Questo comando richiede la chiusura ordinata del canale. Il batch di messaggi corrente viene completato e la procedura del punto di sincronizzazione viene eseguita con l'altra estremità del canale. Se il canale è inattivo, questo comando non termina un canale di ricezione.

Esempio di arresto forzato

```
STOP CHANNEL(QM1.TO.QM2) MODE(FORCE)
```

Questa opzione arresta il canale immediatamente, ma non termina il thread o il processo del canale. Il canale non completa l'elaborazione del batch di messaggi corrente e può, quindi, lasciare il canale in dubbio. In generale, considerare l'utilizzo dell'opzione di arresto della sospensione.

Esempio di arresto

```
STOP CHANNEL(QM1.TO.QM2) MODE(TERMINATE)
```

Questa opzione arresta immediatamente il canale e termina il thread o il processo del canale.

Esempio di arresto (sospensione) arrestato

```
STOP CHANNEL(QM1.TO.QM2) STATUS(STOPPED)
```

Questo comando non specifica un MODE, quindi il valore predefinito è MODE (QUIESCE). Richiede che il canale sia arrestato in modo che non possa essere riavviato in modo automatico, ma deve essere avviato manualmente.

Esempio di arresto (sospensione) inattivo

```
STOP CHANNEL(QM1.TO.QM2) STATUS(INACTIVE)
```

Questo comando non specifica un MODE, quindi il valore predefinito è MODE (QUIESCE). Richiede che il canale venga reso inattivo in modo che venga riavviato automaticamente quando richiesto.

Ridenominazione di un canale

Utilizzare MQSC per ridenominare un canale di messaggi.

Utilizzare MQSC per effettuare le operazioni riportate di seguito:

1. Utilizzare STOP CHANNEL per arrestare il canale.
2. Utilizzare DEFINE CHANNEL per creare una definizione di canale duplicata con il nuovo nome.
3. Utilizzare DISPLAY CHANNEL per verificare che sia stato creato correttamente.
4. Utilizzare DELETE CHANNEL per eliminare la definizione del canale originale.

Se si decide di ridenominare un canale di messaggi, tenere presente che un canale dispone di ***due definizioni di canale*** , una ad ogni estremità. Assicurarsi di rinominare il canale ad entrambe le estremità contemporaneamente.

Reimpostazione di un canale

Utilizzare il comando MQSC RESET CHANNEL per modificare il numero di sequenza del messaggio.

Il comando RESET CHANNEL è disponibile per qualsiasi canale di messaggi, ma non per i canali MQI (connessione client o connessione server). Il primo messaggio avvia la nuova sequenza al successivo avvio del canale.

Se il comando viene emesso su un canale mittente o server, informa l'altro lato della modifica quando il canale viene riavviato.

Concetti correlati

“Introduzione agli oggetti” a pagina 78

I canali devono essere definiti e i relativi oggetti associati devono esistere ed essere disponibili per l'utilizzo, prima che un canale possa essere avviato. Questa sezione mostra come.

"Funzione di controllo canale" a pagina 54
La funzione di controllo del canale consente di definire, monitorare e controllare i canali.

"Connessione di applicazioni mediante l'accodamento distribuito" a pagina 28
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra le installazioni WebSphere MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

Riferimenti correlati

Reimpostazione canale

Risoluzione dei messaggi in dubbio su un canale

Utilizzare il comando MQSC RESOLVE CHANNEL quando i messaggi sono in dubbio da parte di un mittente o di un server. Ad esempio, perché un'estremità del link è stata terminata e non vi è alcuna prospettiva di ripristino.

Il comando RESOLVE CHANNEL accetta uno dei due parametri: BACKOUT o COMMIT. Il backout ripristina i messaggi nella coda di trasmissione, mentre il commit li elimina.

Il programma del canale non tenta di stabilire una sessione con un partner. Invece, determina l'identificativo LUWID (logical unit of work identifier) che rappresenta i messaggi in dubbio. Quindi, come richiesto, emette:

- BACKOUT per ripristinare i messaggi nella coda di trasmissione; oppure
- COMMIT per cancellare i messaggi dalla coda di trasmissione.

Affinché la risoluzione abbia successo:

- Il canale deve essere inattivo
- Il canale deve essere in dubbio
- Il tipo di canale deve essere mittente o server
- È necessario che esista una definizione di canale locale
- Il gestore code locale deve essere in esecuzione

Concetti correlati

"Introduzione agli oggetti" a pagina 78
I canali devono essere definiti e i relativi oggetti associati devono esistere ed essere disponibili per l'utilizzo, prima che un canale possa essere avviato. Questa sezione mostra come.

"Funzione di controllo canale" a pagina 54
La funzione di controllo del canale consente di definire, monitorare e controllare i canali.

"Connessione di applicazioni mediante l'accodamento distribuito" a pagina 28
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra le installazioni WebSphere MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

Riferimenti correlati

Risoluzione canale

Impostazione della comunicazione per Windows

Quando un canale di gestione dell'accodamento distribuito viene avviato, tenta di utilizzare la connessione specificata nella definizione del canale. Perché ciò abbia esito positivo, è necessario che la connessione sia definita e disponibile. Questa sezione spiega come eseguire questa operazione utilizzando una delle quattro forme di comunicazione per sistemi WebSphere MQ per sistemi Windows .

Potrebbe essere utile fare riferimento a Configurazione di esempio - IBM WebSphere MQ per Windows.

Per i sistemi UNIX and Linux , consultare “Impostazione della comunicazione sui sistemi UNIX and Linux” a pagina 94.

Scelta di una connessione

Scegliere tra le seguenti quattro forme di comunicazione per WebSphere MQ per sistemi Windows :

- “Definizione di un collegamento TCP su Windows” a pagina 85
- “Definizione di un collegamento LU 6.2 su Windows” a pagina 87
- “Definizione di una connessione NetBIOS su Windows” a pagina 89
- “Definizione di un collegamento SPX su Windows” a pagina 91 (solo Windows XP e Windows 2003 Server)

Ogni definizione di canale deve specificare solo un protocollo come attributo del protocollo di trasmissione (tipo di trasporto). Uno o più protocolli possono essere utilizzati da un gestore code.

Per i client WebSphere MQ , potrebbe essere utile disporre di canali alternativi che utilizzano protocolli di trasmissione differenti. Per ulteriori informazioni sui client WebSphere MQ , consultare Panoramica dei client.

Concetti correlati

“Connessione di applicazioni mediante l'accodamento distribuito” a pagina 28
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra le installazioni WebSphere MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

“Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 74
Per DQM è necessario creare, monitorare e controllare i canali per i gestori code remoti. È possibile controllare i canali utilizzando comandi, programmi, IBM WebSphere MQ Explorer, file per le definizioni dei canali e un'area di memoria per le informazioni di sincronizzazione.

“Configurazione delle connessioni tra client e server” a pagina 100
Per configurare i collegamenti di comunicazione tra WebSphere MQ i client e i server MQI, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del collegamento, avviare un listener e definire canali.

Definizione di un collegamento TCP su Windows

Definire una connessione TCP configurando un canale all'estremità di invio per specificare l'indirizzo della destinazione ed eseguendo un programma listener all'estremità di ricezione.

Fine invio

Specificare il nome host o l'indirizzo TCP della macchina di destinazione nel campo Nome connessione della definizione di canale.

La porta su cui connettersi è il valore predefinito 1414. Il numero di porta 1414 è assegnato da Internet Assigned Numbers Authority a IBM WebSphere MQ.

Per utilizzare un numero di porta diverso da quello predefinito, specificarlo nel campo del nome della connessione della definizione dell'oggetto canale:

```
DEFINE CHANNEL('channel name') CHLTYPE(SDR) +
          TRPTYPE(TCP) +
          CONNAME('OS2ROG3(1822)') +
          XMITQ('XMitQ name') +
          REPLACE
```

dove 0S2R0G3 è il nome DNS del gestore code remoto e 1822 è la porta richiesta. (deve essere la porta su cui è in ascolto il listener all'estremità di ricezione).

Un canale in esecuzione deve essere arrestato e riavviato per acquisire qualsiasi modifica alla definizione dell'oggetto del canale.

È possibile modificare il numero di porta predefinito specificandolo nel file `.ini` per IBM WebSphere MQ per Windows:

```
TCP:
Port=1822
```

Nota: Per selezionare quale numero di porta TCP/IP utilizzare, IBM WebSphere MQ utilizza il primo numero di porta che trova nella seguente sequenza:

1. Il numero di porta specificato esplicitamente nella definizione del canale o nella riga comandi. Questo numero consente la sovrascrittura del numero di porta predefinito per un canale.
2. L'attributo port specificato nella stanza TCP del file `.ini` . Questo numero consente al numero di porta predefinito di essere sovrascritto per un gestore code.
3. Il valore predefinito è 1414. Questo è il numero assegnato a IBM WebSphere MQ da Internet Assigned Numbers Authority per le connessioni in entrata e in uscita.

Per ulteriori informazioni sui valori impostati utilizzando qm.ini, consultare Stanza del file di configurazione per l'accodamento distribuito.

Ricezione su TCP

Per avviare un programma del canale ricevente, è necessario avviare un programma listener per rilevare le richieste di rete in entrata e avviare il canale associato. È possibile utilizzare il listener IBM WebSphere MQ .

I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente.

Per avviare un programma del canale ricevente, è necessario avviare un programma listener per rilevare le richieste di rete in entrata e avviare il canale associato. È possibile utilizzare il listener IBM WebSphere MQ .

Per eseguire il listener fornito con IBM WebSphere MQ, che avvia nuovi canali come thread, utilizzare il comando runmqlsr .

Un esempio di base dell'utilizzo del comando **runmqlsr** :

```
runmqlsr -t tcp [-m QMNAME] [-p 1822]
```

Le parentesi quadre indicano parametri facoltativi; QMNAME non è richiesto per il gestore code predefinito e il numero di porta non è richiesto se si utilizza il valore predefinito (1414). Il numero di porta non deve essere superiore a 65535.

Nota: Per selezionare quale numero di porta TCP/IP utilizzare, IBM WebSphere MQ utilizza il primo numero di porta che trova nella seguente sequenza:

1. Il numero di porta specificato esplicitamente nella definizione del canale o nella riga comandi. Questo numero consente la sovrascrittura del numero di porta predefinito per un canale.
2. L'attributo port specificato nella stanza TCP del file `.ini` . Questo numero consente al numero di porta predefinito di essere sovrascritto per un gestore code.
3. Il valore predefinito è 1414. Questo è il numero assegnato a IBM WebSphere MQ da Internet Assigned Numbers Authority per le connessioni in entrata e in uscita.

Per prestazioni ottimali, eseguire il listener IBM WebSphere MQ come un'applicazione attendibile come descritto in “Esecuzione di canali e listener come applicazioni attendibili” a pagina 74. Per informazioni sulle applicazioni attendibili, consultare Limitazioni per le applicazioni attendibili

Utilizzo dell'opzione TCP/IP SO_KEEPALIVE

Se si desidera utilizzare l'opzione Windows SO_KEEPALIVE, è necessario aggiungere la seguente voce al registro:

```
TCP:
KeepAlive=yes
```

Per ulteriori informazioni sull'opzione SO_KEEPALIVE, consultare "Verifica che l'altra estremità del canale sia ancora disponibile" a pagina 62.

Su Windows, il valore di registro `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` per l'opzione Windows KeepAliveTime controlla l'intervallo che trascorre prima che la connessione venga controllata. Il valore predefinito è due ore.

Definizione di un collegamento LU 6.2 su Windows

SNA deve essere configurato in modo che sia possibile stabilire una conversazione LU 6.2 tra le macchine.

Una volta configurato SNA, procedere nel modo seguente.

Consultare la seguente tabella per informazioni.

Tabella 9. Impostazioni sul sistema Windows locale per una piattaforma del gestore code remoto

Piattaforma remota	**TPNAME**	**TPPATH**
z/OS o MVS/ESA senza CICS	Le stesse informazioni del lato corrispondente sul gestore code remoto.	-
z/OS o MVS / ESA utilizzando CICS	CKRC (mittente) CKSV (richiedente) CKRC (server)	-
IBM i	Uguale al valore di confronto nella specifica di instradamento sul sistema IBM i .	-
Sistemi UNIX and Linux	Le stesse informazioni del lato corrispondente sul gestore code remoto.	*MQ_INSTALLATION_PATH*/bin/amqcrs6a
Windows	Come specificato nel comando Windows Run Listener o nel programma di transazione richiamabile definito utilizzando TpSetup su Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

MQ_INSTALLATION_PATH rappresenta la directory di alto livello in cui è installato WebSphere MQ .

Se si dispone di più di un gestore code sulla stessa macchina, verificare che i nomi TP nelle definizioni di canale siano univoci.

Per le informazioni più recenti sulla configurazione di AnyNet SNA su TCP/IP, consultare la seguente documentazione in linea IBM : AnyNet SNA su TCP/IP e SNA Node Operations.

Concetti correlati

"Fine invio su LU 6.2" a pagina 88
Creare un oggetto lato CPI-C (destinazione simbolica) dall'applicazione di gestione del prodotto LU 6.2 che si sta utilizzando. Immettere questo nome nel campo Nome connessione nella definizione di canale. Creare anche un collegamento LU 6.2 al partner.

"Ricezione su LU 6.2" a pagina 88
I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente.

Fine invio su LU 6.2
Creare un oggetto lato CPI-C (destinazione simbolica) dall'applicazione di gestione del prodotto LU 6.2 che si sta utilizzando. Immettere questo nome nel campo Nome connessione nella definizione di canale. Creare anche un collegamento LU 6.2 al partner.

Nell'oggetto lato CPI-C, immettere il nome LU partner sulla macchina ricevente, il nome TP e il nome modo. Ad esempio:

```
Partner LU Name              OS2ROG2
Partner TP Name              recv
Mode Name                    #INTER
```

Ricezione su LU 6.2
I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente.

Per avviare un programma del canale di ricezione, è necessario avviare un programma listener per rilevare le richieste di rete in entrata e avviare il canale associato. Si avvia questo programma listener con il comando RUNMQLSR, fornendo il TpName su cui eseguire l'ascolto. In alternativa, è possibile utilizzare TpStart in SNA Server per Windows.

Utilizzo del comando RUNMQLSR

Esempio del comando per avviare il listener:

```
RUNMQLSR -t LU62 -n RECV [-m QMNAME]
```

dove RECV è il TpName specificato all'altra estremità (invio) come "TpName da avviare sul lato remoto". L'ultima parte tra parentesi quadre è facoltativa e non è richiesta per il gestore code predefinito.

È possibile avere più di un gestore code in esecuzione su una macchina. È necessario assegnare un TpName differente a ogni gestore code, quindi avviare un programma listener per ogni gestore code. Ad esempio:

```
RUNMQLSR -t LU62 -m QM1 -n TpName1
RUNMQLSR -t LU62 -m QM2 -n TpName2
```

Per prestazioni ottimali, eseguire il listener WebSphere MQ come un'applicazione attendibile, come descritto in Esecuzione di canali e listener come applicazioni attendibili. Consultare Limitazioni per le applicazioni attendibili per informazioni sulle applicazioni attendibili.

È possibile arrestare tutti i listener WebSphere MQ in esecuzione su un gestore code inattivo, utilizzando il comando:

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

Utilizzo di Microsoft SNA Server su Windows

È possibile utilizzare TpSetup (da SNA Server SDK) per definire un TP richiamabile che poi guida amqcrs6a.exe, oppure è possibile impostare manualmente diversi valori di registro. I parametri che devono essere passati a amqcrs6a.exe sono:

```
   -m QM -n TpName
```

dove *QM* è il nome del gestore code e *TpName* è il nome TP. Per ulteriori informazioni, consultare il manuale *Microsoft SNA Server APPC Programmers Guide* o il manuale *Microsoft SNA Server CPI-C Programmers Guide* .

Se non si specifica un nome gestore code, viene utilizzato il gestore code predefinito.

Definizione di una connessione NetBIOS su Windows

WebSphere MQ utilizza tre tipi di risorsa NetBIOS quando si stabilisce una connessione NetBIOS a un altro prodotto WebSphere MQ : sessioni, comandi e nomi. Ciascuna di queste risorse ha un limite, che viene stabilito per impostazione predefinita o per scelta durante l'installazione di NetBIOS.

Ogni canale in esecuzione, indipendentemente dal tipo, utilizza una sessione NetBIOS e un comando NetBIOS . L'implementazione IBM NetBIOS consente a più processi di utilizzare lo stesso nome NetBIOS locale. Pertanto, è necessario che solo un nome NetBIOS sia disponibile per l'utilizzo da parte di WebSphere MQ. Le implementazioni di altri fornitori, ad esempio l'emulazione NetBIOS di Novell, richiedono un nome locale differente per processo. Verificare i requisiti dalla documentazione per il prodotto NetBIOS che si sta utilizzando.

In tutti i casi, assicurarsi che siano già disponibili risorse sufficienti di ciascun tipo o aumentare i valori massimi specificati nella configurazione. Qualsiasi modifica ai valori richiede un riavvio del sistema.

Durante l'avvio del sistema, il driver di periferica NetBIOS visualizza il numero di sessioni, comandi e nomi disponibili per l'utilizzo da parte delle applicazioni. Queste risorse sono disponibili per tutte le applicazioni basate sul NetBIOSin esecuzione sullo stesso sistema. Pertanto, è possibile che altre applicazioni utilizzino queste risorse prima che WebSphere MQ le acquisisca. L'amministratore della rete LAN dovrebbe essere in grado di chiarire questo.

Concetti correlati

“Definizione del nome IBM WebSphere MQ locale NetBIOS” a pagina 89
Il nome NetBIOS locale utilizzato dai processi del canale IBM WebSphere MQ può essere specificato in tre modi.

“Definizione dei limiti di nome, comando e sessione NetBIOS del gestore code” a pagina 90
I limiti del gestore code per sessioni, comandi e nomi NetBIOS possono essere specificati in due modi.

“Stabilire il numero dell'adattatore LAN” a pagina 90
Affinché i canali funzionino correttamente su NetBIOS, è necessario che il supporto dell'adattatore a ciascuna estremità sia compatibile. IBM WebSphere MQ consente di controllare il numero dell'adattatore LAN (LANA) utilizzando il valore AdapterNum nella stanza NETBIOS del file qm.ini e specificando il parametro `-a` sul comando runmqlsr.

“Avvio della connessione NetBIOS” a pagina 91
Definizione delle fasi necessarie per avviare una connessione.

“Listener di destinazione per la connessione NetBIOS” a pagina 91
Definizione delle operazioni da eseguire all'estremità ricevente della connessione NetBIOS .

Definizione del nome IBM WebSphere MQ locale NetBIOS

Il nome NetBIOS locale utilizzato dai processi del canale IBM WebSphere MQ può essere specificato in tre modi.

In ordine di precedenza, i tre modi sono:

1. Il valore specificato nel parametro `-l` del comando RUNMQLSR, ad esempio:

   ```
   RUNMQLSR -t NETBIOS -l my_station
   ```

2. La variabile di ambiente MQNAME con un valore stabilito dal comando:

   ```
   SET MQNAME=my_station
   ```

   È possibile impostare il valore MQNAME per ogni processo. In alternativa, è possibile impostarlo a livello di sistema nel registro Windows .

   Se si utilizza un'implementazione NetBIOS che richiede nomi univoci, è necessario emettere un comando SET MQNAME in ogni finestra in cui viene avviato un processo IBM WebSphere MQ . Il valore MQNAME è arbitrario ma deve essere univoco per ogni processo.

3. La stanza NETBIOS nel file di configurazione del gestore code qm.ini. Ad esempio:

```
NETBIOS:

  LocalName=my_station
```

Nota:

1. a causa delle variazioni nell'implementazione dei prodotti NetBIOS supportati, si consiglia di rendere ciascun nome NetBIOS univoco nella rete. In caso contrario, potrebbero verificarsi risultati imprevedibili. Se si riscontrano problemi nello stabilire un canale NetBIOS e nel log degli errori del gestore code sono presenti messaggi di errore che mostrano un codice di ritorno NetBIOS di X'15 ', rivedere l'utilizzo dei nomi NetBIOS .
2. Su Windows, non è possibile utilizzare il nome della macchina come nome NetBIOS perché Windows lo utilizza già.
3. L'avvio del canale mittente richiede che venga specificato un nome NetBIOS utilizzando la variabile di ambiente MQNAME o il LocalName nel file qm.ini .

Definizione dei limiti di nome, comando e sessione NetBIOS del gestore code
I limiti del gestore code per sessioni, comandi e nomi NetBIOS possono essere specificati in due modi.

In ordine di precedenza, questi modi sono:

1. I valori specificati nel comando RUNMQLSR:

   ```
   -s  Sessions
   -e  Names
   -o  Commands
   ```

   Se l'operando -m non viene specificato nel comando, i valori si applicano solo al gestore code predefinito.
2. La stanza NETBIOS nel file di configurazione del gestore code qm.ini. Ad esempio:

   ```
   NETBIOS:

     NumSess=Qmgr_max_sess
     NumCmds=Qmgr_max_cmds
     NumNames=Qmgr_max_names
   ```

Stabilire il numero dell'adattatore LAN
Affinché i canali funzionino correttamente su NetBIOS, è necessario che il supporto dell'adattatore a ciascuna estremità sia compatibile. IBM WebSphere MQ consente di controllare il numero dell'adattatore LAN (LANA) utilizzando il valore AdapterNum nella stanza NETBIOS del file qm.ini e specificando il parametro -a sul comando runmqlsr.

Il numero dell'adattatore LAN predefinito utilizzato da IBM WebSphere MQ per connessioni NetBIOS è 0. Verificare il numero utilizzato sul sistema nel modo seguente:

Su Windows, non è possibile interrogare il numero dell'adattatore LAN direttamente tramite il sistema operativo. Utilizzare invece LANACFG.EXE , disponibile da Microsoft. L'output dello strumento visualizza i numeri dell'adattatore LAN virtuale e i relativi collegamenti effettivi. Per ulteriori informazioni sui numeri degli adattatori LAN, consultare Microsoft Knowledge Base article 138037 *HOWTO: Use LANA Numbers in a 32 - bit Environment*.

Specificare il valore corretto per la stanza NETBIOS del file di configurazione del gestore code, qm.ini:

```
NETBIOS:
  AdapterNum=n
```

dove n è il numero dell'adattatore LAN corretto per questo sistema.

Avvio della connessione NetBIOS
Definizione delle fasi necessarie per avviare una connessione.

Per avviare la connessione, attenersi alla seguente procedura all'estremità di invio:

1. Definire il nome della stazione NetBIOS utilizzando il valore MQNAME o LocalName .
2. Verificare il numero dell'adattatore LAN utilizzato sul sistema e specificare il file corretto utilizzando AdapterNum.
3. Nel campo ConnectionName della definizione di canale, specificare il nome NetBIOS utilizzato dal programma listener di destinazione. In Windows, i canali NetBIOS ***devono*** essere eseguiti come thread. Eseguire questa operazione specificando MCATYPE (THREAD) nella definizione del canale.

```
DEFINE CHANNEL (chname) CHLTYPE(SDR) +
       TRPTYPE(NETBIOS) +
       CONNAME(your_station) +
       XMITQ(xmitq) +
       MCATYPE(THREAD) +
       REPLACE
```

Listener di destinazione per la connessione NetBIOS
Definizione delle operazioni da eseguire all'estremità ricevente della connessione NetBIOS .

All'estremità di ricezione, seguire queste istruzioni:

1. Definire il nome della stazione NetBIOS utilizzando il valore MQNAME o LocalName .
2. Verificare il numero dell'adattatore LAN utilizzato sul sistema e specificare il file corretto utilizzando AdapterNum.
3. Definire il canale ricevente:

```
DEFINE CHANNEL (chname) CHLTYPE(RCVR) +
       TRPTYPE(NETBIOS) +
       REPLACE
```

4. Avviare il programma listener WebSphere MQ per stabilire la stazione e rendere possibile contattarla. Ad esempio:

```
RUNMQLSR -t NETBIOS -l your_station [-m qmgr]
```

   Questo comando stabilisce `your_station` come una stazione NetBIOS in attesa di essere contattata. Il nome della stazione NetBIOS deve essere univoco nella rete NetBIOS .

Per prestazioni ottimali, eseguire il listener WebSphere MQ come un'applicazione attendibile come descritto in “Esecuzione di canali e listener come applicazioni attendibili” a pagina 74. Consultare Limitazioni per le applicazioni attendibili per informazioni sulle applicazioni attendibili.

È possibile arrestare tutti i listener WebSphere MQ in esecuzione su un gestore code inattivo, utilizzando il comando:

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

Se non si specifica un nome gestore code, viene utilizzato il gestore code predefinito.

Definizione di un collegamento SPX su Windows
Una connessione SPX si applica solo a client e server che eseguono Windows XP e Windows 2003 Server.

La definizione del canale all'estremità di invio specifica l'indirizzo della destinazione. Un programma listener deve essere eseguito all'estremità di ricezione.

Concetti correlati
“Fine invio su SPX” a pagina 92

Se la macchina di destinazione è remota, specificare l'indirizzo SPX della macchina di destinazione nel campo Nome connessione della definizione di canale.

“Ricezione su SPX” a pagina 92
I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente.

“Parametri IPX/SPX” a pagina 94
Nella maggior parte dei casi, le impostazioni predefinite per i parametri IPX/SPX si adattano alle proprie esigenze. Tuttavia, potrebbe essere necessario modificarne alcune nel proprio ambiente per ottimizzarne l'utilizzo per WebSphere MQ.

Fine invio su SPX
Se la macchina di destinazione è remota, specificare l'indirizzo SPX della macchina di destinazione nel campo Nome connessione della definizione di canale.

L'indirizzo SPX viene specificato nel formato seguente:

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

dove:

network
Indica l'indirizzo di rete a 4 byte della rete su cui si trova la macchina remota,

node
Indica l'indirizzo del nodo a 6 byte, che è l'indirizzo LAN dell'adattatore LAN nella macchina remota

socket
Indica il numero di socket a 2 byte su cui è in ascolto la macchina remota.

Se le macchine locali e remote si trovano sulla stessa rete, non è necessario specificare l'indirizzo di rete. Se l'estremità remota è in ascolto sul socket predefinito (5E86), non è necessario specificare il socket.

Un esempio di un indirizzo SPX completamente specificato specificato nel parametro CONNAME di un comando MQSC è:

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

Nel caso predefinito, in cui le macchine si trovano entrambe sulla stessa rete, questo diventa:

```
CONNAME(08005A7161E5)
```

Il numero socket predefinito può essere modificato specificandolo nel file di configurazione del gestore code (qm.ini):

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

Per ulteriori informazioni sui valori impostati utilizzando qm.ini, consultare Stanza del file di configurazione per l'accodamento distribuito .

Ricezione su SPX
I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente.

Per avviare un programma del canale ricevente, è necessario avviare un programma listener per rilevare le richieste di rete in entrata e avviare il canale associato.

Utilizzare il listener WebSphere MQ .

Utilizzo dell'opzione di backlog del listener SPX

Quando si riceve su SPX, viene impostato un numero massimo di richieste di connessione in sospeso. Può essere considerato un *backlog* di richieste in attesa sulla porta SPX affinché il listener accetti la richiesta. I valori di backlog del listener predefiniti vengono mostrati in Tabella 10 a pagina 93.

Tabella 10. Richieste di connessione in sospeso predefinite su Windows

Piattaforma	**Valore backlog listener predefinito**
Server Windows	5
Workstation Windows	5

Se il backlog raggiunge i valori in Tabella 10 a pagina 93, il codice motivo, MQRC_Q_MGR_NOT_AVAILABLE viene ricevuto durante il tentativo di connessione al gestore code utilizzando MQCONN o MQCONNX. Se ciò accade, è possibile provare a connettersi di nuovo.

Tuttavia, per evitare questo errore, è possibile aggiungere una voce nel file qm.ini o nel registro per Windows:

```
SPX:
ListenerBacklog = n
```

Questo sovrascrive il numero massimo predefinito di richieste in sospeso (consultare Tabella 10 a pagina 93) per il listener SPX.

Nota: Alcuni sistemi operativi supportano un valore maggiore di quello predefinito. Se necessario, questo può essere utilizzato per evitare di raggiungere il limite di connessione.

Per eseguire il listener con l'opzione `backlog` attivata:

- Utilizzare il comando RUNMQLSR -b oppure
- Utilizzare il comando MQSC **DEFINE LISTENER** con l'attributo BACKLOG impostato sul valore richiesto.

Per informazioni sul comando **RUNMQLSR** , consultare runmqlsr. Per informazioni sul comando DEFINE LISTENER, consultare DEFINE LISTENER.

Utilizzo del listener WebSphere MQ

Per eseguire il Listener fornito con WebSphere MQ, che avvia nuovi canali come thread, utilizzare il comando RUNMQLSR. Ad esempio:

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

Le parentesi quadre indicano parametri facoltativi; QMNAME non è richiesto per il gestore code predefinito e il numero socket non è richiesto se si utilizza il valore predefinito (5E86).

Per prestazioni ottimali, eseguire il listener WebSphere MQ come un'applicazione attendibile come descritto in “Esecuzione di canali e listener come applicazioni attendibili” a pagina 74. Consultare Limitazioni per le applicazioni attendibili per ulteriori informazioni sulle applicazioni attendibili.

È possibile arrestare tutti i listener WebSphere MQ in esecuzione su un gestore code inattivo, utilizzando il comando:

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

Se non si specifica un nome gestore code, viene utilizzato il gestore code predefinito.

Parametri IPX/SPX
Nella maggior parte dei casi, le impostazioni predefinite per i parametri IPX/SPX si adattano alle proprie esigenze. Tuttavia, potrebbe essere necessario modificarne alcune nel proprio ambiente per ottimizzarne l'utilizzo per WebSphere MQ.

I parametri effettivi e il metodo di modificarli variano a seconda della piattaforma e del fornitore del supporto per le comunicazioni SPX. La sezione di esempio descrive alcuni di questi parametri, in particolare quelli che potrebbero influenzare il funzionamento dei canali WebSphere MQ e delle connessioni client.

Sistemi Windows

Fare riferimento alla documentazione Microsoft per dettagli completi sull'utilizzo e l'impostazione dei parametri NWLink IPX e SPX. I parametri IPX/SPX si trovano nei seguenti percorsi nel registro:

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

Impostazione della comunicazione sui sistemi UNIX and Linux

DQM è una funzione di accodamento remoto per IBM WebSphere MQ. Fornisce programmi di controllo del canale per il gestore code che formano l'interfaccia per i collegamenti di comunicazione, controllabili dall'operatore di sistema. Le definizioni di canale gestite dalla gestione delle code distribuite utilizzano queste connessioni.

Quando un canale di gestione dell'accodamento distribuito viene avviato, tenta di utilizzare la connessione specificata nella definizione del canale. Per avere esito positivo, è necessario che la connessione sia definita e disponibile. Questa sezione spiega come eseguire questa operazione. Potrebbe anche essere utile fare riferimento alle seguenti sezioni:

- Configurazione di esempio - IBM WebSphere MQ for AIX
- Configurazione di esempio - IBM WebSphere MQ for HP-UX
- Esempio di configurazione - IBM WebSphere MQ for Solaris
- Configurazione di esempio - IBM WebSphere MQ per Linux

Per Windows, consultare “Impostazione della comunicazione per Windows” a pagina 84.

È possibile scegliere tra due forme di comunicazione per WebSphere MQ su sistemi UNIX and Linux :

- “Definizione di un collegamento TCP su UNIX and Linux” a pagina 95
- “Definizione di una connessione LU 6.2 su UNIX and Linux” a pagina 98

Ciascuna definizione di canale deve specificarne una solo come attributo del Protocollo di trasmissione (Tipo di trasporto). Uno o più protocolli possono essere utilizzati da un gestore code.

Per i client IBM WebSphere MQ Explorer MQI, potrebbe essere utile disporre di canali alternativi che utilizzano protocolli di trasmissione differenti. Per ulteriori informazioni sui client IBM WebSphere MQ Explorer MQI, consultare Panoramica sui client IBM WebSphere MQ MQI .

Concetti correlati

“Connessione di applicazioni mediante l'accodamento distribuito” a pagina 28
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra le installazioni WebSphere MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

“Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 74
Per DQM è necessario creare, monitorare e controllare i canali per i gestori code remoti. È possibile controllare i canali utilizzando comandi, programmi, IBM WebSphere MQ Explorer, file per le definizioni dei canali e un'area di memoria per le informazioni di sincronizzazione.

“Configurazione delle connessioni tra client e server” a pagina 100

Per configurare i collegamenti di comunicazione tra WebSphere MQ i client e i server MQI, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del collegamento, avviare un listener e definire canali.

Definizione di un collegamento TCP su UNIX and Linux

La definizione del canale all'estremità di invio specifica l'indirizzo della destinazione. Il listener o il daemon inet è configurato per la connessione all'estremità di ricezione.

Fine invio

Specificare il nome host o l'indirizzo TCP della macchina di destinazione nel campo Nome connessione della definizione di canale. La porta su cui connettersi è il valore predefinito 1414. Il numero di porta 1414 viene assegnato da Internet Assigned Numbers Authority a WebSphere MQ.

Per utilizzare un numero di porta diverso da quello predefinito, modificare il campo del nome della connessione come segue:

```
Connection Name REMHOST(1822)
```

dove REMHOST è il nome host della macchina remota e 1822 è il numero di porta richiesto. (deve essere la porta su cui è in ascolto il listener all'estremità di ricezione).

In alternativa, è possibile modificare il numero di porta specificandolo nel file di configurazione del gestore code (qm.ini):

```
TCP:
  Port=1822
```

Per ulteriori informazioni sui valori impostati utilizzando qm.ini, consultare Stanza del file di configurazione per l'accodamento distribuito.

Ricezione su TCP

È possibile utilizzare il listener TCP/IP, che è il daemon inet (inetd), o il listener WebSphere MQ .

Alcune distribuzioni Linux ora utilizzano il daemon inet esteso (xinetd) invece del daemon inet. Per informazioni su come utilizzare il daemon inet esteso su un sistema Linux , consultare Stabilire una connessione TCP su Linux.

Concetti correlati

“Utilizzo del listener TCP/IP” a pagina 95
Per avviare i canali su UNIX and Linux, è necessario modificare il file /etc/services e il file inetd.conf

“Utilizzo dell'opzione backlog del listener TCP” a pagina 97
In TCP, le connessioni sono considerate incomplete a meno che non si verifichi un handshake a tre vie tra il server e il client. Queste connessioni vengono chiamate richieste di connessione in sospeso. Viene impostato un valore massimo per queste richieste di connessione in sospeso e può essere considerato un backlog di richieste in attesa sulla porta TCP affinché il listener accetti la richiesta.

“Utilizzo del listener WebSphere MQ” a pagina 97
Per eseguire il listener fornito con WebSphere MQ, che avvia nuovi canali come thread, utilizzare il comando `runmqlsr` .

“Utilizzo dell'opzione TCP/IP SO_KEEPALIVE” a pagina 98
Su alcuni sistemi UNIX and Linux , è possibile definire il tempo di attesa TCP prima di verificare che la connessione sia ancora disponibile e la frequenza con cui tenta nuovamente la connessione se il primo controllo ha esito negativo. Questo è un parametro ottimizzabile del kernel o può essere immesso sulla riga comandi.

Utilizzo del listener TCP/IP

Per avviare i canali su UNIX and Linux, è necessario modificare il file /etc/services e il file inetd.conf

Seguire queste istruzioni:

1. Modificare il file /etc/services :

   Nota: Per modificare il file /etc/services , è necessario essere collegati come superuser o root. È possibile modificarlo, ma deve corrispondere al numero di porta specificato all'estremità di invio.

   Aggiungere la seguente riga al file:

   ```
   MQSeries 1414/tcp
   ```

   dove 1414 è il numero di porta richiesto da WebSphere MQ. Il numero di porta non deve essere superiore a 65535.
2. Aggiungere una riga nel file inetd.conf per richiamare il programma amqcrsta, dove *MQ_INSTALLATION_PATH* rappresenta la directory di alto livello in cui è installato WebSphere MQ :

   ```
   MQSeries stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta
   [-m Queue_Man_Name]
   ```

Gli aggiornamenti sono attivi dopo che inetd ha riletto i file di configurazione. Per eseguire questa operazione, immettere i seguenti comandi dall'ID utente root:

- Su AIX:

  ```
  refresh -s inetd
  ```

- Su HP-UX, dall'ID utente mqm:

  ```
  inetd -c
  ```

- Su Solaris 10 o versioni successive:

  ```
  inetconv
  ```

- Su altri sistemi UNIX and Linux (incluso Solaris 9):

  ```
  kill -1 <process number>
  ```

Quando il programma listener avviato da inetd eredita la locale da inetd, è possibile che MQMDE non venga rispettato (unito) e che venga inserito nella coda come dati del messaggio. Per assicurarsi che MQMDE sia rispettato, è necessario impostare correttamente la locale. La locale impostata da inetd potrebbe non corrispondere a quella scelta per altre locali utilizzate dai processi WebSphere MQ . Per impostare la locale:

1. Creare uno script di shell che imposta le variabili di ambiente della locale LANG, LC_COLLATE, LC_CTYPE, LC_MONETARY, LC_NUMERIC, LC_TIME e LC_MESSAGES sulla locale utilizzata per altri processi WebSphere MQ .
2. Nello stesso script di shell, richiamare il programma listener.
3. Modificare il file inetd.conf per richiamare lo script della shell al posto del programma listener.

È possibile avere più di un gestore code sul server. È necessario aggiungere una riga a ciascuno dei due file, per ciascuno dei gestori code. Ad esempio:

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

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

Dove *MQ_INSTALLATION_PATH* rappresenta la directory di alto livello in cui è installato WebSphere MQ .

Ciò evita la generazione di messaggi di errore se esiste una limitazione sul numero di richieste di connessione in sospeso accodate su una singola porta TCP. Per informazioni sul numero di richieste di connessione in sospeso, vedere “Utilizzo dell'opzione backlog del listener TCP” a pagina 97.

Utilizzo dell'opzione backlog del listener TCP
In TCP, le connessioni sono considerate incomplete a meno che non si verifichi un handshake a tre vie tra il server e il client. Queste connessioni vengono chiamate richieste di connessione in sospeso. Viene impostato un valore massimo per queste richieste di connessione in sospeso e può essere considerato un backlog di richieste in attesa sulla porta TCP affinché il listener accetti la richiesta.

I valori di backlog del listener predefiniti vengono visualizzati in Tabella 11 a pagina 97.

Tabella 11. Numero massimo di richieste di connessione in sospeso accodate su una porta TCP/IP

Piattaforma server	**Numero massimo di richieste di connessione**
AIX	100
HP-UX	20
Linux	100
IBM i	255
Solaris	100
Server Windows	100
Workstation Windows	100
z/OS	255

Se il backlog raggiunge i valori riportati in Tabella 11 a pagina 97, la connessione TCP/IP viene rifiutata e il canale non può essere avviato.

Per i canali MCA, ciò fa sì che il canale entri in uno stato RETRY e riprovi la connessione in un secondo momento.

Tuttavia, per evitare questo errore, è possibile aggiungere una voce nel file qm.ini :

```
TCP:
ListenerBacklog = n
```

Sovrascrive il numero massimo predefinito di richieste in sospeso (consultare Tabella 11 a pagina 97) per il listener TCP/IP.

Nota: Alcuni sistemi operativi supportano un valore maggiore di quello predefinito. Se necessario, questo valore può essere utilizzato per evitare di raggiungere il limite di connessione.

Per eseguire il listener con l'opzione `backlog` attivata:

- Utilizzare il comando `runmqlsr -b` oppure
- Utilizzare il comando MQSC **`DEFINE LISTENER`** con l'attributo BACKLOG impostato sul valore richiesto.

Per informazioni sul comando **`runmqlsr`** , consultare runmqlsr. Per informazioni sul comando DEFINE LISTENER, consultare DEFINE LISTENER.

Utilizzo del listener WebSphere MQ
Per eseguire il listener fornito con WebSphere MQ, che avvia nuovi canali come thread, utilizzare il comando `runmqlsr` .

Ad esempio:

```
runmqlsr -t tcp [-m QMNAME] [-p 1822]
```

Le parentesi quadre indicano parametri facoltativi; QMNAME non è richiesto per il gestore code predefinito e il numero di porta non è richiesto se si utilizza il valore predefinito (1414). Il numero di porta non deve essere superiore a 65535.

Per prestazioni ottimali, eseguire il listener WebSphere MQ come un'applicazione attendibile come descritto in “Esecuzione di canali e listener come applicazioni attendibili” a pagina 74. Consultare Limitazioni per le applicazioni attendibili per informazioni sulle applicazioni attendibili.

È possibile arrestare tutti i listener WebSphere MQ in esecuzione su un gestore code inattivo, utilizzando il comando:

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

Se non si specifica un nome gestore code, viene utilizzato il gestore code predefinito.

Utilizzo dell'opzione TCP/IP SO_KEEPALIVE
Su alcuni sistemi UNIX and Linux , è possibile definire il tempo di attesa TCP prima di verificare che la connessione sia ancora disponibile e la frequenza con cui tenta nuovamente la connessione se il primo controllo ha esito negativo. Questo è un parametro ottimizzabile del kernel o può essere immesso sulla riga comandi.

Se si desidera utilizzare l'opzione SO_KEEPALIVE (per ulteriori informazioni, consultare “Verifica che l'altra estremità del canale sia ancora disponibile” a pagina 62), è necessario aggiungere la seguente voce al file di configurazione del gestore code (qm.ini):

```
TCP:
   KeepAlive=yes
```

Consultare la documentazione per il sistema UNIX and Linux per ulteriori informazioni.

Definizione di una connessione LU 6.2 su UNIX and Linux

SNA deve essere configurato in modo che sia possibile stabilire una conversazione LU 6.2 tra le macchine.

Per le informazioni più recenti sulla configurazione di SNA su TCP/IP, consultare la seguente documentazione in linea IBM : Communications Server.

SNA deve essere configurato in modo che sia possibile stabilire una conversazione LU 6.2 tra i sistemi.

Per informazioni, consultare il manuale *Multiplatform APPC Configuration Guide* e la seguente tabella.

Tabella 12. Impostazioni sul sistema UNIX and Linux locale per una piattaforma del gestore code remoto

Piattaforma remota	**TPNAME**	**TPPATH**
z/OS senza CICS	Lo stesso del TPName corrispondente nelle informazioni laterali sul gestore code remoto.	-
z/OS utilizzo di CICS	CKRC (mittente) CKSV (richiedente) CKRC (server)	-
IBM i	Uguale al valore di confronto nella specifica di instradamento sul sistema IBM i .	-
Sistemi UNIX and Linux	Lo stesso del TPName corrispondente nelle informazioni laterali sul gestore code remoto.	*MQ_INSTALLATION_PATH*/bin/amqcrs6a

Tabella 12. Impostazioni sul sistema UNIX and Linux locale per una piattaforma del gestore code remoto (Continua)

Piattaforma remota	**TPNAME**	**TPPATH**
Finestre	Come specificato nel comando Windows Run Listener o nel programma di transazione richiamabile definito utilizzando TpSetup su Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

MQ_INSTALLATION_PATH rappresenta la directory di alto livello in cui è installato WebSphere MQ .

Se si dispone di più di un gestore code sulla stessa macchina, verificare che i nomi TP nelle definizioni di canale siano univoci.

Concetti correlati

"Fine invio" a pagina 99
Su sistemi UNIX and Linux , creare un oggetto lato CPI-C (destinazione simbolica) e immettere questo nome nel campo Nome connessione nella definizione del canale. Creare anche un collegamento LU 6.2 al partner.

"Ricezione su LU 6.2" a pagina 99
Sui sistemi UNIX and Linux , creare un collegamento di ascolto all'estremità ricevente, un profilo di connessione logica LU 6.2 e un profilo TPN.

Fine invio

Su sistemi UNIX and Linux , creare un oggetto lato CPI-C (destinazione simbolica) e immettere questo nome nel campo Nome connessione nella definizione del canale. Creare anche un collegamento LU 6.2 al partner.

Nell'oggetto lato CPI-C, immettere il nome LU partner sulla macchina ricevente, il nome del programma di transazione e il nome del modo. Ad esempio:

```
Partner LU Name              REMHOST
Remote TP Name               recv
Service Transaction Program  no
Mode Name                    #INTER
```

Su HP-UX, utilizzare la variabile di ambiente APPCLLU per denominare la LU locale che il mittente deve utilizzare. Su Solaris, impostare la variabile di ambiente APPC_LOCAL_LU come nome LU locale.

Viene utilizzato SECURITY PROGRAM, dove supportato da CPI-C, quando WebSphere MQ tenta di stabilire una sessione SNA.

Ricezione su LU 6.2

Sui sistemi UNIX and Linux , creare un collegamento di ascolto all'estremità ricevente, un profilo di connessione logica LU 6.2 e un profilo TPN.

Nel profilo TPN, immettere il percorso completo del file eseguibile e il nome del programma di transazione:

```
Full path to TPN executable   MQ_INSTALLATION_PATH/bin/amqcrs6a
Transaction Program name      recv
User ID                       0
```

MQ_INSTALLATION_PATH rappresenta la directory di alto livello in cui è installato WebSphere MQ .

Sui sistemi in cui è possibile impostare l'ID utente, specificare un utente che sia un membro del gruppo mqm. Su AIX, Solaris e HP-UX, impostare le variabili di ambiente APPCTPN (nome transazione) e APPCLLU (nome LU locale) (è possibile utilizzare i pannelli di configurazione per il programma di transazione richiamato).

Potrebbe essere necessario utilizzare un gestore code diverso da quello predefinito. In tal caso, definire un file di comandi che richiama:

```
amqcrs6a -m Queue_Man_Name
```

quindi richiamare il file di comandi.

Configurazione delle connessioni tra client e server

Per configurare i collegamenti di comunicazione tra WebSphere MQ i client e i server MQI, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del collegamento, avviare un listener e definire canali.

In WebSphere MQ, i collegamenti di comunicazioni logiche tra gli oggetti sono denominati *canali*. I canali utilizzati per connettere WebSphere MQ i client MQI ai server sono denominati canali MQI. Si configurano le definizioni di canale a ciascuna estremità del link in modo che l'applicazione WebSphere MQ sul client WebSphere MQ MQI possa comunicare con il gestore code sul server. Per una descrizione dettagliata di come eseguire questa operazione, vedere Canali definiti dall'utente.

Prima di definire i canali MQI, è necessario:

1. Decidi la forma di comunicazione che stai per utilizzare. Vedere “Il tipo di comunicazione da utilizzare” a pagina 100.
2. Definire la connessione ad ogni estremità del canale:

   Per definire la connessione, è necessario:

   - Configurare la connessione.
   - Registrare i valori dei parametri necessari per le definizioni di canali.
   - Abilitare il server per rilevare le richieste di rete in entrata dal client WebSphere MQ MQI, avviando un *listener*.

Il tipo di comunicazione da utilizzare

Piattaforme differenti supportano protocolli di trasmissione differenti. La scelta del protocollo di trasmissione dipende dalla propria combinazione di piattaforme client e server WebSphere MQ .

Esistono fino a quattro tipi di protocollo di trasmissione per i canali MQI a seconda delle piattaforme client e server:

- LU 6.2
- NetBIOS
- SPX
- TCP/IP

Quando si definiscono i canali MQI, ciascuna definizione di canale deve specificare un attributo del protocollo di trasmissione (tipo di trasporto). Un server non è limitato a un solo protocollo, quindi diverse definizioni di canale possono specificare protocolli differenti. Per i client WebSphere MQ MQI, potrebbe essere utile disporre di canali MQI alternativi che utilizzano protocolli di trasmissione differenti.

La scelta del protocollo di trasmissione potrebbe essere limitata dalla particolare combinazione di piattaforme client e server WebSphere MQ . Le combinazioni possibili sono mostrate nella seguente tabella.

Tabella 13. Protocolli di trasmissione - combinazione di piattaforme client e server WebSphere MQ MQI		
Protocollo di trasmissione	**Client WebSphere MQ MQI**	**WebSphere MQ Server**
TCP/IP	Sistemi UNIX Windows	Sistemi UNIX Windows z/OS
LU 6.2	Sistemi UNIX[1] Windows	Sistemi UNIX[1] Windows
NetBIOS	Windows	Windows
SPX	Windows	Windows
Nota: 1. Ad eccezione di Linux per Power Systems		

Per ulteriori informazioni sull'impostazione di diversi tipi di connessioni, consultare i seguenti link:

- “Definizione di un collegamento TCP su Windows” a pagina 85
- “Definizione di un collegamento TCP su UNIX and Linux” a pagina 95
- “Limiti di connessione TCP/IP” a pagina 103
- “Definizione di un collegamento LU 6.2 su Windows” a pagina 87
- “Definizione di una connessione LU 6.2 su UNIX and Linux” a pagina 98
- “Definizione di una connessione NetBIOS su Windows” a pagina 89
- “Definizione di un collegamento SPX su Windows” a pagina 91

Concetti correlati

“Configurazione di un client transazionale esteso” a pagina 104
Questa raccolta di argomenti descrive come configurare la funzione transazionale estesa per ogni categoria di gestore transazioni.

“Definizione di canali MQI” a pagina 113
Per creare un nuovo canale, devi creare **due** definizioni di canale, una per ogni estremità della connessione, utilizzando lo stesso nome di canale e tipi di canale compatibili. In questo caso, i tipi di canali sono *connessione server* e *connessione client*.

“Creazione di definizioni di connessione server e di connessione client su piattaforme differenti” a pagina 115
È possibile creare ogni definizione di canale sul computer a cui si applica. Esistono delle limitazioni su come creare le definizioni di canale su un computer client.

“Creazione di definizioni di connessioni server e client sul server” a pagina 117
E'possibile creare entrambe le definizioni sul server, quindi rendere la definizione di connessione client disponibile per il client.

“Programmi di uscita canale per canali MQI” a pagina 122
Tre tipi di uscite canale sono disponibili per l'ambiente client WebSphere MQ MQI su UNIX, Linux e Windows .

“Connessione di un client a un gruppo di condivisione code” a pagina 126
È possibile connettere un client a un gruppo di condivisione code creando un canale MQI tra un client e un gestore code su un server che è membro di un gruppo di condivisione code.

“Configurazione di un client utilizzando un file di configurazione” a pagina 128

Configurare i client utilizzando gli attributi in un file di testo. Questi attributi possono essere sovrascritti dalle variabili di ambiente o in altri modi specifici della piattaforma.

Attività correlate

Connessione delle applicazioni client MQI IBM MQ ai gestori code

Riferimenti correlati

VISUALIZZA CHLAUTH

SET CHLAUTH

Il tipo di comunicazione da utilizzare

Piattaforme differenti supportano protocolli di comunicazione differenti. La scelta del protocollo di trasmissione dipende dalla propria combinazione di piattaforme client e server WebSphere MQ .

Esistono quattro tipi di comunicazione per i canali MQI su diverse piattaforme:

- LU 6.2
- NetBIOS
- SPX
- TCP/IP

Quando si definiscono i canali MQI, ciascuna definizione di canale deve specificare un attributo del protocollo di trasmissione (tipo di trasporto). Un server non è limitato a un solo protocollo, quindi diverse definizioni di canale possono specificare protocolli differenti. Per i client WebSphere MQ MQI, potrebbe essere utile disporre di canali MQI alternativi che utilizzano protocolli di trasmissione differenti.

La scelta del protocollo di trasmissione dipende anche dalla particolare combinazione delle piattaforme client e server WebSphere MQ . Le combinazioni possibili sono mostrate nella seguente tabella.

Tabella 14. Protocolli di trasmissione - combinazione di WebSphere MQ piattaforme client e server

Protocollo di trasmissione	**Client WebSphere MQ MQI**	**WebSphere MQ Server**
TCP/IP	Sistemi UNIX Finestre	Sistemi UNIX Finestre
LU 6.2	Sistemi UNIX[1] Finestre	Sistemi UNIX[1] Finestre
NetBIOS	Finestre	Finestre
SPX	Finestre	Finestre

Nota:

1. Eccetto Linux (piattaforma POWER)

Concetti correlati

“Definizione di un collegamento TCP su Windows” a pagina 85

Definire una connessione TCP configurando un canale all'estremità di invio per specificare l'indirizzo della destinazione ed eseguendo un programma listener all'estremità di ricezione.

“Definizione di un collegamento TCP su UNIX and Linux” a pagina 95

La definizione del canale all'estremità di invio specifica l'indirizzo della destinazione. Il listener o il daemon inet è configurato per la connessione all'estremità di ricezione.

“Definizione di un collegamento LU 6.2 su Windows” a pagina 87

SNA deve essere configurato in modo che sia possibile stabilire una conversazione LU 6.2 tra le macchine.

"Definizione di una connessione LU 6.2 su UNIX and Linux" a pagina 98
SNA deve essere configurato in modo che sia possibile stabilire una conversazione LU 6.2 tra le macchine.

"Definizione di una connessione NetBIOS su Windows" a pagina 89
WebSphere MQ utilizza tre tipi di risorsa NetBIOS quando si stabilisce una connessione NetBIOS a un altro prodotto WebSphere MQ : sessioni, comandi e nomi. Ciascuna di queste risorse ha un limite, che viene stabilito per impostazione predefinita o per scelta durante l'installazione di NetBIOS.

"Definizione di un collegamento SPX su Windows" a pagina 91
Una connessione SPX si applica solo a client e server che eseguono Windows XP e Windows 2003 Server.

Riferimenti correlati

"Limiti di connessione TCP/IP" a pagina 103
Il numero di richieste di connessione in sospeso che possono essere accodate su una singola porta TCP/IP dipende dalla piattaforma. Si verifica un errore se viene raggiunto il limite.

Definizione di una connessione TCP/IP

Specifica di un tipo di trasporto TCP sulla definizione di canale all'estremità client. Avviare un programma listener sul server.

Specificare una connessione TCP/IP sul client specificando un tipo di trasporto TCP sulla definizione del canale.

I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente. A tale scopo, è necessario avviare un programma listener per rilevare le richieste di rete in entrata e avviare il canale associato. La procedura per avviare un programma listener dipende dalla piattaforma del server.

Consultare gli argomenti correlati per le piattaforme client e server.

Limiti di connessione TCP/IP

Il numero di richieste di connessione in sospeso che possono essere accodate su una singola porta TCP/IP dipende dalla piattaforma. Si verifica un errore se viene raggiunto il limite.

Questo limite di connessione non corrisponde al numero massimo di client che è possibile collegare a un server IBM WebSphere MQ . È possibile collegare più client a un server, fino al livello determinato dalle risorse di sistema del server. I valori di backlog per le richieste di connessione sono riportati nella seguente tabella:

Tabella 15. Numero massimo di richieste di connessione in sospeso accodate su una porta TCP/IP

Piattaforma server	**Numero massimo di richieste di connessione**
AIX	100
HP-UX	20
Linux	100
IBM	255
Solaris	100
Server Windows	100
Workstation Windows	100
z/OS	255

Se viene raggiunto il limite di connessione, il client riceve un codice di ritorno di MQRC_HOST_NOT_AVAILABLE dalla chiamata `MQCONN` e un errore AMQ9202 nel log degli errori del client (`/var/mqm/errors/AMQERR0n.LOG` sui sistemi UNIX and Linux o `amqerr0n.log` nella sottodirectory

degli errori dell'installazione del client IBM WebSphere MQ su Windows). Se il client ritenta la richiesta MQCONN , potrebbe avere esito positivo.

Per aumentare il numero di richieste di connessione che è possibile effettuare ed evitare che i messaggi di errore vengano generati da questa limitazione, è possibile che più listener siano in ascolto su una porta diversa o che abbiano più di un gestore code.

Definizione di una connessione NetBIOS o SPX

Le connessioni NetBIOS e SPX si applicano solo ai sistemi Windows .

Una connessione NetBIOS si applica solo a client e server su cui è in esecuzione Windows. Consultare Definizione di una connessione NetBIOS.

Una connessione SPX si applica solo a un client e a un server su cui è in esecuzione Windows XP o Windows 2003 Server. Consultare Definizione di una connessione SPX.

Configurazione di un client transazionale esteso

Questa raccolta di argomenti descrive come configurare la funzione transazionale estesa per ogni categoria di gestore transazioni.

Per ciascuna piattaforma, il client transazionale esteso fornisce supporto per i seguenti gestori transazioni esterni:

Gestori transazioni compatibili con XA
Il client transazionale esteso fornisce l'interfaccia del gestore risorse XA per supportare i gestori transazioni conformi a XA come CICS e Tuxedo.

Microsoft Transaction Server (solo sistemiWindows)
Solo su sistemi Windows , l'interfaccia del gestore risorse XA supporta anche Microsoft Transaction Server (MTS). Il supporto WebSphere MQ MTS fornito con il client transazionale esteso fornisce il bridge tra MTS e l'interfaccia del gestore risorse XA.

WebSphere Application Server
Le versioni precedenti di WebSphere MQ supportava WebSphere Application Server Versione 4 o Versione 5 e richiedeva di eseguire determinate attività di configurazione per utilizzare il client transazionale esteso. WebSphere Application Server Versione 6 e successive include un provider di messaggistica WebSphere MQ , quindi non è necessario utilizzare il client transazionale esteso.

Concetti correlati

“Configurazione di gestori transazioni compatibili con XA” a pagina 104
Configurare innanzitutto il client di base WebSphere MQ , quindi configurare la funzione transazionale estesa utilizzando le informazioni contenute in questi argomenti.

“ Microsoft Transaction Server” a pagina 112
Non è richiesta alcuna configurazione aggiuntiva prima di poter utilizzare MTS come gestore transazioni. Tuttavia, ci sono alcuni punti da notare.

Configurazione di gestori transazioni compatibili con XA

Configurare innanzitutto il client di base WebSphere MQ , quindi configurare la funzione transazionale estesa utilizzando le informazioni contenute in questi argomenti.

Nota: Questa sezione presuppone che l'utente abbia una conoscenza di base dell'interfaccia XA come pubblicata da Open Group in *Distributed Transaction Processing: The XA Specification*.

Per configurare un client transazionale esteso, è necessario configurare prima il client di base WebSphere MQ come descritto in Installazione di un client IBM WebSphere MQ . Utilizzando le informazioni contenute in questa sezione, è possibile configurare la funzione transazionale estesa per un gestore transazioni compatibile con XA, ad esempio CICS e Tuxedo.

Un gestore transazioni comunica con un gestore code come gestore risorse utilizzando lo stesso canale MQI utilizzato dall'applicazione client connessa al gestore code. Quando il gestore transazioni emette una

chiamata di funzione del gestore risorse (xa_), il canale di MQI viene utilizzato per inoltrare la chiamata al gestore code e per ricevere l'output dal gestore code.

Il gestore transazioni può avviare il canale MQI emettendo una chiamata xa_open per aprire il gestore code come gestore risorse oppure l'applicazione client può avviare il canale MQI emettendo una chiamata MQCONN o MQCONNX.

- Se il gestore transazioni avvia il canale MQI e l'applicazione client successivamente richiama MQCONN o MQCONNX sullo stesso thread, la chiamata MQCONN o MQCONNX viene completata correttamente e viene restituito un handle di connessione all'applicazione. L'applicazione non riceve un codice di completamento MQCC_WARNING con un codice motivo MQRC_ALREADY_CONNECTED.
- Se l'applicazione client avvia il canale MQI e il gestore transazioni in seguito richiama xa_open sullo stesso thread, la chiamata xa_open viene inoltrata al gestore code utilizzando tale canale.

In una situazione di ripristino in seguito a un errore, quando non è in esecuzione alcuna applicazione client, il gestore transazioni può utilizzare un canale MQI dedicato per ripristinare le unità di lavoro incomplete a cui il gestore code partecipava al momento dell'errore.

Tenere presenti le seguenti condizioni quando si utilizza un client transazionale esteso con un gestore transazioni compatibile con XA:

- All'interno di un singolo thread, un'applicazione client può essere connessa a un solo gestore code alla volta. Questa limitazione si applica solo quando si usa un client transazionale esteso; un'applicazione client che utilizza un WebSphere MQ client di base può essere connessa a più di un gestore code contemporaneamente all'interno di un singolo thread.
- Ogni thread di una applicazione client può connettersi a un gestore code differente.
- Un'applicazione client non può utilizzare handle di connessione condivisi.

Per configurare la funzione transazionale estesa, è necessario fornire le seguenti informazioni al gestore transazioni per ciascun gestore code che agisce come gestore risorse:

- Una stringa xa_open
- Un puntatore a una struttura di commutazione XA

Quando il gestore transazioni richiama xa_open per aprire il gestore code come gestore risorse, trasmette la stringa xa_open al client transazionale esteso come argomento, *xa_info*, sulla chiamata. Il client transazionale esteso utilizza le informazioni nella stringa xa_open nei modi seguenti:

- Per avviare un canale MQI per il gestore code del server, se l'applicazione client non ne ha già avviato uno
- Per verificare che il gestore code che il gestore transazioni apre come gestore risorse sia uguale al gestore code a cui si connette l'applicazione client
- Per individuare le funzioni ax_reg e ax_unreg del gestore transazioni, se il gestore code utilizza la registrazione dinamica

Per il formato di una stringa xa_open e per ulteriori dettagli sul modo in cui le informazioni nella stringa xa_open vengono utilizzate da un client transazionale esteso, consultare “Il formato di una stringa xa_open” a pagina 106.

Una struttura di switch XA consente al gestore transazioni di individuare le funzioni xa _ fornite dal client transazionale esteso e specifica se il gestore code utilizza la registrazione dinamica. Per informazioni sulle strutture di switch XA fornite con un client transazionale esteso, consultare “Le strutture di switch XA” a pagina 109.

Per informazioni su come configurare la funzione transazionale estesa per un determinato gestore transazioni e per qualsiasi altra informazione sull'utilizzo del gestore transazioni con un client transazionale esteso, consultare le seguenti sezioni:

- “Configurazione di un client transazionale esteso per CICS” a pagina 111
- “Configurazione di un client transazionale esteso per Tuxedo” a pagina 112

Concetti correlati

“I parametri CHANNEL, TRPTYPE, CONNAME e QMNAME della stringa xa_open” a pagina 108
Utilizzare queste informazioni per comprendere come il client transazionale esteso utilizza questi parametri per determinare il gestore code a cui connettersi.

“Ulteriore elaborazione degli errori per xa_open” a pagina 109
La chiamata xa_open ha esito negativo in determinate circostanze.

Attività correlate

“Utilizzo del client transazionale esteso con canali SSL” a pagina 110
Non è possibile impostare un canale SSL utilizzando la stringa xa_open. Seguire queste istruzioni per utilizzare la tabella di definizione del canale client (ccdt).

Riferimenti correlati

“I parametri TPM e AXLIB” a pagina 108
Un client transazionale esteso utilizza i parametri TPM e AXLIB per individuare le funzioni ax_reg e ax_unreg del gestore transazioni. Queste funzioni vengono utilizzate solo se il gestore code utilizza la registrazione dinamica.

“Ripristino in seguito a un errore nell'elaborazione transazionale estesa” a pagina 109
In seguito a un errore, un gestore transazioni deve essere in grado di recuperare eventuali unità di lavoro incomplete. A tale scopo, il gestore transazioni deve essere in grado di aprire come gestore risorse qualsiasi gestore code che stava partecipando a un'unità di lavoro incompleta al momento dell'errore.

Il formato di una stringa xa_open

Una stringa xa_open contiene coppie di valori e nomi di parametri definiti.

Una stringa xa_open ha il formato seguente:

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

dove *parm_name* è il nome di un parametro e *parm_value* è il valore di un parametro. I nomi dei parametri non sono sensibili al maiuscolo / minuscolo, ma, se non diversamente specificato, i valori dei parametri sono sensibili al maiuscolo / minuscolo. È possibile specificare i parametri in qualsiasi ordine.

I nomi, i significati e i valori validi dei parametri sono i seguenti:

Nome
Significato e valori validi

CHANNEL
Il nome di un canale MQI.

È un parametro facoltativo. Se viene fornito questo parametro, è necessario fornire anche il parametro CONNAME.

TRPTYPE
Il protocollo di comunicazioni per il canale MQI. I seguenti sono valori validi:

LU62
SNA LU 6.2

NETBIOS
NetBIOS

SPX
IPX/SPX

TCP
TCP/IP

È un parametro facoltativo. Se viene omesso, viene utilizzato il valore predefinito di TCP. I valori del parametro non sono sensibili al maiuscolo / minuscolo.

CONNAME
L'indirizzo di rete del gestore code all'estremità del server del canale MQI. I valori validi di questo parametro dipendono dal valore del valore del parametro TRPTYPE:

LU62
Un nome di destinazione simbolico, che identifica una voce di informazioni lato CPI-C.

Il nome qualificato di rete di una LU partner non è un valore valido né un alias LU partner. Questo perché non esistono ulteriori parametri per specificare un nome TP (transaction program) e un nome modo.

NETBIOS
Un nome NetBIOS .

SPX
Un indirizzo di rete a 4 byte, un indirizzo nodo a 6 byte e un numero socket a 2 byte facoltativo. Questi valori devono essere specificati in notazione esadecimale. Un punto deve separare gli indirizzi di rete e di nodo e il numero di socket, se fornito, deve essere racchiuso tra parentesi. Ad esempio:

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

Se il numero socket viene omesso, viene utilizzato il valore predefinito 5e86 .

TCP
Un nome host o un indirizzo IP, facoltativamente seguito da un numero di porta tra parentesi. Se il numero di porta viene omesso, viene utilizzato il valore predefinito 1414.

È un parametro facoltativo. Se questo parametro viene fornito, deve essere fornito anche il parametro CHANNEL.

QMNAME
Il nome del gestore code all'estremità server del canale MQI. Il nome non può essere vuoto o un singolo asterisco (*), né può iniziare con un asterisco. Ciò significa che il parametro deve identificare un gestore code specifico in base al nome.

Questo è un parametro obbligatorio.

Quando un'applicazione client è connessa a un gestore code specifico, qualsiasi ripristino della transazione deve essere elaborato dallo stesso gestore code.

Se l'applicazione si connette a un gestore code z/OS , può specificare il nome di un gestore code specifico o il nome di un gruppo di condivisione code (QSG). Utilizzando il nome del gestore code o il nome QSG, l'applicazione controlla se partecipa a una transazione con un'unità QMGR di disposizione del ripristino o con un'unità GROUP di disposizione del ripristino. La disposizione dell'unità di recupero GROUP consente il recupero della transazione da elaborare su qualsiasi membro del QSG. Per utilizzare le unità di ripristino GROUP, è necessario abilitare l'attributo gestore code **GROUPUR** .

TPM
Il gestore transazioni utilizzato. I valori validi sono CICS e TUXEDO.

Un client transazionale esteso utilizza questo parametro e il parametro AXLIB per lo stesso scopo. Per ulteriori informazioni su questi parametri, consultare Parametri TPM e AXLIB.

È un parametro facoltativo. I valori del parametro non sono sensibili al maiuscolo / minuscolo.

AXLIB
Il nome della libreria che contiene le funzioni ax_reg e ax_unreg del gestore transazioni.

È un parametro facoltativo.

Ecco un esempio di una stringa xa_open:

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

I parametri CHANNEL, TRPTYPE, CONNAME e QMNAME della stringa xa_open

Utilizzare queste informazioni per comprendere come il client transazionale esteso utilizza questi parametri per determinare il gestore code a cui connettersi.

Se i parametri CHANNEL e CONNAME sono forniti nella stringa xa_open, il client transazionale esteso utilizza questi parametri e il parametro TRPTYPE per avviare un canale MQI per il gestore code del server.

Se i parametri CHANNEL e CONNAME non vengono forniti nella stringa xa_open, il client transazionale esteso utilizza il valore della variabile di ambiente MQSERVER per avviare un canale MQI. Se la variabile di ambiente MQSERVER non è definita, il client transazionale esteso utilizza la voce nella definizione di canale client identificata dal parametro QMNAME.

In ciascuno di questi casi, il client transazionale esteso verifica che il valore del parametro QMNAME sia il nome del gestore code all'estremità server del canale MQI. Se non lo è, la chiamata xa_open ha esito negativo e il gestore transazioni riporta l'errore all'applicazione.

Se il client delle applicazioni si connette a un gestore code z/OS alla versione V7.0.1 o successiva, è possibile specificare un nome QSG (queue - sharing group) per il parametro QMNAME. Ciò consente al client applicativo di partecipare a una transazione con un'unità di disposizione di recupero GROUP.

Se l'applicazione utilizza un nome QSG nel campo del parametro QMNAME e la proprietà GROUPUR è disabilitata sul gestore code a cui si connette, la chiamata xa_open non riesce.

Se l'applicazione si connette a un gestore code con una versione precedente a V7.0.1, la chiamata xa_open riesce ma la transazione ha una disposizione di unità di ripristino QMGR. Verificare che le applicazioni che richiedono la disposizione dell'unità di recupero GROUP si connettano solo ai gestori code alla versione V7.0.1 o successiva.

Quando l'applicazione client successivamente richiama MQCONN o MQCONNX sullo stesso thread utilizzato dal gestore transazioni per emettere la chiamata xa_open, l'applicazione riceve un handle di connessione per il canale MQI avviato dalla chiamata xa_open. Un secondo canale MQI non viene avviato. Il client transazionale esteso controlla che il valore del parametro *QMgrName* nella chiamata MQCONN o MQCONNX sia il nome del gestore code all'estremità del server del canale MQI. In caso contrario, la chiamata MQCONN o MQCONNX ha esito negativo con un codice motivo MQRC_ANOTHER_Q_MGR_CONNECTED. Se il valore del parametro *QMgrName* è vuoto o un singolo asterisco (*), o inizia con un asterisco, la chiamata MQCONN o MQCONNX ha esito negativo con un codice motivo di MQRC_Q_MGR_NAME_ERROR.

Se l'applicazione client ha già avviato un canale MQI richiamando MQCONN o MQCONNX prima che il gestore transazioni chiami xa_open sullo stesso thread, il gestore transazioni utilizza invece questo canale MQI. Un secondo canale MQI non viene avviato. Il client transazionale esteso verifica che il valore del parametro QMNAME nella stringa xa_open sia il nome del gestore code server. In caso contrario, la chiamata xa_open ha esito negativo.

Se un'applicazione client avvia prima un canale MQI, il valore del parametro *QMgrName* nella chiamata MQCONN o MQCONNX può essere vuoto o un singolo asterisco (*) oppure può iniziare con un asterisco. In queste circostanze, tuttavia, è necessario assicurarsi che il gestore code a cui si connette l'applicazione sia lo stesso gestore code che il gestore transazioni intende aprire come gestore risorse quando in seguito richiama xa_open sullo stesso thread. È possibile che si verifichino meno problemi, quindi, se il valore del parametro *QMgrName* identifica esplicitamente il gestore code per nome.

I parametri TPM e AXLIB

Un client transazionale esteso utilizza i parametri TPM e AXLIB per individuare le funzioni ax_reg e ax_unreg del gestore transazioni. Queste funzioni vengono utilizzate solo se il gestore code utilizza la registrazione dinamica.

Se il parametro TPM viene fornito in una stringa xa_open, ma il parametro AXLIB non viene fornito, il client transazionale esteso assume un valore per il parametro AXLIB basato sul valore del parametro TPM. Consultare Tabella 16 a pagina 109 per i valori assunti del parametro AXLIB.

Tabella 16. Valori assunti del parametro AXLIB		
Valore di TPM	**Piattaforma**	**Valore assunto di AXLIB**
CICS	AIX	/usr/lpp/encina/lib/libEncServer.a(EncServer_shr.o)
CICS	HP-UX	/opt/encina/lib/libEncServer.sl
CICS	Solaris	/opt/encina/lib/libEncServer.so
CICS	Sistemi Windows	libEnc
Tuxedo	AIX	/usr/lpp/tuxedo/lib/libtux.a(libtux.so.60)
Tuxedo	HP-UX	/opt/tuxedo/lib/libtux.sl
Tuxedo	Solaris	/opt/tuxedo/lib/libtux.so.60
Tuxedo	Sistemi Windows	libtux

Se il parametro AXLIB viene fornito in una stringa xa_open, il client transazionale esteso utilizza il suo valore per sovrascrivere qualsiasi valore assunto basato sul valore del parametro TPM. Il parametro AXLIB può essere utilizzato anche per un gestore transazioni per il quale il parametro TPM non ha un valore specificato.

Ulteriore elaborazione degli errori per xa_open

La chiamata xa_open ha esito negativo in determinate circostanze.

Gli argomenti in questa sezione descrivono situazioni in cui la chiamata xa_open ha esito negativo. Ha esito negativo anche se si verifica una delle seguenti situazioni:

- Sono presenti errori nella stringa xa_open.
- Informazioni insufficienti per avviare un canale MQI.
- Si è verificato un problema durante il tentativo di avviare un canale MQI (ad esempio, il gestore code server non è in esecuzione).

Ripristino in seguito a un errore nell'elaborazione transazionale estesa

In seguito a un errore, un gestore transazioni deve essere in grado di recuperare eventuali unità di lavoro incomplete. A tale scopo, il gestore transazioni deve essere in grado di aprire come gestore risorse qualsiasi gestore code che stava partecipando a un'unità di lavoro incompleta al momento dell'errore.

Se è necessario modificare le informazioni di configurazione, è necessario assicurarsi che tutte le unità di lavoro incomplete siano state risolte prima di apportare le modifiche. In alternativa, è necessario verificare che le modifiche di configurazione non influiscano sulla capacità del gestore transazioni di aprire i gestori code che devono essere aperti. Di seguito sono riportati esempi di tali modifiche di configurazione:

- Modifica del contenuto di una stringa xa_open
- Modifica del valore della variabile di ambiente MQSERVER
- Modifica delle voci nella tabella di definizione del canale client (CCDT)
- Eliminazione di una definizione di canale di connessione server

Le strutture di switch XA

Due strutture switch XA vengono fornite con il client transazionale esteso su ciascuna piattaforma.

Queste strutture di switch sono:

MQRMIXASwitch
Questa struttura switch viene utilizzata da un gestore transazioni quando un gestore code, che funge da gestore risorse, non utilizza la registrazione dinamica.

MQRMIXASwitchDynamic
Questa struttura di switch viene utilizzata da un gestore transazioni quando un gestore code, che funge da gestore risorse, utilizza la registrazione dinamica.

Queste strutture di switch si trovano nelle librerie mostrate in Tabella 17 a pagina 110.

Tabella 17. Librerie WebSphere MQ contenenti le strutture di switch XA

Piattaforma	**Libreria contenente le strutture di switch XA**
AIX HP-UX Linux Solaris	*MQ_INSTALLATION_PATH*/lib/libmqcxa
Sistemi Windows	*MQ_INSTALLATION_PATH*\bin\mqcxa.dll [1]
MQ_INSTALLATION_PATH rappresenta la directory di alto livello in cui è installato WebSphere MQ .	

Il nome del gestore risorse WebSphere MQ in ogni struttura switch è MQSeries_XA_RMI, ma molti gestori code possono condividere la stessa struttura switch.

Concetti correlati

“Registrazione dinamica ed elaborazione transazionale estesa” a pagina 110
L'utilizzo della registrazione dinamica è una forma di ottimizzazione perché può ridurre il numero di chiamate alla funzione xa _ emesse dal gestore transazioni.

Registrazione dinamica ed elaborazione transazionale estesa
L'utilizzo della registrazione dinamica è una forma di ottimizzazione perché può ridurre il numero di chiamate alla funzione xa _ emesse dal gestore transazioni.

Se un gestore code non utilizza la registrazione dinamica, un gestore transazioni coinvolge il gestore code in ogni unità di lavoro. Il gestore transazioni esegue questa operazione richiamando xa_start, xa_end e xa_prepare, anche se il gestore code non dispone di risorse aggiornate all'interno dell'unità di lavoro.

Se un gestore code utilizza la registrazione dinamica, un gestore transazioni viene avviato supponendo che il gestore code non sia coinvolto in un'unità di lavoro e non richiami xa_start. Il gestore code viene quindi coinvolto nell'unità di lavoro solo se le relative risorse vengono aggiornate all'interno del controllo del punto di sincronizzazione. Se ciò si verifica, il client transazionale esteso richiama ax_reg per registrare il coinvolgimento del gestore code.

Utilizzo del client transazionale esteso con canali SSL

Non è possibile impostare un canale SSL utilizzando la stringa xa_open. Seguire queste istruzioni per utilizzare la tabella di definizione del canale client (ccdt).

Informazioni su questa attività

A causa della dimensione limitata della stringa xa_open xa_info, non è possibile passare tutte le informazioni richieste per configurare un canale SSL utilizzando il metodo xa_open string di connessione a un gestore code. Pertanto, è necessario utilizzare la tabella di definizione del canale client oppure, se il gestore transazioni lo consente, creare il canale con MQCONNX prima di emettere la chiamata xa_open.

Per utilizzare la tabella di definizione del canale client, seguire queste istruzioni:

Procedura

1. Specificare una stringa xa_open contenente solo il parametro qmname (nome gestore code) obbligatorio, ad esempio: `XA_Open_String=qmname=MYQM`
2. Utilizzare un gestore code per definire un canale CLNTCONN (client-connection) con i parametri SSL richiesti. Includere il nome gestore code nell'attributo QMNAME nella definizione CLNTCONN. Questo verrà associato al qmname nella stringa xa_open.

3. Rendere la definizione CLNTCONN disponibile per il sistema client in una CCDT (client channel definition table) o, su Windows, nella directory attiva.
4. Se si sta utilizzando una CCDT, identificare la CCDT contenente la definizione del canale CLNTCONN utilizzando le variabili di ambiente MQCHLLIB e MQCHLTAB. Impostare queste variabili negli ambienti utilizzati dall'applicazione client e dal gestore transazioni.

Risultati

Ciò fornisce al gestore transazioni una definizione di canale per il gestore code appropriato con gli attributi SSL necessari per autenticarsi correttamente, incluso SSLCIPH, CipherSpec.

Configurazione di un client transazionale esteso per CICS

Si configura un client transazionale esteso per l'utilizzo da parte di CICS aggiungendo una definizione della risorsa XAD a una regione CICS .

Aggiungere la definizione della risorsa XAD utilizzando il comando CICS resource definition online (RDO), **cicsadd**. La definizione della risorsa XAD specifica le seguenti informazioni:

- Una stringa xa_open
- Il nome percorso completo di un file di caricamento switch

Un file di caricamento switch viene fornito per l'utilizzo da parte di CICS su ognuna delle seguenti piattaforme: AIX, HP-UX, Solaris e Windows .Ogni file di caricamento switch contiene una funzione che restituisce un puntatore alla struttura di switch XA utilizzata per la registrazione dinamica, MQRMIXASwitchDynamic. Consultare Tabella 18 a pagina 111 per il nome percorso completo di ciascun file di caricamento switch.

Tabella 18. I file di caricamento switch

Piattaforma	**File di caricamento switch**
AIX HP-UX Linux Solaris	*MQ_INSTALLATION_PATH*/lib/amqczsc
Sistemi Windows	*MQ_INSTALLATION_PATH*\bin\mqcc4swi.dll [1]
MQ_INSTALLATION_PATH rappresenta la directory di alto livello in cui è installato WebSphere MQ .	

Di seguito è riportato un esempio di definizione della risorsa XAD per i sistemi Windows :

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

Per ulteriori informazioni sull'aggiunta di una definizione di risorsa XAD a una regione CICS , consultare *CICS Administration Reference* e il manuale *CICS Administration Guide* per la propria piattaforma.

Si notano le seguenti informazioni sull'utilizzo di CICS con un client transazionale esteso:

- È possibile aggiungere una sola definizione di risorsa XAD per WebSphere MQ a una regione CICS . Questo significa che solo un gestore code può essere associato a una regione e tutte le applicazioni CICS in esecuzione nella regione possono connettersi solo al gestore code. Se si desidera eseguire le applicazioni CICS che si collegano a un gestore code differente, è necessario eseguire le applicazioni in una regione differente.
- Ogni server delle applicazioni in una regione richiama xa_open durante l'inizializzazione e l'avvio di un canale MQI per il gestore code associato alla regione. Ciò significa che il Gestore code deve essere avviato prima dell'avvio di un server delle applicazioni, altrimenti la chiamata xa_open non riesce.

Tutte WebSphere MQ le applicazioni client MQI elaborate successivamente dal server delle applicazioni utilizzano lo stesso canale MQI.

- Quando viene avviato un canale MQI e non c'è alcuna uscita di protezione all'estremità client del canale, l'ID utente che passa dal sistema client all'MCA di connessione server è `cics`. In determinate circostanze, il gestore code utilizza questo ID utente per i controlli di autorizzazione quando la connessione server MCA successivamente tenta di accedere alle risorse del gestore code per conto di un'applicazione client. Se questo ID utente viene utilizzato per i controlli delle autorizzazioni, è necessario assicurarsi che disponga dell'autorizzazione per accedere a tutte le risorse necessarie per accedere.

  Per informazioni su quando il gestore code utilizza questo ID utente per i test di autorizzazione, consultare Sicurezza.
- Le uscite di terminazione attività CICS fornite per l'utilizzo sui sistemi client WebSphere MQ sono elencate in Tabella 19 a pagina 112. Queste uscite vengono configurate nello stesso modo in cui vengono configurate le uscite corrispondenti per sistemi server WebSphere MQ . Per queste informazioni, quindi, consultare Abilitazione delle uscite utente CICS.

Tabella 19. Uscite di terminazione attività CICS

Piattaforma	Sorgente	Libreria
AIX HP-UX Linux Solaris	amqzscgx.c	amqczscg
Sistemi Windows	amqzscgn.c	mqcc1415.dll

Configurazione di un client transazionale esteso per Tuxedo

Per configurare la definizione della risorsa XAD per l'utilizzo da parte di Tuxedo, aggiornare il file UBBCONFIG e la tabella del gestore risorse.

Per configurare la definizione della risorsa XAD per l'utilizzo da parte di Tuxedo, effettuare quanto segue:

- Nella sezione GROUPS del file Tuxedo UBBCONFIG per un'applicazione, utilizzare il parametro OPENINFO per specificare una stringa xa_open.

  Per un esempio di come eseguire questa operazione, consultare il file UBBCONFIG di esempio, fornito per l'utilizzo con i programmi di esempio Tuxedo. In AIX, HP-UXe Solaris, il nome del file è ubbstxcx.cfg e, su sistemi Windows , il nome del file è `ubbstxcn.cfg`.
- Nella voce per un gestore code nella tabella del gestore risorse Tuxedo:
  - udataobj/RM (AIX, HP-UXe Solaris)
  - udataobj\rm (sistemi Finestre)

  specificare il nome di una struttura di commutazione XA e il nome percorso completo della libreria che contiene la struttura. Per un esempio di come eseguire questa operazione per ciascuna piattaforma, consultare Esempi TUXEDO. Tuxedo supporta la registrazione dinamica di un gestore risorse e, pertanto, è possibile utilizzare MQRMIXASwitch o MQRMIXASwitchDynamic.

Microsoft Transaction Server

Non è richiesta alcuna configurazione aggiuntiva prima di poter utilizzare MTS come gestore transazioni. Tuttavia, ci sono alcuni punti da notare.

Tenere presenti le seguenti informazioni sull'utilizzo di MTS con il client transazionale esteso:

- Un'applicazione MTS avvia sempre un canale MQI quando si connette a un gestore code del server. MTS, nel ruolo di gestore transazioni, utilizza lo stesso canale MQI per comunicare con il gestore code.

- A seguito di un errore, MTS deve essere in grado di recuperare eventuali unità di lavoro incomplete. Per far ciò, MTS deve essere in grado di comunicare con qualsiasi gestore code che partecipava a un'unità di lavoro incompleta al momento dell'errore.

  Quando un'applicazione MTS si connette a un gestore code del server e avvia un canale MQI, il client transazionale esteso estrae informazioni sufficienti dai parametri della chiamata MQCONN o MQCONNX per consentire il riavvio del canale in seguito a un errore, se necessario. Il client transazionale esteso trasmette le informazioni a MTS e MTS registra le informazioni nel relativo log.

  Se l'applicazione MTS emette una chiamata MQCONN, queste informazioni sono semplicemente il nome del gestore code. Se l'applicazione MTS emette una chiamata MQCONNX e fornisce una struttura di definizione del canale, MQCD, le informazioni includono anche il nome del canale MQI, l'indirizzo di rete del gestore code del server e il protocollo di comunicazione per il canale.

  In una situazione di recupero, MTS restituisce queste informazioni al client transazionale esteso, che utilizza per riavviare il canale MQI.

  Se è necessario modificare le informazioni di configurazione, assicurarsi che tutte le unità di lavoro incomplete siano state risolte prima di apportare le modifiche. In alternativa, verificare che le modifiche di configurazione non influiscano sulla capacità del client transazionale esteso di riavviare un canale MQI utilizzando le informazioni registrate da MTS. Di seguito sono riportati esempi di tali modifiche di configurazione:

  - Modifica del valore della variabile di ambiente MQSERVER
  - Modifica delle voci nella tabella di definizione del canale client (CCDT)
  - Eliminazione di una definizione di canale di connessione server
- Si notano le condizioni seguenti quando si utilizza un client transazionale esteso con MTS:
  - All'interno di un singolo thread, un'applicazione client può essere connessa a un solo gestore code alla volta.
  - Ogni thread di una applicazione client può connettersi a un gestore code differente.
  - Un'applicazione client non può utilizzare handle di connessione condivisi.

Definizione di canali MQI

Per creare un nuovo canale, devi creare **due** definizioni di canale, una per ogni estremità della connessione, utilizzando lo stesso nome di canale e tipi di canale compatibili. In questo caso, i tipi di canali sono *connessione server* e *connessione client*.

Canali definiti dall'utente

Quando il server non definisce automaticamente i canali, esistono due modi per creare le definizioni di canale e fornire all'applicazione WebSphere MQ su WebSphere MQ MQI l'accesso al canale.

Questi due metodi sono descritti in dettaglio:

1. Creare una definizione di canale sul client WebSphere MQ e l'altra sul server.

   Ciò si applica a qualsiasi combinazione di piattaforme server e client WebSphere MQ . Utilizzarlo quando si inizia a utilizzare il sistema o per verificare la configurazione.

   Consultare “Creazione di definizioni di connessione server e di connessione client su piattaforme differenti” a pagina 115 per i dettagli su come utilizzare questo metodo.
2. Creare entrambe le definizioni di canale sulla macchina server.

   Utilizzare questo metodo quando si impostano più canali e WebSphere MQ macchine client MQI contemporaneamente.

   Consultare “Creazione di definizioni di connessioni server e client sul server” a pagina 117 per i dettagli su come utilizzare questo metodo.

Canali definiti automaticamente

I prodotti WebSphere MQ su piattaforme diverse da z/OS includono una funzione che può creare automaticamente una definizione di canale sul server, se non esiste.

Se una richiesta di collegamento in entrata viene ricevuta da un client e non è possibile trovare una definizione di connessione al server appropriata su tale gestore code, WebSphere MQ crea automaticamente una definizione e la aggiunge al gestore code. La definizione automatica è basata sulla definizione del canale di connessione server predefinito SYSTEM.AUTO.SVRCONN. È possibile abilitare la definizione automatica delle definizioni di connessione server aggiornando l'oggetto del gestore code utilizzando il comando ALTER QMGR con il parametro CHAD (o il comando PCF Modifica gestore code con il parametro ChannelAutoDef).

Per ulteriori informazioni sulla creazione automatica delle definizioni di canale, consultare Definizione automatica dei canali riceventi e di connessione server.

Concetti correlati

“Canali definiti automaticamente” a pagina 114
I prodotti WebSphere MQ su piattaforme diverse da z/OS includono una funzione che può creare automaticamente una definizione di canale sul server, se non esiste.

“Canali definiti dall'utente” a pagina 114
Quando il server non definisce automaticamente i canali, esistono due modi per creare le definizioni di canale e fornire all'applicazione WebSphere MQ su WebSphere MQ MQI l'accesso al canale.

“Funzione di controllo canale” a pagina 54
La funzione di controllo del canale consente di definire, monitorare e controllare i canali.

Canali definiti automaticamente

I prodotti WebSphere MQ su piattaforme diverse da z/OS includono una funzione che può creare automaticamente una definizione di canale sul server, se non esiste.

Se una richiesta di collegamento in entrata viene ricevuta da un client e non è possibile trovare una definizione di connessione al server appropriata su tale gestore code, WebSphere MQ crea automaticamente una definizione e la aggiunge al gestore code. La definizione automatica è basata sulla definizione del canale di connessione server predefinito SYSTEM.AUTO.SVRCONN. È possibile abilitare la definizione automatica delle definizioni di connessione server aggiornando l'oggetto del gestore code utilizzando il comando ALTER QMGR con il parametro CHAD (o il comando PCF Modifica gestore code con il parametro ChannelAutoDef).

Canali definiti dall'utente

Quando il server non definisce automaticamente i canali, esistono due modi per creare le definizioni di canale e fornire all'applicazione WebSphere MQ su WebSphere MQ MQI l'accesso al canale.

Questi due metodi sono descritti in dettaglio:

1. Creare una definizione di canale sul client WebSphere MQ e l'altra sul server.

   Ciò si applica a qualsiasi combinazione di piattaforme server e client WebSphere MQ . Utilizzarlo quando si inizia a utilizzare il sistema o per verificare la configurazione.

   Consultare “Creazione di definizioni di connessione server e di connessione client su piattaforme differenti” a pagina 115 per i dettagli su come utilizzare questo metodo.
2. Creare entrambe le definizioni di canale sulla macchina server.

   Utilizzare questo metodo quando si impostano più canali e WebSphere MQ macchine client MQI contemporaneamente.

   Consultare “Creazione di definizioni di connessioni server e client sul server” a pagina 117 per i dettagli su come utilizzare questo metodo.

Creazione di definizioni di connessione server e di connessione client su piattaforme differenti

È possibile creare ogni definizione di canale sul computer a cui si applica. Esistono delle limitazioni su come creare le definizioni di canale su un computer client.

Su tutte le piattaforme, è possibile utilizzare i comandi WebSphere MQ Script (MQSC), i comandi PCF (programmable command format) o IBM WebSphere MQ Explorer per definire un canale di connessione server sulla macchina server.

Poiché i comandi MQSC non sono disponibili su una macchina su cui è stato installato WebSphere MQ solo come client MQI WebSphere MQ , è necessario utilizzare diversi modi di definire un canale di connessione client sulla macchina client.

Concetti correlati

"Creazione di un canale di connessione client su un client IBM WebSphere MQ MQI" a pagina 116
È possibile definire un canale di connessione client sulla stazione di lavoro client utilizzando MQSERVER o utilizzando la struttura MQCNO su una chiamata MQCONNX.

Attività correlate

"Definizione di un canale di connessione server sul server" a pagina 115
Avviare MQSC, se necessario, quindi definire il canale di connessione server.

Definizione di un canale di connessione server sul server

Avviare MQSC, se necessario, quindi definire il canale di connessione server.

Procedura

1. Opzionale: Se la piattaforma server non è z/OS, creare e avviare prima un gestore code, quindi avviare i comandi MQSC.
   a) Creare un gestore code, denominato QM1 , ad esempio:

   ```
   crtmqm QM1
   ```

   b) Avviare il gestore code:

   ```
   strmqm QM1
   ```

   c) Comandi di avvio MQSC:

   ```
   runmqsc QM1
   ```

2. Definire un canale con il nome scelto e un tipo di canale *server - connection*.

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

   Questa definizione di canale è associata al gestore code in esecuzione sul server.
3. Utilizzare il seguente comando per consentire l'accesso di connessione in entrata al gestore code:

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

   - Dove SET CHLAUTH utilizza il nome del canale definito nel passo precedente.
   - Dove *'indirizzo IP'* è l'indirizzo IP del client.
   - Dove *'userid'* è l'ID che si desidera fornire al canale per il controllo dell'accesso alle code di destinazione. Questo campo è sensibile al maiuscolo / minuscolo.

   È possibile scegliere di identificare la connessione in entrata utilizzando un numero di attributi differenti. L'esempio utilizza l'indirizzo IP. Gli attributi alternativi includono l'ID utente client e il DN (Distinguished Name) del soggetto SSL o TLS. Per ulteriori informazioni, consultare Record di autenticazione di canale

Creazione di un canale di connessione client su un client IBM WebSphere MQ MQI

È possibile definire un canale di connessione client sulla stazione di lavoro client utilizzando MQSERVER o utilizzando la struttura MQCNO su una chiamata MQCONNX.

Utilizzo di MQSERVER

È possibile utilizzare la variabile di ambiente MQSERVER per specificare una definizione semplice di un canale di connessione client. È semplice nel senso che è possibile specificare solo alcuni attributi del canale utilizzando questo metodo.

- Specificare una definizione di canale semplice su Windows nel modo seguente:

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

- Specificare una semplice definizione di canale su sistemi UNIX and Linux nel modo seguente:

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

dove:

- `ChannelName` deve essere lo stesso nome definito sul server. Non può contenere una barra.
- `TransportType` può essere uno dei valori riportati di seguito, a seconda della piattaforma client MQI IBM WebSphere MQ :
  - LU62
  - TCP
  - NETBIOS
  - SPX

  Nota: Su sistemi UNIX and Linux , il TransportType è sensibile al maiuscolo / minuscolo e deve essere maiuscolo. Una chiamata `MQCONN` o `MQCONNX` restituisce 2058 se TransportType non è riconosciuto
- `ConnectionName` è il nome del server come definito nel protocollo di comunicazione (TransportType).

Ad esempio, su Windows:

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

oppure, su sistemi UNIX and Linux :

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

Nota: Per modificare il numero di porta TCP/IP, consultare “SERVER MQT” a pagina 150.

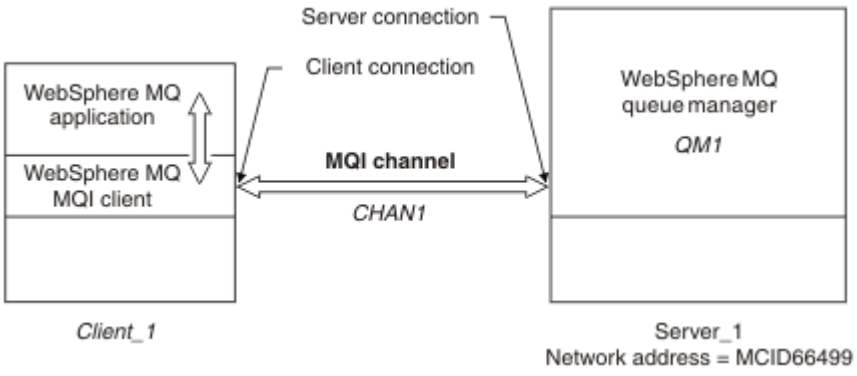


Figura 17. Definizione di canale semplice

Alcuni altri esempi di definizioni di canali semplici sono:

- Su Windows:

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

- Su sistemi UNIX and Linux :

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

dove B0X99 è la LU 6.2 ConnectionName.

Sul client IBM WebSphere MQ MQI, tutte le richieste **MQCONN** o **MQCONNX** tentano quindi di utilizzare il canale definito, a meno che il canale non venga sovrascritto in una struttura MQCD a cui si fa riferimento dalla struttura MQCNO fornita a **MQCONNX**.

Nota: Per ulteriori informazioni sulla variabile di ambiente *MQSERVER* , consultare “SERVER MQT” a pagina 150.

Utilizzo della struttura MQCNO su una chiamata MQCONNX

Un'applicazione client IBM WebSphere MQ MQI può utilizzare la struttura delle opzioni di connessione, MQCNO, su una chiamata **MQCONNX** per fare riferimento a una struttura di definizioni di canale, MQCD, contenente la definizione di un canale di connessione client.

In questo modo, l'applicazione client può specificare gli attributi **ChannelName**, **TransportType**e **ConnectionName** di un canale al runtime, consentendo all'applicazione client di connettersi a più gestori code del server contemporaneamente.

Tenere presente che se si definisce un canale utilizzando la variabile di ambiente *MQSERVER* , non è possibile specificare gli attributi **ChannelName**, **TransportType**e **ConnectionName** al runtime.

Un'applicazione client può anche specificare gli attributi di un canale come **MaxMsgLength** e **SecurityExit**. La specifica di tali attributi consente all'applicazione client di specificare i valori per gli attributi che non sono i valori predefiniti e consente ai programmi di uscita canale di essere richiamati all'estremità client di un canale MQI.

Se un canale utilizza SSL (Secure Sockets Layer) o TLS (Transport Layer Security), un'applicazione client può anche fornire informazioni relative a SSL o TLS nella struttura MQCD.Ulteriori informazioni relative a SSL o TLS possono essere fornite nella struttura delle opzioni di configurazione SSL o TLS, MQSCO, a cui fa riferimento anche la struttura MQCNO in una chiamata **MQCONNX** .

Per ulteriori informazioni sulle strutture MQCNO, MQCD e MQSCO, consultare MQCNO, MQCDe MQSCO.

Nota: Il programma di esempio per MQCONNX è denominato **amqscnxc**. Un altro programma di esempio denominato **amqsssl**c dimostra l'utilizzo della struttura MQSCO.

Creazione di definizioni di connessioni server e client sul server

E'possibile creare entrambe le definizioni sul server, quindi rendere la definizione di connessione client disponibile per il client.

Definire innanzitutto un canale di connessione server, quindi definire un canale di connessione client. Su tutte le piattaforme, è possibile utilizzare i comandi WebSphere MQ Script (MQSC), i comandi PCF (programmable command format) o IBM WebSphere MQ Explorer per definire un canale di connessione server sulla macchina server.

Le definizioni di canale di connessione client create sul server vengono rese disponibili ai client utilizzando una CCDT (client channel definition table).

Concetti correlati

“Tabella definizione canale client” a pagina 118

La tabella di definizione del canale client (CCDT) determina le definizioni di canale e le informazioni di autenticazione utilizzate dalle applicazioni client per connettersi al gestore code. Su piattaforme diverse da z/OS viene creata automaticamente una CCDT. È quindi necessario renderla disponibile per l'applicazione client.

Attività correlate

“Definizione del canale di connessione server sul server” a pagina 120
Creare una definizione di canale di connessione server per il gestore code.

“Definizione del canale di connessione client nel server” a pagina 120
Dopo aver definito il canale di connessione server, si definisce ora il canale di connessione client corrispondente.

“Accesso alle definizioni del canale di connessione client” a pagina 121
Rendere la CCDT (client channel definition table) disponibile per le applicazioni client copiandola o condividandola, quindi specificarne l'ubicazione e il nome sul computer client.

Tabella definizione canale client

La tabella di definizione del canale client (CCDT) determina le definizioni di canale e le informazioni di autenticazione utilizzate dalle applicazioni client per connettersi al gestore code. Su piattaforme diverse da z/OS viene creata automaticamente una CCDT. È quindi necessario renderla disponibile per l'applicazione client.

Lo scopo della CCDT (client channel definition table) è determinare le definizioni di canale utilizzate dalle applicazioni client per connettersi al gestore code. La definizione di canale specifica anche le informazioni di autenticazione che si applicano alle connessioni.

CDT è un file binario. Viene generato da un gestore code. Il gestore code non legge il file CCDT.

Su piattaforme diverse da z/OS, CCDT viene creata quando viene creato il gestore code. I canali di connessione client vengono aggiunti alla tabella quando si utilizza il comando **DEFINE CHANNEL** e le relative definizioni vengono modificate quando si immette il comando **ALTER CHANNEL** .

È possibile utilizzare CCDT per fornire i client con le informazioni di autenticazione per verificare la revoca del certificato SSL. Definire un elenco nomi contenente gli oggetti delle informazioni di autenticazione e impostare l'attributo gestore code **SSLCRLNameList** sul nome dell'elenco nomi.

Esistono diversi modi per un'applicazione client per utilizzare una CCDT. La CCDT può essere copiata sul computer client. È possibile copiare la CCDT in un'ubicazione condivisa da più di un client. È possibile rendere il CCDT accessibile per il client come un file condiviso, mentre rimane sul server.

Se si utilizza FTP per copiare il file, utilizzare l'opzione `bin` per impostare la modalità binaria; non utilizzare la modalità `ASCII` predefinita. Qualunque sia il metodo scelto per rendere disponibile la CCDT, la posizione deve essere sicura per impedire modifiche non autorizzate ai canali.

Piattaforme diverse da z/OS

Una CCDT predefinita denominata `AMQCLCHL.TAB` viene creata quando si crea un gestore code.

Per impostazione predefinita, AMQCLCHL.TAB si trova nella seguente directory su un server:

- UNIX Linux Su sistemi UNIX and Linux :

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

  Il nome della directory a cui fa riferimento *QUEUEMANAGERNAME* è sensibile al maiuscolo / minuscolo sui sistemi UNIX and Linux . Il nome della directory potrebbe non essere lo stesso del nome del gestore code, se il nome del gestore code contiene caratteri speciali.

- Windows Su Windows:

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

MQ_INSTALLATION_PATH rappresenta la directory di livello superiore in cui è installato IBM WebSphere MQ .

Tuttavia, è possibile che si sia scelto di utilizzare una directory differente per i dati del gestore code. È possibile specificare il parametro **-md** *DataPath* quando si utilizza il comando **crtmqm** . In tal caso, AMQCLCHL.TAB si trova nella directory @ipcc del *DataPath* specificato.

Il percorso della CCDT può essere modificato impostando MQCHLLIB. Se si imposta MQCHLLIB, tenere presente che se si dispone di più gestori code sullo stesso server, essi condividono la stessa ubicazione CCDT.

La CCDT viene creata quando viene creato il gestore code. Ogni voce di una CCDT rappresenta una connessione client a un gestore code specifico. Viene aggiunta una nuova voce quando si definisce un canale di connessione client utilizzando il comando **DEFINE CHANNEL** , e la voce viene aggiornata quando si modificano i canali di connessione client utilizzando il comando **ALTER CHANNEL** .

Come specificare l'ubicazione della CCDT sul client

Su un sistema client, è possibile specificare l'ubicazione della CCDT in due modi:

- Utilizzo delle variabili di ambiente MQCHLLIB per specificare la directory in cui si trova la tabella e MQCHLTAB per specificare il nome file della tabella.
- Utilizzo del file di configurazione client. Nella stanza CHANNELS , utilizzare gli attributi ChannelDefinitionDirectory per specificare la directory in cui si trova la tabella e ChannelDefinitionFile per specificare il nome file.

Se l'ubicazione è specificata sia nel file di configurazione client che utilizzando le variabili di ambiente, le variabili di ambiente hanno la priorità. È possibile utilizzare questa funzione per specificare un'ubicazione standard nel file di configurazione del client e sovrascriverla utilizzando le variabili di ambiente quando necessario.

Riferimenti correlati

"MQCHLLIB" a pagina 148
MQCHLLIB specifica il percorso di directory del file contenente la tabella di definizione del canale client (CCDT). Il file viene creato sul server, ma può essere copiato sulla workstation client WebSphere MQ .

Informazioni correlate

Utilizzo dei certificati revocati

CDT (migration and client channel definition tables)

In generale, il formato interno della tabella di definizione del canale del client potrebbe cambiare da un livello di release di IBM WebSphere MQ a quello successivo. Di conseguenza, un client IBM WebSphere MQ MQI può utilizzare una tabella di definizione di canale client solo quando è stata preparata da un gestore code del server che è allo stesso livello di release del client o a un livello di release precedente.

Un client MQI versione 7.1 IBM WebSphere MQ può utilizzare una tabella di definizione del canale client preparata da un gestore code versione 6.0 . Ma un client della versione 6.0 non può utilizzare una tabella di definizione di canale client preparata da un gestore code della versione 7.1 .

Canali di connessione client in Active Directory

Su sistemi Windows che supportano Active Directory, IBM WebSphere MQ pubblica i canali di connessione client in Active Directory per fornire il bind client-server dinamico.

Quando gli oggetti del canale di connessione client sono definiti, vengono scritti in un file di definizione del canale client , denominato AMQCLCHL.TAB per impostazione predefinita. Se i canali di connessione client utilizzano il protocollo TCP / IP, il server IBM WebSphere MQ li pubblica anche in Active Directory. Quando il client IBM WebSphere MQ stabilisce come connettersi al server, ricerca una definizione di oggetto del canale di connessione client pertinente utilizzando il seguente ordine di ricerca:

1. Struttura dati MQCONNX MQCD

2. variabile di ambiente MQSERVER
3. file di definizione canale client
4. Active Directory

Questo ordine indica che le applicazioni correnti non sono interessate da alcuna modifica. È possibile considerare queste voci in Active Directory come record nel file di definizione del canale client e il client IBM WebSphere MQ le elabora nello stesso modo. Per configurare e gestire il supporto per la pubblicazione di definizioni di canali di connessione client in Active Directory, utilizzare il comando `setmqscp` , come descritto in setmqscp.

Definizione del canale di connessione server sul server

Creare una definizione di canale di connessione server per il gestore code.

Procedura

1. Sulla macchina server, definire un canale con il nome scelto e un tipo di canale *server - connection*. Ad esempio:

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

2. Utilizzare il seguente comando per consentire l'accesso di connessione in entrata al gestore code:

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

   - Dove SET CHLAUTH utilizza il nome del canale definito nel passo precedente.
   - Dove *'indirizzo IP'* l'indirizzo IP è l'indirizzo IP del client.
   - Dove *'userid'* è l'ID che si desidera fornire al canale per il controllo dell'accesso alle code di destinazione. Questo campo è sensibile al maiuscolo / minuscolo.

   È possibile scegliere di identificare la connessione in entrata utilizzando un numero di attributi differenti. L'esempio utilizza l'indirizzo IP. Gli attributi alternativi includono l'ID utente client e il DN (Distinguished Name) del soggetto SSL o TLS. Per ulteriori informazioni, consultare Record di autenticazione di canale

   Questa definizione di canale è associata al gestore code in esecuzione sul server.

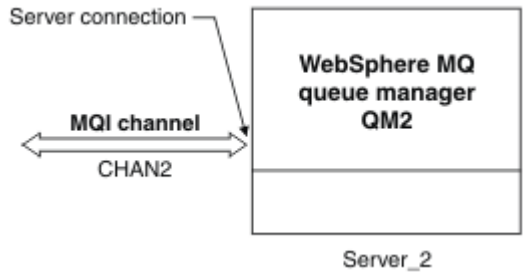


Figura 18. Definizione del canale di connessione server

Definizione del canale di connessione client nel server

Dopo aver definito il canale di connessione server, si definisce ora il canale di connessione client corrispondente.

Prima di iniziare

Definire il canale di connessione server.

Procedura

1. Definire un canale con lo stesso nome del canale di connessione server, ma con un tipo di canale *connessione client*. È necessario indicare il nome connessione (CONNAME). Per TCP/IP, il nome della connessione è l'indirizzo di rete o il nome host della macchina server. È inoltre consigliabile specificare il nome del gestore code (QMNAME) a cui si desidera connettere l'applicazione IBM WebSphere MQ , in esecuzione nell'ambiente client. Variando il nome del gestore code, è possibile definire una serie di canali per connettersi a gestori code differenti.

   ```
   DEFINE CHANNEL(CHAN2) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
   CONNAME(9.20.4.26) QMNAME(QM2) DESCR('Client-connection to Server_2')
   ```

2. Utilizzare il seguente comando per consentire l'accesso di connessione in entrata al gestore code:

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

   - Dove SET CHLAUTH utilizza il nome del canale definito nel passo precedente.
   - Dove *'indirizzo IP'* è l'indirizzo IP del client.
   - Dove *'userid'* è l'ID che si desidera fornire al canale per il controllo dell'accesso alle code di destinazione. Questo campo è sensibile al maiuscolo / minuscolo.

   È possibile scegliere di identificare la connessione in entrata utilizzando un numero di attributi differenti. L'esempio utilizza l'indirizzo IP. Gli attributi alternativi includono l'ID utente client e il DN (Distinguished Name) del soggetto SSL o TLS. Per ulteriori informazioni, consultare Record di autenticazione di canale

Risultati

Su piattaforme diverse da z/OS, questa definizione di canale è memorizzata in un file denominato CCDT (client channel definition table), associato con il gestore code. La tabella di definizione del canale client può contenere più di una definizione del canale di connessione client. Per ulteriori informazioni sulla tabella di definizioni di canali client e per le informazioni corrispondenti sul modo in cui le definizioni di canali di connessione client vengono memorizzate su z/OS, consultare “Tabella definizione canale client” a pagina 118.

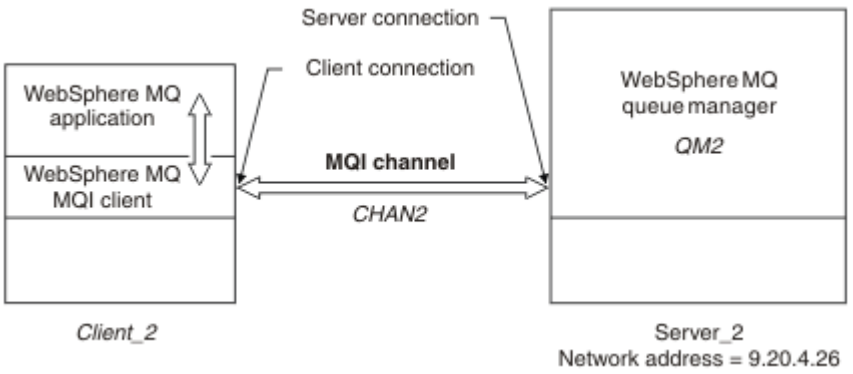


Figura 19. Definizione del canale di connessione client

Accesso alle definizioni del canale di connessione client

Rendere la CCDT (client channel definition table) disponibile per le applicazioni client copiandola o condividandola, quindi specificarne l'ubicazione e il nome sul computer client.

Prima di iniziare

Sono stati definiti i canali di connessione client necessari.

Su z/OS, è stata creata una CCDT. Su altre piattaforme, la CCDT viene creata e aggiornata automaticamente.

Informazioni su questa attività

Affinché un'applicazione del client utilizzi la tabella di definizione del canale client (CCDT), è necessario renderla disponibile e specificarne l'ubicazione e il nome

Procedura

1. Rendere CCDT disponibile per le applicazioni client in uno dei tre seguenti modi:
   a) Opzionale: Copiare la CCDT sul computer client.
   b) Opzionale: Copiare la CCDT in una posizione condivisa da più di un client.
   c) Opzionale: Lasciare CCDT sul server ma renderlo condivisibile dal client.

   Qualunque sia la posizione scelta per la CCDT, la posizione deve essere sicura per evitare modifiche non autorizzate ai canali.
2. Sul client, specificare l'ubicazione e il nome del file che contiene CCDT in uno di tre modi:
   a) Opzionale: Utilizzare la sezione CHANNELS del file di configurazione client. Per ulteriori informazioni, vedere “Stanza CHANNELS del file di configurazione client” a pagina 138.
   b) Opzionale: Utilizzare le variabili di ambiente MQCHLLIB e MQCHLTAB.

      Ad esempio, è possibile impostare le variabili di ambiente immettendo:

      - Su sistemi HP Integrity NonStop Servere UNIX and Linux :

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

      dove *MQ_INSTALLATION_PATH* rappresenta la directory di alto livello in cui è installato WebSphere MQ .
   c) Opzionale: Solo su Windows, utilizzare il comando di controllo **setmqscp** per pubblicare le definizioni di canale di connessione client in Active Directory

   Se la variabile di ambiente MQSERVER è impostata, un client WebSphere MQ utilizza la definizione del canale di connessione client specificata da MQSERVER, al posto di qualsiasi definizione nella tabella di definizione del canale client.

Programmi di uscita canale per canali MQI

Tre tipi di uscite canale sono disponibili per l'ambiente client WebSphere MQ MQI su UNIX, Linux e Windows .

Sono:

- Uscita invio
- Uscita ricezione
- Uscita di sicurezza

Queste uscite sono disponibili sia sul client che sull'estremità server del canale. Le uscite non sono disponibili per l'applicazione se si utilizza la variabile di ambiente MQSERVER. Le uscite dei canali sono descritte in Programmi di uscita dei canali di messaggistica.

Le uscite di invio e ricezione funzionano insieme. Esistono diversi modi possibili in cui è possibile utilizzarle:

- Suddivisione e riassemblaggio di un messaggio
- Compressione e decompressione dei dati in un messaggio (questa funzionalità è fornita come parte di WebSphere MQ, ma è possibile utilizzare una tecnica di compressione differente)

- Crittografia e decrittografia dei dati utente (questa funzionalità è fornita come parte di WebSphere MQ, ma è possibile utilizzare una diversa tecnica di crittografia)
- Registrazione su giornale di ogni messaggio inviato e ricevuto

È possibile utilizzare l'uscita di protezione per assicurarsi che il server e il client WebSphere MQ vengano identificati correttamente e per controllare l'accesso.

Se le uscite di invio o ricezione sul lato connessione server dell'istanza del canale devono eseguire chiamate MQI sulla connessione a cui sono associate, utilizzano l'handle di connessione fornito nel campo MQCXP Hconn . È necessario essere consapevoli che le uscite di invio e ricezione della connessione client non possono effettuare chiamate MQI.

Concetti correlati

"Uscite di sicurezza su una connessione client" a pagina 123
È possibile utilizzare i programmi di uscita di sicurezza per verificare che il partner all'altra estremità di un canale sia autentico. Considerazioni speciali si applicano quando un'uscita di sicurezza viene applicata a una connessione client.

Uscite utente, uscite API e servizi installabili WebSphere MQ

Attività correlate

Estensione delle funzioni del gestore code

Riferimenti correlati

"Percorso delle uscite" a pagina 123
Un percorso predefinito per l'ubicazione delle uscite del canale è definito nel file di configurazione client. Le uscite canale vengono caricate quando un canale viene inizializzato.

"Identificazione della chiamata API in un programma di uscita di invio o ricezione" a pagina 125
Quando si utilizzano i canali MQI per i client, il byte 10 del buffer dell'agent identifica la chiamata API in uso quando viene richiamata un'uscita di invio o ricezione. Ciò è utile per identificare quali flussi di canale includono i dati utente e potrebbe richiedere l'elaborazione come la crittografia o la firma digitale.

Percorso delle uscite

Un percorso predefinito per l'ubicazione delle uscite del canale è definito nel file di configurazione client. Le uscite canale vengono caricate quando un canale viene inizializzato.

Su sistemi UNIX, Linux e Windows, un file di configurazione client viene aggiunto al sistema durante l'installazione del client WebSphere MQ MQI. In questo file è definito un percorso predefinito per l'ubicazione delle uscite del canale sul client, utilizzando la stanza:

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

dove *stringa* è un percorso file in un formato appropriato per la piattaforma

Quando un canale viene inizializzato, dopo una chiamata MQCONN o MQCONNX , viene eseguita la ricerca nel file di configurazione del client. La stanza ClientExitPath viene letta e vengono caricate tutte le uscite del canale specificate nella definizione del canale.

Uscite di sicurezza su una connessione client

È possibile utilizzare i programmi di uscita di sicurezza per verificare che il partner all'altra estremità di un canale sia autentico. Considerazioni speciali si applicano quando un'uscita di sicurezza viene applicata a una connessione client.

La Figura 20 a pagina 125 illustra l'utilizzo delle uscite di sicurezza in una connessione client, utilizzando il gestore di autorizzazioni oggetto WebSphere MQ per autenticare un utente. SecurityParmsPtr o SecurityParmsOffset è impostato nella struttura MQCNO sul client e ci sono uscite di sicurezza ad entrambe le estremità del canale. Una volta terminato il normale scambio di messaggi di sicurezza e quando il canale è pronto per l'esecuzione, la struttura MQCSP a cui si accede dal campo SecurityParms di

MQCXP viene passata all'exit di sicurezza sul client. Il tipo di exit è impostato su MQXR_SEC_PARMS. L'uscita di sicurezza può scegliere di non fare nulla per l'identificativo utente e la parola d'ordine, oppure può modificare uno o entrambi. I dati restituiti dall'uscita vengono quindi inviati all'estremità di connessione server del canale. La struttura MQCSP viene ricreata all'estremità della connessione server del canale e viene inoltrata all'uscita di sicurezza della connessione server a cui si accede dal campo SecurityParms di MQCXP. L'uscita di sicurezza riceve ed elabora questi dati. Questa elaborazione è in genere per annullare qualsiasi modifica apportata ai campi ID utente e password nell'uscita client, che vengono quindi utilizzati per autorizzare la connessione del gestore code. Alla struttura MQCSP risultante si fa riferimento utilizzando il Ptr SecurityParmsnella struttura MQCNO sul sistema del gestore code.

Se SecurityParmsPtr o SecurityParmsOffset sono impostati nella struttura MQCNO e c'è un'uscita di sicurezza ad una sola estremità del canale, l'uscita di sicurezza riceve ed elabora la struttura MQCSP. Le azioni come la crittografia non sono appropriate per una singola uscita utente, poiché non esiste alcuna uscita per eseguire l'azione complementare.

Se SecurityParmsPtr e SecurityParmsOffset non sono impostati nella struttura MQCNO e c'è un'uscita di sicurezza in una o in entrambe le estremità del canale, vengono richiamate l'uscita o le uscite di sicurezza. Entrambe le uscite di sicurezza possono restituire la propria struttura MQCSP, indirizzata tramite il Ptr SecurityParms; l'uscita di sicurezza non viene richiamata nuovamente fino a quando non viene terminata (ExitReason di MQXR_TERM). Il writer di uscita può liberare la memoria utilizzata per MQCSP in tale fase.

Quando un'istanza del canale di connessione server condivide più di una conversazione, il pattern di chiamate all'uscita di sicurezza è limitato alla seconda e alle successive conversazioni.

Per la prima conversazione, il pattern è lo stesso come se l'istanza del canale non stesse condividendo le conversazioni. Per le seconde e successive conversazioni, l'uscita di sicurezza non viene mai richiamata con MQXR_INIT, MQXR_INIT_SEC o MQXR_SEC_MSG. Viene richiamato con MQXR_SEC_PARMS.

In un'istanza del canale con conversazioni condivise, MQXR_TERM viene richiamato solo per l'ultima conversazione in esecuzione.

Ogni conversazione ha l'opportunità nel richiamo MQXR_SEC_PARMS dell'uscita per modificare MQCD; all'estremità della connessione server del canale questa funzione può essere utile per variare, ad esempio, i valori MCAUserIdentifier o LongMCAUserIdPtr prima che venga effettuata la connessione al gestore code.

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

Figura 20. Scambio avviato dalla connessione client con accordo per la connessione client utilizzando i parametri di sicurezza

Nota: Le applicazioni di uscita di sicurezza create prima della release di WebSphere MQ v7.1 potrebbero richiedere un aggiornamento. Per ulteriori informazioni, consultare Programmi di uscita di sicurezza del canale.

Identificazione della chiamata API in un programma di uscita di invio o ricezione

Quando si utilizzano i canali MQI per i client, il byte 10 del buffer dell'agent identifica la chiamata API in uso quando viene richiamata un'uscita di invio o ricezione. Ciò è utile per identificare quali flussi di canale includono i dati utente e potrebbe richiedere l'elaborazione come la crittografia o la firma digitale.

La seguente tabella mostra i dati che vengono visualizzati in byte 10 del flusso del canale quando viene elaborata una chiamata API.

Nota: Questi non sono gli unici valori di questo byte. Esistono altri valori **riservati** .

Tabella 20. Identificazione delle chiamate API

Chiamata API	**Valore del byte 10 per la richiesta**	**Valore del byte 10 per la risposta**
MQCONN “1” a pagina 126,“2” a pagina 126	X'81 '	'91'
MQDISC “1” a pagina 126	X'82 '	X' 92 '

Tabella 20. Identificazione delle chiamate API (Continua)

Chiamata API	**Valore del byte 10 per la richiesta**	**Valore del byte 10 per la risposta**
MQOPEN “3” a pagina 126	X'83 '	X' 93 '
MQCLOSE	84 '	'94'
MQGET “4” a pagina 126	X'85 '	X' 95 '
MQPUT “4” a pagina 126	X'86 '	X' 96 '
MQPUT1 richiesta “4” a pagina 126	X'87 '	X' 97 '
Richiesta MQSET	X'88 '	'98'
Richiesta MQINQ	X'89 '	X' 99 '
Richiesta MQCMIT	X'8A'	X'9A'
Richiesta MQBACK	'8B'	X'9B'
Richiesta MQSTAT	'8D'	X'9D'
Richiesta MQSUB	'8E'	'9E'
Richiesta MQSUBRQ	'8F'	'9F'
richiesta xa_start	X'A1'	X'B1'
richiesta xa_end	X'A2'	X'B2'
Richiesta xa_open	X'A3'	X'B3'
richiesta xa_close	X'A4'	'B4'
Richiesta xa_prepare	'A5'	X'B5'
richiesta xa_commit	'A6'	'B6'
richiesta x_rollback	X'A7'	X'B7'
richiesta xa_forget	'A8'	X'B8'
richiesta xa_recover	X'A9'	'B9'
Richiesta xa_complete	X'AA'	X'BA '

Note:

1. La connessione tra il server e il client viene avviata dall'applicazione client utilizzando MQCONN. Pertanto, per questo comando in particolare, esistono diversi altri flussi di rete. Lo stesso vale per MQDISC, che termina la connessione di rete.
2. MQCONNX viene trattato allo stesso modo di MQCONN per la connessione client - server.
3. Se viene aperto un elenco di distribuzione di grandi dimensioni, è possibile che vi sia più di un flusso di rete per ogni chiamata MQOPEN per passare tutti i dati richiesti all'MCA SVRCONN.
4. I messaggi di grandi dimensioni possono superare la dimensione del segmento di trasmissione. Se ciò si verifica, possono essere presenti molti flussi di rete risultanti da una singola chiamata API.

Connessione di un client a un gruppo di condivisione code

È possibile connettere un client a un gruppo di condivisione code creando un canale MQI tra un client e un gestore code su un server che è membro di un gruppo di condivisione code.

Un gruppo di condivisione code è formato da un insieme di gestori code che possono accedere allo stesso insieme di code condivise.

Un client inserito in una coda condivisa può connettersi a qualsiasi membro del gruppo di condivisione code. I vantaggi della connessione a un gruppo di condivisione code sono possibili aumenti della disponibilità di front-end e back-end e aumento della capacità. È possibile connettersi a un gestore code specifico o all'interfaccia generica.

La connessione diretta a un gestore code in un gruppo di condivisione code offre il vantaggio di poter inserire messaggi in una coda di destinazione condivisa, il che aumenta la disponibilità di backend.

La connessione all'interfaccia generica di un gruppo di condivisione code apre una sessione con uno dei gestori code del gruppo. Ciò aumenta la disponibilità di front-end, poiché il gestore code client può connettersi a qualsiasi gestore code nel gruppo. Connettersi al gruppo utilizzando l'interfaccia generica quando non si desidera connettersi ad un gestore code specifico all'interno del gruppo di condivisione code.

L'interfaccia generica può essere un nome gruppo WLM/DNS o un nome risorsa generico VTAM oppure un'altra interfaccia comune al gruppo di condivisione code.

Per connettersi all'interfaccia generica di un gruppo di condivisione code, è necessario creare definizioni di canale a cui può accedere qualsiasi gestore code del gruppo. Per fare ciò, è necessario disporre delle stesse definizioni su ciascun gestore code nel gruppo.

Definire il canale SVRCONN come segue:

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

Le definizioni di canale sul server sono memorizzate in un repository DB2 condiviso. Ogni gestore code nel gruppo di condivisione code effettua una copia locale della definizione, assicurando che ci si connetterà sempre al corretto canale di connessione server quando si emette una chiamata MQCONN o MQCONNX.

Definire il canale CLNTCONN come segue:

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

Poiché l'interfaccia generica del gruppo di condivisione code è memorizzata nel campo CONNAME nel canale di connessione client, è ora possibile connettersi a qualsiasi gestore code del gruppo e inserirlo nelle code condivise di proprietà di tale gruppo.

Concetti correlati

“Creazione di definizioni di canale” a pagina 127
Per connettersi all'interfaccia generica di un gruppo di condivisione code, è necessario creare definizioni di canale a cui può accedere qualsiasi gestore code del gruppo. Per fare ciò, è necessario disporre delle stesse definizioni su ciascun gestore code nel gruppo.

Creazione di definizioni di canale

Per connettersi all'interfaccia generica di un gruppo di condivisione code, è necessario creare definizioni di canale a cui può accedere qualsiasi gestore code del gruppo. Per fare ciò, è necessario disporre delle stesse definizioni su ciascun gestore code nel gruppo.

Definire il canale SVRCONN come segue:

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

Le definizioni di canale sul server sono memorizzate in un repository DB2 condiviso. Ogni gestore code nel gruppo di condivisione code effettua una copia locale della definizione, assicurando che ci si connetterà sempre al corretto canale di connessione server quando si emette una chiamata MQCONN o MQCONNX.

Definire il canale CLNTCONN come segue:

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

Poiché l'interfaccia generica del gruppo di condivisione code è memorizzata nel campo CONNAME nel canale di connessione client, è ora possibile connettersi a qualsiasi gestore code del gruppo e inserirlo nelle code condivise di proprietà di tale gruppo.

Configurazione di un client utilizzando un file di configurazione

Configurare i client utilizzando gli attributi in un file di testo. Questi attributi possono essere sovrascritti dalle variabili di ambiente o in altri modi specifici della piattaforma.

Configurare il IBM WebSphere MQ MQI client utilizzando un file di testo, simile al file di configurazione del gestore code, qm.ini, utilizzato su piattaforme UNIX and Linux . Il file contiene un numero di stanze, ognuna delle quali contiene un numero di righe nel formato **attribute-name**=*valore* .

In questa documentazione, si fa riferimento a questo file come al *WebSphere MQ*; il suo nome file è generalmente mqclient.ini, ma è possibile scegliere di assegnare un altro nome. Le informazioni di configurazione in questo file si applicano a tutte le piattaforme e ai client che utilizzano MQI, IBM WebSphere MQ classes for Java, IBM WebSphere MQ classes for JMS, IBM WebSphere MQ classes for .NETe XMS.

Anche se gli attributi nel file di configurazione IBM WebSphere MQ MQI client si applicano alla maggior parte dei client IBM WebSphere MQ , esistono alcuni attributi che non vengono letti dai client .NET e XMS .NET gestiti o dai client che utilizzano IBM WebSphere MQ classes for Java o IBM WebSphere MQ classes for JMS. Per ulteriori informazioni, consultare “Quali client IBM WebSphere MQ possono leggere ciascun attributo” a pagina 130.

Le funzioni di configurazione si applicano a tutte le connessioni effettuate da un'applicazione client a qualsiasi gestore code, piuttosto che essere specifiche di una singola connessione a un gestore code. Gli attributi relativi a una connessione a un singolo gestore code possono essere configurati in modo programmatico, ad esempio utilizzando una struttura MQCD o utilizzando una CCDT (Client Channel Definition Table).

Le variabili di ambiente che erano supportate nelle release di IBM WebSphere MQ precedenti alla Versione 7.0 continuano ad essere supportate e, se tale variabile di ambiente corrisponde a un valore equivalente nel file di configurazione del client, la variabile di ambiente sovrascrive il valore del file di configurazione del client.

Per un'applicazione client che utilizza IBM WebSphere MQ classes for JMS, è anche possibile sovrascrivere il file di configurazione client nei modi riportati di seguito:

- impostazione delle proprietà nel file di configurazione JMS
- impostazione delle proprietà di sistema Java, che sovrascrive anche il file di configurazione JMS

Per il client .NET, è anche possibile sovrascrivere il file di configurazione client e le variabili di ambiente equivalenti utilizzando il file di configurazione dell'applicazione .NET.

Notare che non è possibile impostare più connessioni del canale utilizzando il file di configurazione del client.

File di configurazione client di esempio

```
#* Module Name: mqclient.ini                                          *#
#* Type       : WebSphere MQ MQI client configuration file             *#
#  Function   : Define the configuration of a client                   *#
#*                                                                     *#
#*********************************************************************#
#* Notes      :                                                        *#
#* 1) This file defines the configuration of a client                  *#
#*                                                                     *#
#*********************************************************************#
```

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

TCP:
   Library1=DLLName1
   KeepAlive = Yes
   ClntSndBuffSize=32768
   ClntRcvBuffSize=32768
   Connect_Timeout=0

MessageBuffer:
   MaximumSize=-1
   Updatepercentage=-1
   PurgeTime=0

LU62:
   TPName
   Library1=DLLName1
   Library2=DLLName2

PreConnect:
    Module=amqldapi
    Function=myFunc
    Data=ldap://myLDAPServer.com:389/cn=wmq,ou=ibm,ou=com
    Sequence=1

CHANNELS:
 DefRecon=YES
 ServerConnectionParms=SALES.SVRCONN/TCP/hostname.x.com(1414)
```

Riferimenti correlati

“Ubicazione del file di configurazione client” a pagina 129
Un file di configurazione client IBM WebSphere MQ MQI può essere contenuto in diverse ubicazioni.

“Stanza CHANNELS del file di configurazione client” a pagina 138
Utilizzare la stanza CHANNELS per specificare le informazioni sui canali client.

“Stanza di percorso ClientExitdel file di configurazione del client” a pagina 140
Utilizzare la stanza ClientExitPath per specificare le ubicazioni predefinite delle uscite del canale sul client.

“LU62, NETBIOS e stanze SPX del file di configurazione client” a pagina 140
Solo su sistemi Windows, utilizzare queste stanze per specificare i parametri di configurazione per i protocolli di rete specificati.

“Stanza MessageBuffer del file di configurazione client” a pagina 141
Utilizzare la sezione MessageBuffer per specificare informazioni sui buffer di messaggi.

“Stanza SSL del file di configurazione client” a pagina 143
Utilizzare la stanza SSL per specificare le informazioni sull'utilizzo di SSL o TLS.

“Stanza TCP del file di configurazione client” a pagina 145
Utilizzare la stanza TCP per specificare i parametri di configurazione del protocollo di rete TCP.

“Utilizzo delle variabili di ambiente WebSphere MQ” a pagina 146
Questa sezione descrive le variabili di ambiente che è possibile utilizzare con applicazioni client WebSphere MQ MQI.

“Modifica delle informazioni di configurazione del gestore code” a pagina 436
Gli attributi qui descritti modificano la configurazione di un singolo gestore code. Sovrascrivono le impostazioni per WebSphere MQ.

Ubicazione del file di configurazione client

Un file di configurazione client IBM WebSphere MQ MQI può essere contenuto in diverse ubicazioni.

Un'applicazione client utilizza il seguente percorso di ricerca per individuare il file di configurazione del client IBM WebSphere MQ MQI:

1. L'ubicazione specificata dalla variabile di ambiente MQCLNTCF.

Il formato di questa variabile di ambiente è un URL completo. Ciò significa che il nome file potrebbe non essere necessariamente `mqclient.ini` e facilita l'inserimento del file su un file system collegato in rete.

Tieni presente quanto segue:

- I client C, .NET e XMS supportano solo il protocollo `file:` ; il protocollo `file:` viene assunto se la stringa URL non inizia con `protocol:`
- Per consentire JRE Java 1.4.2 , che non supportano la lettura delle variabili di ambiente, la variabile di ambiente MQCLNTCF può essere sovrascritta con una proprietà di sistema Java MQCLNTCF.

2. Un file denominato `mqclient.ini` nella directory di lavoro corrente dell'applicazione.
3. Un file denominato `mqclient.ini` nella directory di dati IBM WebSphere MQ per sistemi Windows, UNIX and Linux .

   Tieni presente quanto segue:

   - La directory di dati IBM WebSphere MQ non esiste su alcune piattaforme, ad esempio, IBM i e z/OS, o nei casi in cui il client è stato fornito con un altro prodotto.
   - Su sistemi UNIX and Linux , la directory è `/var/mqm`
   - Su piattaforme Windows , configurare la variabile di ambiente MQ_FILE_PATH durante l'installazione in modo che punti alla directory dei dati. Di solito è `C:\Program Files\IBM\WebSphere MQ`
   - Per consentire JRE Java 1.4.2 che non supportano le variabili di ambiente di lettura, è possibile sovrascrivere manualmente la variabile di ambiente MQ_FILE_PATH con una proprietà di sistema Java MQ_FILE_PATH.

4. Un file denominato `mqclient.ini` in una directory standard appropriata per la piattaforma e accessibile agli utenti:

   - Per tutti i client Java, questo è il valore della proprietà di sistema Java `user.home` .
   - Per client C su piattaforme UNIX and Linux , questo è il valore della variabile di ambiente HOME.
   - Per i client C su Windows , sono i valori concatenati delle variabili di ambiente HOMEDRIVE e HOMEPATH.

Nota: Per il client IBM WebSphere MQ per HP Integrity NonStop Server, il file `mqclient.ini` deve essere ubicato nel filesystem OSS. Le applicazioni Guardian devono collocare il file `mqclient.ini` nella directory di dati IBM WebSphere MQ o impostare la variabile di ambiente MQCLNTCF su un'ubicazione nel filesystem OSS.

Quali client IBM WebSphere MQ possono leggere ciascun attributo

La maggior parte degli attributi nel file di configurazione IBM WebSphere MQ MQI client può essere utilizzata dal client C e dai client .NET non gestiti. Tuttavia, esistono alcuni attributi che non vengono letti dai client .NET e XMS .NET gestiti o dai client che utilizzano IBM WebSphere MQ classes for Java o IBM WebSphere MQ classes for JMS.

Tabella 21. Quali attributi si applicano a ciascun tipo di client

Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestito.NET**	**GestitoXMS . NET**
Stanza CHANNELS						
CCSID	Il numero della serie di caratteri codificati da utilizzare.	Sì	No	No	Sì	Sì

Tabella 21. Quali attributi si applicano a ciascun tipo di client (Continua)

Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestito.NET**	**GestitoXMS . NET**
ChannelDefinitionDirectory	Il percorso della directory del file contenente la tabella di definizione del canale client.	Sì	No	No	Sì	Sì
File ChannelDefinition	Il nome del file contenente la tabella di definizione del canale client.	Sì	No	No	Sì	Sì
ReconDelay	Un'opzione di gestione per configurare il ritardo di riconnessione per i programmi client che possono riconnettersi automaticamente.	Sì	No	Sì	Sì	Sì
DefRecon	Un'opzione di gestione per abilitare i programmi client a riconnettersi automaticamente o per disabilitare la riconnessione automatica di un programma client che è stato scritto per riconnettersi automaticamente.	Sì	No	Sì	Sì	Sì

Tabella 21. Quali attributi si applicano a ciascun tipo di client (Continua)

Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestito.NET**	**GestitoXMS . NET**
MQReconnectTimeout	Il timeout in secondi per riconnettersi a un client.	Sì	No	No	Sì	No
ServerConnectionParametri	L'ubicazione del server IBM WebSphere MQ e il metodo di comunicazione da utilizzare.	Sì	No	No	Sì	Sì
Put1DefaultAlwaysSync	Controlla il comportamento della chiamata della funzione MQPUT1 con opzione `MQPMO_RESPONSE_AS_Q_DEF`.	Sì	Sì	Sì	Sì	Sì
StanzaClientExitPath						
ExitsDefaultPath	Specifica l'ubicazione delle uscite canale a 32 bit per i client.	Sì	No	No	Sì	Sì
ExitsDefaultPath64	Specifica l'ubicazione delle uscite del canali a 64 bit per i client.	Sì	No	No	Sì	Sì
JavaExitsClassPath	I valori da aggiungere al percorso classi quando viene eseguita un'uscita Java .	No	Sì	Sì	No	No
Stanza MessageBuffer						

Tabella 21. Quali attributi si applicano a ciascun tipo di client (Continua)

Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestito.NET**	**GestitoXMS .NET**
MaximumSize	La dimensione, in kilobyte, del buffer di lettura anticipata, nell'intervallo compreso tra 1 e 999 999.	Sì	Sì	Sì	Sì	Sì
PurgeTime	Intervallo, in secondi, dopo il quale vengono eliminati i messaggi rimasti nel buffer di lettura anticipata.	Sì	Sì	Sì	Sì	Sì
UpdatePercentage	Il valore percentuale di aggiornamento, nell'intervallo compreso tra 1 e 100, utilizzato per calcolare il valore di soglia per stabilire quando un'applicazione client effettua una nuova richiesta al server.	Sì	Sì	Sì	Sì	Sì
Stanza SSL						

Tabella 21. Quali attributi si applicano a ciascun tipo di client (Continua)

Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestito.NET**	**GestitoXMS . NET**
CDPCheckExtensions	Specifica se i canali SSL o TLS su questo gestore code tentano di controllare i server CDP denominati nelle estensioni certificato del punto CrlDistribution.	Sì	No	No	No	No
CertificateLabel	L'etichetta del certificato della definizione del canale.	Sì	No	No	No	No
PoliticaCertificateVal	Determina il tipo di convalida del certificato utilizzato.	Sì	No	No	No	No
ClientRevocationClientRevocation	Determina in che modo è configurato il controllo della revoca del certificato se la chiamata di connessione client utilizza un canale SSL/TLS.	Sì	No	No	No	No

Tabella 21. Quali attributi si applicano a ciascun tipo di client (Continua)

Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestito.NET**	**GestitoXMS . NET**
EncryptionPolicySuiteB	Determina se un canale utilizza la crittografia conforme a Suite - B e quale livello di potenza deve essere utilizzato.	Sì	No	No	No	No
OCSPAuthentication	Definisce il comportamento di IBM WebSphere MQ quando OCSP è abilitato e il controllo della revoca OCSP non è in grado di determinare lo stato della revoca del certificato.	Sì	No	No	No	No
OCSPCheckExtensions	Controlla se IBM WebSphere MQ agisce sulle estensioni del certificato di accesso AuthorityInfo .	Sì	No	No	No	No
SSLCryptoHardware	Imposta la stringa del parametro richiesta per configurare l'hardware crittografico PKCS #11 presente sul sistema.	Sì	No	No	No	No

Tabella 21. Quali attributi si applicano a ciascun tipo di client (Continua)

Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestito.NET**	**GestitoXMS . NET**
SSLFipsRequired	Specifica se devono essere utilizzati solo algoritmi certificati FIPS se la crittografia viene eseguita in IBM WebSphere MQ.	Sì	No	No	No	No
SSLHTTPProxyName	La stringa è il nome host o l'indirizzo di rete del server proxy HTTP che deve essere utilizzato da GSKit per i controlli OCSP.	Sì	No	No	No	No
SSLKeyRepository	L'ubicazione del repository di chiavi che contiene il certificato digitale dell'utente, in formato stem.	Sì	No	No	No	No
SSLKeyResetConteggio	Il numero di byte non crittografati inviati e ricevuti su un canale SSL o TLS prima che la chiave segreta venga rinegoziata.	Sì	No	No	No	No
Stanza TCP						

Tabella 21. Quali attributi si applicano a ciascun tipo di client (Continua)

Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestito.NET**	**GestitoXMS . NET**
ClntRcvBuffSize	La dimensione, in byte, del buffer di ricezione TCP/IP utilizzato dall'estremità client di un canale di connessione server di connessione client.	Sì	Sì	Sì	Sì	Sì
ClntSndBuffSize	La dimensione in byte del buffer di invio TCP/IP utilizzato dall'estremità client di un canale di connessione server di connessione client.	Sì	Sì	Sì	Sì	Sì
Timeout connessione	Il numero di secondi prima del timeout di un tentativo di connessione del socket.	Sì	Sì	Sì	No	No
IPAddressVersion	Specifica quale protocollo IP utilizzare per una connessione di canale.	Sì	No	No	Sì	Sì
KeepAlive	Attiva o disattiva la funzione KeepAlive .	Sì	Sì	Sì	Sì	Sì

Tabella 21. Quali attributi si applicano a ciascun tipo di client (Continua)						
Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestito.NET**	**GestitoXMS . NET**
Windows Library1	Solo su Windows , il nome della DLL dei socket TCP/IP.	Sì	No	No	No	No

Per HP Integrity NonStop Server, è possibile utilizzare le stanze TMF e TmfGateway per comunicare con TMF/Gateway.

Stanza CHANNELS del file di configurazione client

Utilizzare la stanza CHANNELS per specificare le informazioni sui canali client.

I seguenti attributi possono essere inclusi nella stanza CHANNELS:

CCSID=*numero*
Il numero della serie di caratteri codificati da utilizzare.

Il numero CCSID è equivalente al parametro di ambiente MQCCSID.

ChannelDefinitionDirectory=*percorso*
Il percorso della directory del file contenente la tabella di definizione del canale client.

Su sistemi Windows , il valore predefinito è la directory di installazione IBM WebSphere MQ , di solito `C:\Program Files\IBM\WebSphere MQ`. Su sistemi UNIX and Linux , il valore predefinito è `/var/mqm`.

Il percorso della directory ChannelDefinitionequivale al parametro di ambiente MQCHLLIB.

ChannelDefinitionFile=*nome file*|`AMQCLCHL.TAB`
Il nome del file contenente la tabella di definizione del canale client.

La tabella di definizione del canale client equivale al parametro di ambiente MQCHLTAB.

ReconDelay=(ritardo [, rand])(ritardo [, rand]) ...
L'attributo ReconDelay fornisce un'opzione amministrativa per configurare il ritardo di riconnessione per i programmi client che possono riconnettersi automaticamente. Ecco un esempio di configurazione:

```
ReconDelay=(1000,200)(2000,200)(4000,1000)
```

L'esempio mostrato definisce un ritardo iniziale di un secondo, più un intervallo casuale fino a 200 millisecondi. Il ritardo successivo è di due secondi più un intervallo casuale di un massimo di 200 millisecondi. Tutti i ritardi successivi sono di quattro secondi, più un intervallo casuale fino a 1000 millisecondi.

DefRecon=NO|YES|QMGR|DISABLED
L'attributo DefRecon fornisce un'opzione di gestione per abilitare i programmi client a riconnettersi automaticamente o per disabilitare la riconnessione automatica di un programma client che è stato scritto per riconnettersi automaticamente. È possibile scegliere di impostare quest' ultima opzione se un programma utilizza un'opzione, come `MQPMO_LOGICAL_ORDER`, che non è compatibile con la riconnessione.

L'interpretazione delle opzioni DefRecon dipende dall'impostazione di un valore `MQCNO_RECONNECT_*` nel programma client e dal valore impostato.

Se il programma client si connette utilizzando MQCONNo imposta l'opzione MQCNO_RECONNECT_AS_DEF utilizzando MQCONNX, il valore di riconnessione impostato da DefRecon diventa effettivo. Se nel programma non è impostato alcun valore di riconnessione o dall'opzione DefRecon , il programma client non viene riconnesso automaticamente.

La riconnessione automatica del client non è supportata dalle classi IBM WebSphere MQ per Java.

No
A meno che non venga sovrascritto da MQCONNX, il client non viene riconnesso automaticamente.

Sì
A meno che non venga sovrascritto da MQCONNX, il client si riconnette automaticamente.

QMGR
A meno che non venga sovrascritto da MQCONNX, il client si riconnette automaticamente, ma solo allo stesso gestore code. L'opzione QMGR ha lo stesso effetto di MQCNO_RECONNECT_Q_MGR.

Disabilitato
La riconnessione è disabilitata, anche se richiesta dal programma client utilizzando la chiamata MQI MQCONNX .

La riconnessione automatica del client dipende da due valori:

- L'opzione di riconnessione impostata nell'applicazione
- Valore DefRecon nel file mqclient.ini

Tabella 22. La riconnessione automatica dipende dai valori impostati nell'applicazione e nel file mqclient.ini

Valore DefRecon in mqclient.ini	**Opzioni di riconnessione impostate nell'applicazione**			
	MQCNO_RECONNECT	MQCNO_RECONNECT_Q_MGR	MQCNO_RECONNECT_AS_DEF	MQCNO_RECONNECT_DISABLED
No	Sì	QMGR	NO	NO
Sì	Sì	QMGR	Sì	NO
QMGR	Sì	QMGR	QMGR	NO
Disabilitato	NO	NO	NO	NO

MQReconnectTimeout
Il timeout in secondi per riconnettersi a un client. Il valore predefinito è 1800 secondi (30 minuti).

I client IBM WebSphere MQ classes for XMS .NET possono specificare un timeout per la riconnessione utilizzando la proprietà XMSC.WMQ_CLIENT_RECONNECT_TIMEOUT. Il valore predefinito per questa proprietà è 1800 secondi (30 minuti).

ServerConnectionParms
ServerConnectionParms è equivalente al parametro di ambiente MQSERVER e specifica il percorso del server IBM WebSphere MQ e il metodo di comunicazione da utilizzare. L'attributo parametri ServerConnectiondefinisce solo un canale semplice; non è possibile utilizzarlo per definire un canale SSL o un canale con uscite canale. È una stringa nel formato *ChannelName*/*TransportType*/*ConnectionName*, *ConnectionName* deve essere un nome di rete completo. *ChannelName* non può contenere la barra ("/") poiché questo carattere viene utilizzato per separare il nome del canale, il tipo di trasporto e il nome della connessione.

Quando si utilizzano i parametri ServerConnectionper definire un canale client, viene utilizzata una lunghezza massima di 100 MB. Pertanto, la dimensione massima del messaggio in vigore per il canale è il valore specificato nel canale SVRCONN sul server.

Tenere presente che è possibile effettuare una singola connessione del canale client. Ad esempio, se si dispone di due voci:

```
ServerConnectionParms=R1.SVRCONN/TCP/localhost(1963)
ServerConnectionParms=R2.SVRCONN/TCP/localhost(1863)
```

viene utilizzato solo il secondo.

Specificare *ConnectionName* come un elenco separato da virgole di nomi per il tipo di trasporto indicato. In genere, è richiesto un solo nome. È possibile fornire più *nomi host* per configurare più connessioni con le stesse proprietà. Le connessioni vengono tentate nell'ordine in cui sono specificate nell'elenco delle connessioni fino a quando non viene stabilita correttamente una connessione. Se nessuna connessione ha esito positivo, il client inizia nuovamente l'elaborazione. Gli elenchi di connessioni sono un'alternativa ai gruppi di gestori code per configurare le connessioni per i client ricollegabili.

Put1DefaultAlwaysSync=NO|SÌ
Controlla il comportamento della chiamata della funzione MQPUT1 con opzione MQPMO_RESPONSE_AS_Q_DEF.

NO
Se MQPUT1 è impostato con MQPMO_SYNCPOINT, si comporta come MQPMO_ASYNC_RESPONSE. Allo stesso modo, se MQPUT1 è impostato con MQPMO_NO_SYNCPOINT, si comporta come MQPMO_SYNC_RESPONSE. Questo è il valore predefinito.

Sì
MQPUT1 si comporta come se MQPMO_SYNC_RESPONSE fosse impostato, indipendentemente dal fatto che MQPMO_SYNCPOINT o MQPMO_NO_SYNCPOINT sia impostato.

Stanza di percorso ClientExitdel file di configurazione del client

Utilizzare la stanza ClientExitPath per specificare le ubicazioni predefinite delle uscite del canale sul client.

I seguenti attributi possono essere inclusi nella stanza Percorso ClientExit:

ExitsDefaultPath=*stringa*
Specifica l'ubicazione delle uscite canale a 32 bit per i client.

ExitsDefaultPath64=*stringa*
Specifica l'ubicazione delle uscite del canali a 64 bit per i client.

JavaExitsClassPath=*stringa*
I valori da aggiungere al percorso classi quando viene eseguita un'uscita Java. Ciò viene ignorato dalle uscite in qualsiasi altra lingua.

Nel file di configurazione JMS, il nomeClassPath di JavaExitsviene fornito come com.ibm.mq.cfgstandard. e questo nome completo viene utilizzato anche nella proprietà di sistema MQ V7.0 di Websphere. Nella versione 6.0 questo attributo è stato specificato utilizzando la proprietà di sistema com.ibm.mq.exitClasspath, documentata nel readme della versione 6.0 . l'utilizzo di com.ibm.mq.exitClasspath è obsoleto. Se sono presenti sia JavaExitsClassPath che exitClasspath , viene rispettato JavaExitsClassPath . Se è presente solo l'utilizzo exitClasspath , viene ancora rispettato in Websphere MQ V7.0.

LU62, NETBIOS e stanze SPX del file di configurazione client

Solo su sistemi Windows, utilizzare queste stanze per specificare i parametri di configurazione per i protocolli di rete specificati.

LU62

Utilizzare la stanza LU62 per specificare i parametri di configurazione del protocollo SNA LU 6.2 . I seguenti attributi possono essere inclusi in questa sezione:

Library1=*NomeDLL*|_WCPIC32
Il nome della DLL APPC.

Library2=*NomeDLL*|_WCPIC32
Lo stesso di Library1, utilizzato se il codice è memorizzato in due librerie separate.

TPName
Il nome TP da avviare sul sito remoto.

NETBIOS

Utilizzare la stanza NETBIOS per specificare i parametri di configurazione del protocollo NetBIOS . I seguenti attributi possono essere inclusi in questa sezione:

AdapterNum=*numero*|_0
Il numero dell'adattatore LAN.

Library1=*NomeDLL*|_NETAPI32
Il nome della DLL NetBIOS.

LocalName=*nome*
Il nome con cui questo computer è noto sulla LAN.

Equivale al parametro di ambiente MQNAME.

NumCmds=*numero*|1
Quanti comandi allocare.

NumSess=*numero*|1
Quante sessioni allocare.

SPX

Utilizzare la stanza SPX per specificare i parametri di configurazione del protocollo SPX. I seguenti attributi possono essere inclusi in questa sezione:

BoardNum=*numero*|_0
Il numero dell'adattatore LAN.

KeepAlive=YES|NO
Attivare o disattivare la funzione KeepAlive .

KeepAlive=YES fa sì che SPX controlli periodicamente che l'altra estremità della connessione sia ancora disponibile. In caso contrario, il canale viene chiuso.

Library1=*NomeDLL*|_WSOCK32.DLL
Il nome della DLL SPX.

Library2=*NomeDLL*|_WSOCK32.DLL
Lo stesso di Library1, utilizzato se il codice è memorizzato in due librerie separate.

Socket=*numero*|5E86
Il numero di socket SPX in notazione esadecimale.

Stanza MessageBuffer del file di configurazione client

Utilizzare la sezione MessageBuffer per specificare informazioni sui buffer di messaggi.

I seguenti attributi possono essere inclusi nella sezione MessageBuffer :

MaximumSize=*intero*|_1
La dimensione, in kilobyte, del buffer di lettura anticipata, nell'intervallo compreso tra 1 e 999 999.

Esistono i seguenti valori speciali:

-1
Il client determina il valore appropriato.

0
La lettura anticipata è disabilitata per il client.

PurgeTime=*intero*|__600

Intervallo, in secondi, dopo il quale vengono eliminati i messaggi rimasti nel buffer di lettura anticipata.

Se l'applicazione client sta selezionando i messaggi basati su MsgId o CorrelId , è possibile che il buffer di lettura anticipata contenga messaggi inviati al client con un MsgId o un CorrelIdprecedentemente richiesto. Questi messaggi vengono bloccati nel buffer di lettura anticipata fino a quando non viene emesso un MQGET con un MsgId o CorrelIdappropriato. È possibile eliminare i messaggi dal buffer di lettura anticipata impostando PurgeTime. Tutti i messaggi rimasti nel buffer di lettura anticipata per un periodo più lungo dell'intervallo di eliminazione vengono eliminati automaticamente. Questi messaggi sono già stati rimossi dalla coda sul gestore code, quindi, a meno che non vengano consultati, vengono persi.

L'intervallo valido è compreso tra 1 e 999 999 999 secondi o il valore speciale 0, che indica che non viene eseguita alcuna eliminazione.

UpdatePercentage=*intero*|__-1

Il valore percentuale di aggiornamento, nell'intervallo compreso tra 1 e 100, utilizzato per calcolare il valore di soglia per stabilire quando un'applicazione client effettua una nuova richiesta al server. Il valore speciale -1 indica che il client determina il valore appropriato.

Il client invia periodicamente una richiesta al server indicando la quantità di dati che l'applicazione client ha utilizzato. Una richiesta viene inviata quando il numero di byte, *n*, richiamati dal client tramite chiamate MQGET supera una soglia *T*. *n* viene reimpostato su zero ogni volta che viene inviata una nuova richiesta al server.

La soglia T è calcolata come segue:

```
T = Upper - Lower
```

Il valore superiore è uguale alla dimensione del buffer di lettura anticipata, specificata dall'attributo *MaximumSize* , in kilobyte. Il suo valore predefinito è 100 Kb.

Inferiore è inferiore a Superiore ed è specificato dall'attributo *UpdatePercentage* . Questo attributo è un numero compreso nell'intervallo tra 1 e 100 e ha un valore predefinito di 20. Inferiore è calcolato come segue:

```
Lower = Upper x UpdatePercentage / 100
```

Esempio 1:

Gli attributi MaximumSize e UpdatePercentage assumono i valori predefiniti di 100 Kb e 20 Kb.

Il client richiama MQGET per richiamare un messaggio e lo fa ripetutamente. Questa operazione continua fino a quando MQGET non ha utilizzato n byte.

Utilizzo del calcolo

```
T = Upper - Lower
```

T è (100 - 20) = 80 Kb.

Quindi, quando le chiamate MQGET hanno rimosso 80 Kb da una coda, il client effettua automaticamente una nuova richiesta.

Esempio 2:

Gli attributi MaximumSize assumono il valore predefinito di 100 Kb e viene scelto un valore di 40 per UpdatePercentage.

Il client richiama MQGET per richiamare un messaggio e lo fa ripetutamente. Questa operazione continua fino a quando MQGET non ha utilizzato n byte.

Utilizzo del calcolo

```
T = Upper - Lower
```

T è (100 - 40) = 60 Kb

Quindi, quando le chiamate MQGET hanno rimosso 60 Kb da una coda, il client effettua automaticamente una nuova richiesta. Ciò è più rapido rispetto all'ESEMPIO 1 in cui sono stati utilizzati i valori predefiniti.

Pertanto, la scelta di una soglia maggiore di *T* tende a ridurre la frequenza con cui le richieste vengono inviate dal client al server. Al contrario, la scelta di una soglia più piccola *T* tende ad aumentare la frequenza delle richieste inviate dal client al server.

Tuttavia, la scelta di una soglia elevata *T* può significare che il guadagno di prestazioni della lettura anticipata viene ridotto man mano che aumenta la possibilità che il buffer di lettura anticipata diventi vuoto. Quando ciò accade, una chiamata MQGET potrebbe dover essere sospesa, in attesa che i dati arrivino dal server.

Stanza SSL del file di configurazione client

Utilizzare la stanza SSL per specificare le informazioni sull'utilizzo di SSL o TLS.

I seguenti attributi possono essere inclusi nella stanza SSL:

CDPCheckExtensions=YES|NO
CDPCheckExtensions specifica se i canali SSL o TLS su questo gestore code tentano di controllare i server CDP denominati nelle estensioni del certificato CrlDistributionPoint.

Questo attributo può presentare i seguenti valori:

- YES: i canali SSL o TLS tentano di controllare i server CDP per determinare se un certificato digitale è revocato.
- NO: i canali SSL o TLS non tentano di verificare i server CDP. Questo è il valore predefinito.

CertificateLabel = *stringa*
L'etichetta del certificato della definizione del canale.

Questo attributo può essere letto da client C e .NET non gestiti.

CertificateValPolicy=*stringa*
Determina il tipo di convalida del certificato utilizzato.

ANY
Utilizzare qualsiasi politica di convalida del certificato supportata dalla libreria dei socket protetti sottostante. Questa è l'impostazione predefinita.

RFC5280
Utilizzare solo la convalida del certificato conforme allo standard RFC 5280.

ClientRevocationChecks = REQUIRED | OPTIONAL | DISABLED
Determina in che modo è configurato il controllo della revoca del certificato se la chiamata di connessione client utilizza un canale SSL/TLS. Vedere anche **OCSPAuthentication**.

Questo attributo può essere letto da client C e .NET non gestiti.

Questo attributo può presentare i seguenti valori:

OBBLIGATORIO (valore predefinito)
Tenta di caricare la configurazione della revoca del certificato da CCDT ed esegue il controllo della revoca come configurato. Se il file CCDT non può essere aperto o non è possibile convalidare il certificato (ad esempio, perché un server OCSP o CRL non è disponibile), la chiamata MQCONN ha esito negativo. Non viene eseguito alcun controllo di revoca se CCDT non contiene alcuna configurazione di revoca, ma ciò non causa l'esito negativo del canale.

Windows Sui sistemi Windows , è anche possibile utilizzare Active Directory per il controllo della revoca CRL. Non è possibile utilizzare Active Directory per il controllo della revoca OCSP.

Facoltativo
Come per REQUIRED, ma se non è possibile caricare la configurazione di revoca del certificato, il canale non ha esito negativo.

DISABILITATO
Non è stato effettuato alcun tentativo di caricare la configurazione di revoca del certificato da CCDT e non è stato eseguito alcun controllo di revoca del certificato.

Nota: Se si utilizza MQCONNX invece delle chiamate MQCONN, è possibile scegliere di fornire i record delle informazioni di autenticazione (MQAIR) tramite MQSCO. Il funzionamento predefinito con MQCONNX non ha quindi esito negativo se il file CCDT non può essere aperto, ma presuppone che si stia fornendo un MQAIR (anche se si sceglie di non farlo).

EncryptionPolicySuiteB=*stringa*
Determina se un canale utilizza la crittografia conforme a Suite - B e quale livello di potenza deve essere utilizzato. I valori possibili sono:

NESSUNO
La crittografia compatibile Suite - B non viene utilizzata. Questa è l'impostazione predefinita.

128_BIT,192_BIT
Imposta il livello di sicurezza su entrambi i livelli a 128 bit e 192 bit.

128_BIT
Imposta il livello di sicurezza a 128 bit.

192_BIT
Imposta il livello di sicurezza su 192 bit.

OCSPAuthentication=OPTIONAL|REQUIRED|WARN
Definisce il comportamento di WebSphere MQ quando OCSP è abilitato e il controllo della revoca OCSP non è in grado di determinare lo stato della revoca del certificato. Esistono tre valori possibili:

Facoltativo
Qualsiasi certificato con uno stato di revoca che non può essere determinato dal controllo OCSP viene accettato e non viene generato alcun avviso o messaggio di errore. La connessione SSL o TLS continua come se non fosse stato effettuato alcun controllo di revoca.

Obbligatorio
Il controllo OCSP deve produrre un risultato di revoca definitivo per ogni certificato SSL o TLS che viene controllato. Qualsiasi certificato SSL o TLS con uno stato di revoca che non può essere verificato viene rifiutato con un messaggio di errore. Se i messaggi di evento SSL del gestore code sono abilitati, viene generato un messaggio MQRC_CHANNEL_SSL_ERROR con un ReasonQualifier di MQRQ_SSL_HANDSHAKE_ERROR. La connessione è chiusa.

Questo è il valore predefinito.

WARN
Un'avvertenza viene riportata nei log degli errori del gestore code se un controllo della revoca OCSP non è in grado di determinare lo stato di revoca di un certificato SSL o TLS. Se i messaggi di evento SSL del gestore code sono abilitati, viene generato un messaggio MQRC_CHANNEL_SSL_WARNING con un ReasonQualifier di MQRQ_SSL_UNKNOWN_REVOCATION. La connessione può continuare

OCSPCheckExtensions=YES|NO
Controlla se WebSphere MQ agisce sulle estensioni del certificato AuthorityInfoAccess. Se il valore è impostato su NO, WebSphere MQ ignora le estensioni del certificato di accesso AuthorityInfoe non tenta un controllo di sicurezza OCSP. Il valore predefinito è Sì.

SSLCryptoHardware=*stringa*
Imposta la stringa del parametro richiesta per configurare l'hardware crittografico PKCS #11 presente sul sistema.

Specificare una stringa nel seguente formato: GSK_PKCS11=*percorso driver e nome file*;*etichetta token*;*password token*;*impostazione codifica simmetrica*;

Ad esempio: GSK_PKCS11=/usr/lib/pkcs11/
PKCS11_API.so;tokenlabel;passw0rd;SYMMETRIC_CIPHER_ON

Il percorso del driver è un percorso assoluto della libreria condivisa che fornisce il supporto per la scheda PKCS #11 . Il nome file del driver è il nome della libreria condivisa. Un esempio del valore

richiesto per il percorso del driver PKCS #11 e il nome file è `/usr/lib/pkcs11/PKCS11_API.so`. Per accedere alle operazioni di cifratura simmetrica tramite GSKit, specificare il parametro di impostazione della cifratura simmetrica. Il valore di questo parametro è:

SYMMETRIC_CIPHER_OFF
Non accedere alle operazioni di cifratura simmetrica. Questa è l'impostazione predefinita.

SIMMETRICA_CIFRA_ON
Accedere alle operazioni di cifratura simmetriche.

La lunghezza massima della stringa è 256 caratteri. Il valore predefinito è uno spazio vuoto. Se si specifica una stringa non nel formato corretto, viene generato un errore.

SSLFipsRequired=YES|_NO
Specifica se devono essere utilizzati solo algoritmi certificati FIPS se la crittografia viene eseguita in WebSphere MQ. Se l'hardware di crittografia è configurato, i moduli di crittografia utilizzati sono quei moduli forniti dal prodotto hardware. Questi potrebbero, o meno, essere certificati FIPS ad un particolare livello, a seconda del prodotto hardware in uso.

SSLHTTPProxyName=*stringa*
La stringa è il nome host o l'indirizzo di rete del server proxy HTTP che deve essere utilizzato da GSKit per i controlli OCSP. Questo indirizzo può essere seguito da un numero di porta facoltativo, racchiuso tra parentesi. Se non si specifica alcun numero, viene utilizza la porta HTTP predefinita (80). Sulle piattaforme HP-UX PA - RISC e Sun Solaris SPARC, e per i client a 32 bit su AIX, l'indirizzo di rete può essere solo un indirizzo IPv4 ; su altre piattaforme può essere un indirizzo IPv4 o IPv6 .

Questo attributo potrebbe essere necessario se, ad esempio, un firewall impedisce l'accesso all'URL del responder OCSP.

SSLKeyRepository=*nomepercorso*
L'ubicazione del repository di chiavi che contiene il certificato digitale dell'utente, in formato stem. In altre parole, include il percorso completo e il nome file senza estensione.

SSLKeyResetCount=*intero*|_0
Il numero di byte non crittografati inviati e ricevuti su un canale SSL o TLS prima che la chiave segreta venga rinegoziata.

Il valore deve essere compreso tra 0 e 999999999.

Il valore predefinito è 0, che significa che le chiavi segrete non vengono mai rinegoziate.

Se si specifica un valore compreso tra 1 e 32768, i canali SSL o TLS utilizzano un conteggio di reimpostazione della chiave segreta di 32768 (32Kb). Ciò per evitare un numero eccessivo di reimpostazioni della chiave, che si verificherebbe per i valori di reimpostazione della chiave segreta.

Stanza TCP del file di configurazione client

Utilizzare la stanza TCP per specificare i parametri di configurazione del protocollo di rete TCP.

I seguenti attributi possono essere inclusi nella stanza TCP:

ClntRcvBuffSize=*numero*|_32768
La dimensione, in byte, del buffer di ricezione TCP/IP utilizzato dall'estremità client di un canale di connessione server di connessione client. Un valore pari a zero indica che il sistema operativo gestirà le dimensioni del buffer, rispetto alle dimensioni del buffer fissate da WebSphere MQ.

ClntSndBuffSize=*numero*|_32768
La dimensione in byte del buffer di invio TCP/IP utilizzato dall'estremità client di un canale di connessione server di connessione client. Un valore pari a zero indica che il sistema operativo gestirà le dimensioni del buffer, rispetto alle dimensioni del buffer fissate da WebSphere MQ.

Connect_Timeout=*numero*
Il numero di secondi prima del timeout di un tentativo di connessione del socket; il valore predefinito è 0, a meno che il canale non sia stato configurato con un peso del canale client diverso da zero, nel qual caso il valore predefinito è 5.

IPAddressVersion=MQIPADDR_IPV4|MQIPADDR_IPV6
Specifica quale protocollo IP utilizzare per una connessione di canale.

Dispone dei valori di stringa possibili di MQIPADDR_IPV4 o MQIPADDR_IPV6. Questi valori hanno lo stesso significato di IPV4 e IPV6 in **ALTER QMGR IPADDRV**.

KeepAlive=YES|NO
Attivare o disattivare la funzione KeepAlive . KeepAlive=YES fa sì che TCP/IP controlli periodicamente che l'altra estremità della connessione sia ancora disponibile. In caso contrario, il canale viene chiuso.

Windows **Library1=*NomeDLL*|WSOCK32**
(Solo Windows) Il nome della DLL socket TCP/IP.

stanze TMF e TMF/Gateway

Il TMF/Gateway fornito da IBM WebSphere MQ viene eseguito in un ambiente Pathway. Utilizzare le stanze di TMF e TMF/Gateway per specificare i parametri di configurazione richiesti per il client IBM WebSphere MQ per HP Integrity NonStop Server per comunicare con TMF/Gateway.

Se si desidera utilizzare TMF, è necessario definire una stanza TMF e una stanza TmfGateway per ciascun gestore code con cui si sta comunicando. Tutti i valori sono derivati dalla configurazione.

Stanza TMF

PathMon=*nome*
Il nome del processo Pathmon definito che definisce le classi server per TMF/Gateway.

Stanza TmfGateway

I seguenti attributi possono essere inclusi in questa sezione:

QManager=*nome*
Il nome del gestore code.

Server=*nome*
Il nome della classe server per il TMF/Gateway configurato per tale gestore code.

Esempio

Di seguito è riportato un esempio di una stanza TMF definita con due stanze TmfGateway per due gestori code differenti su server differenti:

```
TMF:
   PathMon=$PSD1P

TmfGateway:
   QManager=MQ5B
   Server=MQ-MQ5B

TmfGateway:
   QManager=MQ5C
   Server=MQ-MQ5C
```

Utilizzo delle variabili di ambiente WebSphere MQ

Questa sezione descrive le variabili di ambiente che è possibile utilizzare con applicazioni client WebSphere MQ MQI.

È possibile utilizzare le variabili di ambiente nei modi seguenti:

- Impostare le variabili nel proprio profilo di sistema per effettuare una modifica permanente
- Immettere un comando dalla riga comandi per apportare una modifica solo per questa sessione
- Per assegnare a una o più variabili un determinato valore in base all'applicazione in esecuzione, aggiungere i comandi ad un file di script di comandi utilizzato dall'applicazione

WebSphere MQ utilizza i valori predefiniti per quelle variabili che non è stato impostato.

I comandi sono disponibili su tutte le piattaforme client WebSphere MQ MQI, se non diversamente specificato.

Per ogni variabile di ambiente, utilizzare il comando relativo alla piattaforma per visualizzare l'impostazione corrente o per reimpostare il valore di una variabile.

Ad esempio:

Impostazione o reimpostazione del valore di una variabile di ambiente		
Effetto	**Comando**	
	Windows	**Sistemi UNIX and Linux**
Rimuove la variabile	SET MQSERVER=	annulla impostazione MQSERVER
Visualizza l'impostazione corrente	SERVER MQSET	echo $MQSERVER
Visualizza tutte le variabili di ambiente per la sessione	set	set

Per informazioni sulle singole variabili, consultare i topic secondari riportati di seguito:

Concetti correlati

“Configurazione di un client utilizzando un file di configurazione” a pagina 128
Configurare i client utilizzando gli attributi in un file di testo. Questi attributi possono essere sovrascritti dalle variabili di ambiente o in altri modi specifici della piattaforma.

Riferimenti correlati

Variabili di ambiente

MQCCSID

MQCCSID specifica il numero della serie di caratteri codificati da utilizzare e sostituisce il valore CCSID con cui è stato configurato il server.

Per ulteriori informazioni, consultare Scelta del CCSID (coded character set identifier) del client o del server .

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Per Windows:

```
SET MQCCSID=number
```

- Per sistemi UNIX and Linux :

```
export MQCCSID=number
```

MQCERTVPOL

MQCERTVPOL specifica la politica di convalida del certificato utilizzata.

Per ulteriori informazioni sulle politiche di validazione dei certificati in WebSphere MQ, consultare Politiche di validazione dei certificati in WebSphere MQ.

Questa variabile di ambiente sovrascrive l'impostazione *CertificateValPolicy* nella sezione SSL del file ini del client. La variabile può essere impostata su uno dei due seguenti valori:

ANY
Utilizzare qualsiasi politica di convalida del certificato supportata dalla libreria dei socket protetti sottostante.

RFC5280
Utilizzare solo la convalida del certificato conforme allo standard RFC 5280.

Per impostare questa variabile, utilizzare uno dei seguenti comandi:

- Per Windows:

```
SET MQCERTVPOL=value
```

- Per sistemi UNIX and Linux :

```
export MQCERTVPOL=value
```

MQCHLLIB

MQCHLLIB specifica il percorso di directory del file contenente la tabella di definizione del canale client (CCDT). Il file viene creato sul server, ma può essere copiato sulla workstation client WebSphere MQ .

Se MQCHLLIB non è impostato, il percorso per il client assume il valore predefinito:

- Windows Per Windows: *MQ_INSTALLATION_PATH*
- UNIX Linux Per i sistemi UNIX and Linux : /var/mqm/

Per i comandi **crtmqm** e **strmqm** , il percorso assume il valore predefinito di una delle due serie di percorsi. Se *datapath* è impostato, il percorso assume il valore predefinito di uno dei primi set. Se *datapath* non è impostato, il percorso assume il valore predefinito di uno della seconda serie.

- Windows Per Windows: *datapath*\@ipcc
- UNIX Linux Per i sistemi UNIX e Linux: *datapath*/@ipcc

Oppure:

- Windows Per Windows: *MQ_INSTALLATION_PATH*\data\qmgrs*qmgrname*\@ipcc
- UNIX Linux Per i sistemi UNIX and Linux : /prefix/qmgrs/*qmgrname*/@ipcc

dove:

- *MQ_INSTALLATION_PATH* rappresenta la directory di livello superiore in cui è installato IBM WebSphere MQ .
- Se presente, *datapath* è il valore di DataPath definito nella stanza del gestore code.
- *prefix* è il valore del prefisso definito nella stanza del gestore code. Il prefisso è generalmente /var/mqm su piattaforme UNIX e Linux.
- *qmgrname* è il valore dell'attributo Directory definito nella stanza del gestore code. Il valore potrebbe essere diverso dal nome del gestore code effettivo. Il valore potrebbe essere stato modificato per sostituire i caratteri speciali.
- La stanza del gestore code è definita nel file mqs.ini su UNIXe Linuxe nel registro su Windows

Note:

1. Se impostato, MQCHLLIB sovrascrive il percorso utilizzato per individuare la CCDT.
2. Le variabili di ambiente, come ad esempio MQCHLLIB, possono essere indirizzate a un processo o a un lavoro o a livello di sistema, in un modo specifico per la piattaforma.
3. Se si imposta MQCHLLIB a livello di sistema su un server, questo imposta lo stesso percorso al file CCDT per tutti i gestori code sul server. Se non si imposta la variabile di ambiente MQCHLLIB , il percorso è diverso per ciascun gestore code. I gestori code leggono il valore di MQCHLLIB, se impostato, sul comando **crtmqm** o **strmqm** .
4. Se si creano più gestori code su un server, la distinzione è importante, per il seguente motivo. Se si imposta MQCHLLIB a livello di sistema, ogni gestore code aggiorna lo stesso file CCDT. Il file contiene

le definizioni di connessione client da tutti i gestori code sul server. Se la stessa definizione esiste su più gestori code, ad esempio SYSTEM.DEF.CLNTCONN , il file contiene la definizione più recente. Quando si crea un gestore code, se MQCHLLIB è impostato, SYSTEM.DEF.CLNTCONN viene aggiornato in CCDT. L'aggiornamento sovrascrive il SYSTEM.DEF.CLNTCONN creato da un gestore code differente. Se è stata modificata la precedente definizione, le modifiche vengono perse. Per questo motivo, è necessario considerare la ricerca di alternative all'impostazione di MQCHLLIB come una variabile di ambiente a livello di sistema sul server.

5. L'opzione NOREPLACE MQSC e PCF su una definizione di connessione client non controlla il contenuto del file CCDT. Una definizione di canale di connessione client con lo stesso nome precedentemente creato, ma non da questo gestore code, viene sostituita, indipendentemente dall'opzione NOREPLACE . Se la definizione è stata precedentemente creata dallo stesso gestore code, la definizione non viene sostituita.
6. Il comando **rcrmqobj** `-t clchltab` elimina e ricrea il file CCDT. Il file viene ricreato con solo le definizioni di connessione client create sul gestore code su cui è in esecuzione il comando.
7. Altri comandi che aggiornano CCDT modificano solo i canali di connessione client che hanno lo stesso nome di canale. Altri canali di connessione client nel file non vengono modificati.
8. Il percorso per MQCHLLIB non richiede virgolette.

Esempi

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Windows Per Windows:

```
SET MQCHLLIB=pathname
```

  Ad esempio:

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

- UNIX Linux Per sistemi UNIX and Linux :

```
export MQCHLLIB=pathname
```

MQCHLTAB

MQCHLTAB specifica il nome del file contenente la tabella di definizione del canale client (ccdt). Il nome file predefinito è AMQCLCHL.TAB.

Per informazioni sulla posizione della tabella di definizione del canale client su un server, consultare “Tabella definizione canale client” a pagina 118.

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Su Windows:

```
SET MQCHLTAB=filename
```

- Su sistemi UNIX and Linux :

```
export MQCHLTAB=filename
```

Ad esempio:

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

Come per il client, la variabile di ambiente MQCHLTAB sul server specifica il nome della tabella di definizione del canale client.

MQIPADRV

MQIPADDRV specifica quale protocollo IP utilizzare per una connessione del canale. Ha i valori di stringa possibili di "MQIPADDR_IPV4" o "MQIPADDR_IPV6". Questi valori hanno lo stesso significato di IPV4 e IPV6 in ALTER QMGR IPADDRV. Se non è impostato, viene utilizzato "MQIPADDR_IPV4".

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Per Windows:

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

- Per sistemi UNIX and Linux :

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

NOME

MQNAME specifica il nome NetBIOS locale che i processi WebSphere MQ possono utilizzare.

Consultare “Definizione di una connessione NetBIOS su Windows” a pagina 89 per una descrizione completa e per le regole di precedenza sul client e sul server.

Per impostare questa variabile utilizzare questo comando:

```
SET MQNAME=Your_env_Name
```

Ad esempio:

```
SET MQNAME=CLIENT1
```

NetBIOS su alcune piattaforme richiede un nome differente (impostato da MQNAME) per ogni applicazione se si stanno eseguendo più applicazioni WebSphere MQ contemporaneamente sul client WebSphere MQ MQI.

SERVER MQT

La variabile di ambiente MQSERVER viene utilizzata per definire un canale minimo. MQSERVER specifica l'ubicazione del server WebSphere MQ e il metodo di comunicazione da utilizzare.

Non è possibile utilizzare MQSERVER per definire un canale SSL o un canale con uscite canale. Per i dettagli su come definire un canale SSL, consultare Protezione dei canali con SSL.

ConnectionName deve essere un nome di rete completo. *ChannelName* non può contenere il carattere barra (/) perché questo carattere viene utilizzato per separare il nome del canale, il tipo di trasporto e il nome della connessione. Quando la variabile di ambiente MQSERVER viene utilizzata per definire un canale del client, viene utilizzata una lunghezza massima del messaggio (MAXMSGL) di 100 MB. Pertanto, la dimensione massima del messaggio in vigore per il canale è il valore specificato nel canale SVRCONN sul server.

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Per Windows:

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

- Per sistemi UNIX and Linux :

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

TransportType può essere uno dei valori riportati di seguito, a seconda della piattaforma client IBM WebSphere MQ :

- LU62
- TCP
- NETBIOS
- SPX

ConnectionName può essere un elenco separato da virgole di nomi di connessione. I nomi di connessione nell'elenco vengono utilizzati in modo simile a più connessioni in una tabella di connessioni client. L'elenco *ConnectionName* potrebbe essere utilizzato come alternativa ai gruppi di gestori code per specificare più connessioni per il client da provare. Se si configura un gestore code a più istanze, è possibile utilizzare un elenco *ConnectionName* per specificare diverse istanze del gestore code.

Porta predefinita TCP/IP

Per impostazione predefinita, per TCP/IP, WebSphere MQ presume che il canale sarà connesso alla porta 1414.

È possibile modificare questo valore:

- Aggiunta del numero di porta tra parentesi come ultima parte di ConnectionName:
  - Per Windows:

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

  - Per sistemi UNIX and Linux :

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

- Modifica del file `mqclient.ini` aggiungendo il numero di porta al nome del protocollo, ad esempio:

  ```
  TCP:
  port=2001
  ```

- Aggiunta di WebSphere MQ al file dei servizi come descritto in “Utilizzo del listener TCP/IP” a pagina 95.

Socket predefinito SPX

Per impostazione predefinita, per SPX, WebSphere MQ presume che il canale sarà connesso al socket 5E86.

È possibile modificare questo valore:

- Aggiunta del numero socket tra parentesi come ultima parte di ConnectionName:

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

  Per connessioni SPX, specificare ConnectionName e socket nel formato `network.node(socket)`. Se il client WebSphere MQ e il server si trovano sulla stessa rete, non è necessario specificare la rete. Se si utilizza il socket predefinito, non è necessario specificarlo.

- Modifica del file `qm.ini` aggiungendo il numero di porta al nome del protocollo, ad esempio:

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

Utilizzo di MQSERVER

Se si utilizza la variabile di ambiente MQSERVER per definire il canale tra la macchina client MQI WebSphere MQ e una macchina server, questo è l'unico canale disponibile per l'applicazione e non viene effettuato alcun riferimento alla CCDT (client channel definition table).

In questa situazione, il programma listener in esecuzione sulla macchina server determina il gestore code a cui si connetterà l'applicazione. Sarà lo stesso gestore code a cui è connesso il programma listener.

Se la richiesta MQCONN o MQCONNX specifica un gestore code diverso da quello a cui è connesso il listener oppure se il parametro MQSERVER *TransportType* non è riconosciuto, la richiesta MQCONN o MQCONNX ha esito negativo con codice di ritorno MQRC_Q_MGR_NAME_ERROR.

Sui sistemiUNIX and Linux , è possibile definire MQSERVER come in uno dei seguenti esempi:

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

Tutte le richieste MQCONN o MQCONNX tentano di utilizzare il canale definito a meno che non sia stato fatto riferimento a una struttura MQCD dalla struttura MQCNO fornita a MQCONNX, nel qual caso il canale specificato dalla struttura MQCD ha la priorità su qualsiasi valore specificato dalla variabile di ambiente MQSERVER.

La variabile di ambiente MQSERVER ha la precedenza su qualsiasi definizione di canale client indicata da MQCHLLIB e MQCHLTAB.

Annullamento di MQSERVER

Per annullare MQSERVER e tornare alla tabella di definizione del canale client indicata da MQCHLLIB e MQCHLTAB, immettere quanto segue:

- Su Windows:

```
SET MQSERVER=
```

- Su sistemi UNIX and Linux :

```
unset MQSERVER
```

CCRYMQSSL

MQSSLCRYP contiene una stringa di parametri che consente di configurare l'hardware crittografico presente sul sistema. I valori consentiti sono gli stessi del parametro SSLCRYP del comando ALTER QMGR.

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Su sistemi Windows :

```
SET MQSSLCRYP=string
```

- Su sistemi UNIX and Linux :

```
export MQSSLCRYP=string
```

Riferimenti correlati
parametro **ALTER QMGR** command **SSLCRYP**

FIPS MQSSL

MQSSLFIPS specifica se devono essere utilizzati solo algoritmi certificati FIPS se la codifica viene eseguita in WebSphere MQ. I valori sono gli stessi del parametro SSLFIPS del comando ALTER QMGR.

L'utilizzo di algoritmi certificati FIPS è influenzato dall'utilizzo dell'hardware di crittografia, consultare Specifica che solo i CipherSpec CipherSpecs vengono utilizzati al runtime sul client MQI.

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Su sistemi Windows :

```
SET MQSSLFIPS=YES|NO
```

- Su sistemi UNIX and Linux :

```
export MQSSLFIPS=YES|NO
```

Il valore predefinito è NO.

MQSSLKEYR

MQSSLKEYR specifica l'ubicazione del repository delle chiavi che contiene il certificato digitale appartenente all'utente, in formato di radice. Il formato stem indica che include il percorso completo e il nome file senza un'estensione. Per i dettagli completi, consultare il parametro SSLKEYR del comando ALTER QMGR.

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Su sistemi Windows :

```
SET MQSSLKEYR=pathname
```

- Su sistemi UNIX and Linux :

```
export MQSSLKEYR=pathname
```

Non è impostato alcun valore predefinito.

MQSSLPROX

MQSSLPROXY specifica il nome host e il numero porta del server proxy HTTP che deve essere utilizzato da GSKit per i controlli OCSP.

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Su sistemi Windows :

```
SET MQSSLPROXY=string
```

- Su sistemi UNIX and Linux :

```
export MQSSLPROXY="string"
```

La stringa è il nome host o l'indirizzo di rete del server proxy HTTP che deve essere utilizzato da GSKit per i controlli OCSP. Questo indirizzo può essere seguito da un numero di porta facoltativo, racchiuso tra parentesi. Se non si specifica alcun numero, viene utilizza la porta HTTP predefinita (80).

Ad esempio, su sistemi UNIX and Linux , è possibile utilizzare uno dei seguenti comandi:

-
```
export MQSSLPROXY="proxy.example.com(80)"
```

-
```
export MQSSLPROXY="127.0.0.1"
```

RESET MQSSL

MQSSLRESET rappresenta il numero di byte non crittografati inviati e ricevuti su un canale SSL o TLS prima che la chiave segreta venga rinegoziata.

Per ulteriori informazioni sulla rinegoziazione della chiave segreta, vedi Reimpostazione delle chiavi segrete SSL e TLS .

Può essere impostato su un valore intero compreso tra 0 e 999 999 999. Il valore predefinito è 0, che indica che le chiavi segrete non vengono mai rinegoziate. Se si specifica un conteggio di reimpostazione della chiave segreta SSL o TLS compreso tra 1 byte e 32 KB, i canali SSL o TLS utilizzano un conteggio di reimpostazione della chiave segreta di 32 KB. Questo conteggio di reimpostazioni segrete serve ad evitare un numero eccessivo di reimpostazioni di chiavi che si verificherebbe per valori di reimpostazione di chiavi segrete SSL o TLS di piccole dimensioni.

Per impostare questa variabile utilizzare uno dei seguenti comandi:

- Su sistemi Windows :

```
SET MQSSLRESET=integer
```

- Su sistemi UNIX and Linux :

```
export MQSSLRESET=integer
```

Controllo della pubblicazione / sottoscrizione in coda

È possibile avviare, arrestare e visualizzare lo stato della pubblicazione / sottoscrizione in coda. È inoltre possibile aggiungere e rimuovere i flussi e aggiungere ed eliminare i gestori code da una gerarchia broker.

Consultare i seguenti argomenti secondari per ulteriori informazioni sul controllo della pubblicazione / sottoscrizione accodata:

Impostazione degli attributi dei messaggi di pubblicazione / sottoscrizione accodati

Si controlla il funzionamento di alcuni attributi dei messaggi di pubblicazione / sottoscrizione utilizzando gli attributi del gestore code. Gli altri attributi controllati nella stanza *Broker* del file `qm.ini` .

Informazioni su questa attività

È possibile impostare i seguenti attributi di pubblicazione / sottoscrizione: per i dettagli, vedere Parametri del gestore code

Tabella 23. Parametri di configurazione di pubblicazione / sottoscrizione

Descrizione	**Nome parametro MQSC**
Conteggio tentativi messaggi di comando	**PSRTYCNT**
Elimina messaggio di input di comando non consegnabile	**PSNPMSG**
Comportamento che segue il messaggio di risposta del comando non distribuibile	**PSNPRES**
Elabora i messaggi di comando nel punto di sincronizzazione	**PSSYNCPT**

La stanza Broker viene utilizzata per gestire le seguenti impostazioni di configurazione:

- `PersistentPublishRetry=yes | force`

  Se si specifica `Sì`, se una pubblicazione di un messaggio persistente tramite l'interfaccia di pubblicazione / sottoscrizione in coda ha esito negativo e non è stata richiesta alcuna risposta negativa, l'operazione di pubblicazione viene ritentata.

  Se è stato richiesto un messaggio di risposta negativa, la risposta negativa viene inviata e non si verificano ulteriori tentativi.

Se si specifica Forza, se una pubblicazione di un messaggio persistente tramite l'interfaccia di pubblicazione / sottoscrizione in coda non riesce, l'operazione di pubblicazione viene ritentata fino a quando non viene elaborata correttamente. Non viene inviata alcuna risposta negativa.

- NonPersistentPublishRetry= sì | force

  Se si specifica Sì, se una pubblicazione di un messaggio non persistente attraverso l'interfaccia di pubblicazione / sottoscrizione in coda ha esito negativo e non è stata richiesta alcuna risposta negativa, l'operazione di pubblicazione viene ritentata.

  Se è stato richiesto un messaggio di risposta negativa, la risposta negativa viene inviata e non si verificano ulteriori tentativi.

  Se è stato specificato Forza, se una pubblicazione di un messaggio non persistente tramite l'interfaccia di pubblicazione / sottoscrizione in coda ha esito negativo, l'operazione di pubblicazione viene ritentata fino a quando non viene elaborata correttamente. Non viene inviata alcuna risposta negativa.

  Nota: Se si desidera abilitare questa funzionalità per i messaggi non persistenti, oltre a impostare il valore NonPersistentPublishRetry , è necessario assicurarsi che l'attributo del gestore code **PSSYNCPT** sia impostato su Sì.

  Questa operazione potrebbe anche avere un impatto sulle prestazioni dell'elaborazione delle pubblicazioni non persistenti poiché **MQGET** dalla coda STREAM ora si verifica nel punto di sincronizzazione.

- PublishBatchDimensione =*numero*

  Il broker normalmente elabora i messaggi di pubblicazione all'interno del punto di sincronizzazione. Può essere inefficiente eseguire il commit di ciascuna pubblicazione singolarmente e, in alcune circostanze, il broker può elaborare più messaggi di pubblicazione in una singola unità di lavoro. Questo parametro specifica il numero massimo di messaggi di pubblicazione che possono essere elaborati in una singola unità di lavoro

  Il valore predefinito per PublishBatchDimensione è 5.

- PublishBatchIntervallo =*numero*

  Il broker normalmente elabora i messaggi di pubblicazione all'interno del punto di sincronizzazione. Può essere inefficiente eseguire il commit di ciascuna pubblicazione singolarmente e, in alcune circostanze, il broker può elaborare più messaggi di pubblicazione in una singola unità di lavoro. Questo parametro specifica il tempo massimo (in millisecondi) tra il primo messaggio in un batch e qualsiasi pubblicazione successiva inclusa nello stesso batch.

  Un intervallo batch di 0 indica che è possibile elaborare fino a PublishBatchDimensione messaggi, purché i messaggi siano immediatamente disponibili.

  Il valore predefinito per PublishBatchIntervallo è zero.

Procedura

Utilizzare WebSphere MQ Explorer, comandi programmabili o il comando **runmqsc** per modificare gli attributi del gestore code che controllano il funzionamento della pubblicazione / sottoscrizione.

Esempio

PSNPRES ALTER QMGR (SAFE)

Avvio della pubblicazione / sottoscrizione accodata

Prima di iniziare

Leggere la descrizione di PSMODE per comprendere le tre modalità di pubblicazione / sottoscrizione:

- COMPAT

- Disabilitato
- Abilitato

Nota: Se è stata eseguita la migrazione da Version 6.0 , è necessario utilizzare **strmqbrk** per migrare lo stato del broker di pubblicazione / sottoscrizione di Version 6.0 se si sta utilizzando un gestore code aggiornato. Ciò non si applica a z/OS.

Informazioni su questa attività

Impostare l'attributo QMGR PSMODE per avviare l'interfaccia di pubblicazione / sottoscrizione accodata (nota anche come broker) o il motore di pubblicazione / sottoscrizione (noto anche come pubblicazione / sottoscrizione versione 7) o entrambi. Per avviare la pubblicazione / sottoscrizione accodata è necessario impostare PSMODE su ENABLED. Il valore predefinito è ENABLED.

Procedura

Utilizzare WebSphere MQ Explorer o il comando **runmqsc** per abilitare l'interfaccia di pubblicazione / sottoscrizione accodata, se l'interfaccia non è già abilitata.

Esempio

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

Operazioni successive

WebSphere MQ elabora i comandi di pubblicazione / sottoscrizione accodati e le chiamate MQI (Message Queue Interface) di pubblicazione / sottoscrizione.

Arresto della pubblicazione / sottoscrizione in coda

Prima di iniziare

La pubblicazione / sottoscrizione accodata è obsoleta.

Leggere la descrizione di PSMODE per comprendere le tre modalità di pubblicazione / sottoscrizione:

- COMPAT
- DISABILITATO
- Abilitato

Informazioni su questa attività

Impostare l'attributo PSMODE QMGR per arrestare l'interfaccia di pubblicazione / sottoscrizione accodata (nota anche come broker) o il motore di pubblicazione / sottoscrizione (noto anche come pubblicazione / sottoscrizione versione 7) o entrambi. Per arrestare la pubblicazione / sottoscrizione in coda è necessario impostare PSMODE su COMPAT. Per arrestare completamente il motore di pubblicazione / sottoscrizione, impostare PSMODE su DISABLED.

Procedura

Utilizzare WebSphere MQ Explorer o il comando **runmqsc** per disabilitare l'interfaccia di pubblicazione / sottoscrizione accodata.

Esempio

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

Aggiunta di uno stream

È possibile aggiungere i flussi manualmente in modo che coesistano con i flussi migrati dai gestori code Version 6.0 .

Prima di iniziare

Familiarizzare con il modo in cui operano i flussi di pubblicazione / sottoscrizione leggendo l'argomento, Flussi e argomenti.

Informazioni su questa attività

Utilizzare il comando PCF, **runmqsc**o IBM WebSphere MQ Explorer per eseguire queste operazioni.

Nota: È possibile eseguire i passi 1 e 2 in qualsiasi ordine. Eseguire il passo 3 solo dopo che i passi 1 e 2 sono stati entrambi completati.

Procedura

1. Definire una coda locale con lo stesso nome del flusso Version 6.0 .
2. Definire un argomento locale con lo stesso nome del flusso Version 6.0 .
3. Aggiungere il nome della coda all'elenco nomi, SYSTEM.QPUBSUB.QUEUE.NAMELIST
4. Ripetere le operazioni per tutti i gestori code in Version 7.1 o superiore che si trovano nella gerarchia di pubblicazione / sottoscrizione.

Aggiunta 'Sport'

Nell'esempio di condivisione del flusso 'Sport', i gestori code Version 6.0 e Version 7.1 operano nella stessa gerarchia di pubblicazione / sottoscrizione. I gestori code Version 6.0 condividono un flusso denominato 'Sport'. L'esempio mostra come creare una coda e un argomento su Version 7.1 gestori code denominati 'Sport', con una stringa argomento 'Sport' condivisa con il flusso versione 6 'Sport'.

Un' Version 7.1 applicazione di pubblicazione, pubblicazione nell'argomento 'Sport', con la stringa di argomenti 'Soccer/Results' , crea la stringa di argomenti risultante 'Sport/Soccer/Results' . Sui gestori code Version 7.1 , i sottoscrittori dell'argomento 'Sport', con stringa argomento 'Soccer/Results' ricevono la pubblicazione.

Sui gestori code Version 6.0 , i sottoscrittori del flusso 'Sport' , con la stringa di argomenti 'Soccer/Results' ricevono la pubblicazione.

```
runmqsc QM1
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM1.
define qlocal('Sport')
     1 : define qlocal('Sport')
AMQ8006: WebSphere MQ queue created.
define topic('Sport') topicstr('Sport')
     2 : define topic('Sport') topicstr('Sport')
AMQ8690: WebSphere MQ topic created.
alter namelist(SYSTEM.QPUBSUB.QUEUE.NAMELIST) NAMES('Sport', 'SYSTEM.BROKER.DEFAULT.STREAM',
'SYSTEM.BROKER.ADMIN.STREAM')
     3 : alter namelist(SYSTEM.QPUBSUB.QUEUE.NAMELIST) NAMES('Sport',
'SYSTEM.BROKER.DEFAULT.STREAM', 'SYSTEM.BROKER.ADMIN.STREAM')
AMQ8551: WebSphere MQ namelist changed.
```

Nota: È necessario fornire sia i nomi esistenti nell'oggetto elenco nomi, sia i nuovi nomi che si stanno aggiungendo al comando **alter namelist** .

Operazioni successive

Le informazioni sul flusso vengono trasmesse ad altri broker nella gerarchia.

Se un broker è Version 6.0, gestirlo come un broker Version 6.0 . In altre parole, è possibile creare manualmente la coda di flusso o consentire al broker di creare dinamicamente la coda di flusso quando è necessaria. La coda è basata sulla definizione di coda modello, SYSTEM.BROKER.MODEL.STREAM.

Se un broker è Version 7.1, è necessario configurare manualmente ciascun gestore code Version 7.1 nella gerarchia.

Eliminazione di uno stream

È possibile eliminare un flusso da un gestore code IBM WebSphere MQ Version 7.1o successivo.

Prima di iniziare

L'utilizzo della pubblicazione / sottoscrizione in coda è obsoleto in IBM WebSphere MQ Version 7.1.

Prima di eliminare un flusso, è necessario verificare che non vi siano sottoscrizioni rimanenti al flusso e disattivare tutte le applicazioni che utilizzano il flusso. Se le pubblicazioni continuano a fluire in un flusso eliminato, è necessario un notevole sforzo di gestione per ripristinare il sistema ad uno stato di funzionamento pulito.

Informazioni su questa attività

Per istruzioni sull'eliminazione del flusso da qualsiasi gestore code Version 6.0 a cui è connesso, consultare Eliminazione di un flusso (ps11870_.htm nella documentazione di v6.0).

Procedura

1. Trovare tutti i broker connessi che ospitano questo stream.
2. Annullare tutte le sottoscrizioni al flusso su tutti i broker.
3. Rimuovere la coda (con lo stesso nome del flusso) dall'elenco nomi, SYSTEM.QPUBSUB.QUEUE.NAMELIST.
4. Eliminare o eliminare tutti i messaggi dalla coda con lo stesso nome del flusso.
5. Cancellare la coda con lo stesso nome del flusso.
6. Eliminare l'oggetto argomento associato.

Operazioni successive

1. Ripetere i passi da 3 a 5 su tutti gli altri Version 7.1connessi, o successivi, gestori code che ospitano il flusso.
2. Rimuovere il flusso da tutti gli altri gestori code connessi Version 6.0o versioni precedenti.

Aggiunta di un punto di sottoscrizione

Come aggiungere un punto di sottoscrizione che non è stato migrato da IBM WebSphere MQ Event Broker o IBM WebSphere MQ Message Broker da **migmbbrk**. Estendere un'applicazione di pubblicazione / sottoscrizione accodata esistente che è stata migrata da IBM WebSphere MQ Event Broker o IBM WebSphere MQ Message Broker con un nuovo punto di sottoscrizione.

Prima di iniziare

1. Completare la migrazione da IBM WebSphere MQ Event Broker e IBM WebSphere MQ Message broker Version 6.0 a IBM WebSphere MQ Version 7.1.
2. Verificare che il punto di sottoscrizione non sia già definito in SYSTEM.QPUBSUB.SUBPOINT.NAMELIST.
3. Verificare se è presente un oggetto argomento o una stringa argomento con lo stesso nome del punto di sottoscrizione.

Informazioni su questa attività

Le applicazioni IBM WebSphere MQ Event Broker esistenti utilizzano i punti di sottoscrizione. Le nuove applicazioni IBM WebSphere MQ Version 7.1 non utilizzano i punti di sottoscrizione, ma possono interagire con le applicazioni esistenti che utilizzano il meccanismo di migrazione dei punti di sottoscrizione.

Un punto di sottoscrizione potrebbe non essere stato migrato da **migmbbrk**, se il punto di sottoscrizione non era in uso al momento della migrazione.

È possibile aggiungere un punto di sottoscrizione ai programmi di pubblicazione / sottoscrizione in coda esistenti migrati da IBM WebSphere MQ Event Broker.

I punti di sottoscrizione non funzionano con programmi di pubblicazione / sottoscrizione accodati che utilizzano intestazioni MQRFH1 , che sono stati migrati da IBM WebSphere MQ Version 6.0o precedenti.

Non è necessario aggiungere punti di sottoscrizione per utilizzare le applicazioni di pubblicazione / sottoscrizione integrate scritte per IBM WebSphere MQ Version 7.1.

Procedura

1. Aggiungere il nome del punto di sottoscrizione a SYSTEM.QPUBSUB.SUBPOINT.NAMELIST.
   - Su z/OS, **NLTYPE** è NONE, il valore predefinito.
   - Ripetere il passo su ogni gestore code connesso nella stessa topologia di pubblicazione / sottoscrizione.
2. Aggiungere un oggetto argomento, preferibilmente assegnandogli il nome del punto di sottoscrizione, con una stringa di argomento corrispondente al nome del punto di sottoscrizione.
   - Se il punto di sottoscrizione si trova in un cluster, aggiungere l'oggetto argomento come un argomento cluster sull'host dell'argomento cluster.
   - Se esiste un oggetto argomento con la stessa stringa argomento del nome del punto di sottoscrizione, utilizzare l'oggetto argomento esistente. È necessario comprendere le conseguenze del punto di sottoscrizione che riutilizza un argomento esistente. Se l'argomento esistente fa parte di un'applicazione esistente, è necessario risolvere il conflitto tra due argomenti con lo stesso nome.
   - Se esiste un oggetto argomento con lo stesso nome del punto di sottoscrizione, ma con una stringa argomento differente, creare un argomento con un nome diverso.
3. Impostare l'attributo **Topic** WILDCARD sul valore BLOCK.

   Il blocco delle sottoscrizioni a # o * isola le sottoscrizioni con caratteri jolly ai punti di sottoscrizione, consultare Caratteri jolly e punti di sottoscrizione.
4. Impostare gli attributi richiesti nell'oggetto argomento.

Esempio

L'esempio mostra un file di comandi **runmqsc** che aggiunge due punti di sottoscrizione, USD e GBP.

```
DEFINE TOPIC(USD) TOPICSTR(USD)
DEFINE TOPIC(GBP) TOPICSTR(GBP) WILDCARD(BLOCK)
ALTER NL(SYSTEM.QPUBSUB.SUBPOINT.NAMELIST) NAMES(SYSTEM.BROKER.DEFAULT.SUBPOINT, USD, GBP)
```

Nota:

1. Includere il punto di sottoscrizione predefinito nell'elenco di punti di sottoscrizione aggiunti utilizzando il comando **ALTER** . **ALTER** elimina i nomi esistenti nell'elenco nomi.
2. Definire gli argomenti prima di modificare l'elenco nomi. Il gestore code controlla l'elenco nomi solo quando il gestore code viene avviato e quando l'elenco nomi viene modificato.

Connettere un gestore code ad una gerarchia broker

È possibile connettere un gestore code locale a un gestore code principale per modificare una gerarchia broker.

Prima di iniziare

1. Abilitare la modalità di pubblicazione / sottoscrizione accodata. Consultare Avvio della pubblicazione / sottoscrizione accodata.
2. Questa modifica viene propagata al gestore code principale utilizzando una connessione IBM WebSphere MQ . Esistono due modi per stabilire la connessione.
   - Connettere i gestori code ad un cluster IBM WebSphere MQ , consultare Aggiunta di un gestore code ad un cluster
   - Stabilire una connessione del canale point - to - point utilizzando una coda di trasmissione o un alias del gestore code, con lo stesso nome del gestore code principale. Per ulteriori informazioni su come stabilire una connessione canale point-to-point, consultare WebSphere MQ tecniche di messaggistica distribuita.

Informazioni su questa attività

Utilizzare il comando `ALTER QMGR PARENT` *`(PARENT_NAME)`* runmqsc per collegare gli elementi child agli elementi parent.

La pubblicazione / sottoscrizione distribuita viene implementata utilizzando i cluster di gestori code e le definizioni di argomenti in cluster. Per l'interoperabilità con IBM WebSphere MQ Version 6.0 e WebSphere Message Broker Version 6.1 e WebSphere Event Broker Version 6.1 e versioni precedenti, è anche possibile connettere i gestori code Version 7.1 o versioni successive a una gerarchia broker, purché sia abilitata la modalità di pubblicazione / sottoscrizione accodata.

Procedura

PARENT QMGR ALTER (PARENT)

Esempio

Il primo esempio mostra come collegare QM2 come elemento secondario di QM1e quindi interrogare QM2 per la connessione:

```
C:>runmqsc QM2
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM2
alter qmgr parent(QM1)
     1 : alter qmgr parent(QM1)
AMQ8005: WebSphere MQ queue manager changed.
display pubsub all
     2 : display pubsub all
AMQ8723: Display pub/sub status details.
   QMNAME(QM2)                             TYPE(LOCAL)
   STATUS(ACTIVE)
AMQ8723: Display pub/sub status details.
   QMNAME(QM1)                             TYPE(PARENT)
   STATUS(ACTIVE)
```

L'esempio successivo mostra il risultato della query di QM1 per le relative connessioni:

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

```
    QMNAME(QM2)                             TYPE(CHILD)
    STATUS(ACTIVE)
```

Operazioni successive

È possibile definire argomenti su un broker o su un gestore code disponibili per i publisher e i sottoscrittori sui gestori code connessi. Per ulteriori informazioni, consultare Definizione di un argomento di gestione

Concetti correlati

Stream e argomenti

Introduzione alla messaggistica di pubblicazione / sottoscrizione di WebSphere MQ

Riferimenti correlati

VISUALIZZA PUBSUB

Disconnettere un gestore code da una gerarchia broker

Disconnettere un gestore code secondario da un gestore code principale in una gerarchia broker.

Informazioni su questa attività

Utilizzare il comando **ALTER QMGR** per disconnettere un gestore code da una gerarchia broker. È possibile disconnettere un gestore code in qualsiasi ordine in qualsiasi momento.

La richiesta corrispondente di aggiornare l'elemento principale viene inviata quando la connessione tra i gestori code è in esecuzione.

Procedura

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

Esempio

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

Operazioni successive

È possibile eliminare tutti i flussi, le code e i canali definiti manualmente che non sono più necessari.

Configurazione di un cluster di gestore code

Utilizzare i link in questo argomento per scoprire come funzionano i cluster, come progettare una configurazione cluster e per ottenere un esempio di come impostare un cluster semplice.

Prima di iniziare

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

- Funzionamento dei cluster
- “Confronto tra cluster e accodamento distribuito” a pagina 164
- “Componenti di un cluster” a pagina 166

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 180.

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

- “Organizzazione di un cluster” a pagina 182
- “Convenzioni di denominazione cluster” a pagina 182
- “Cluster sovrapposti” a pagina 183

Esempio

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 21 a pagina 162 mostra un cluster denominato DEMOCLSTR con due gestori code denominati QM1 e QM2.

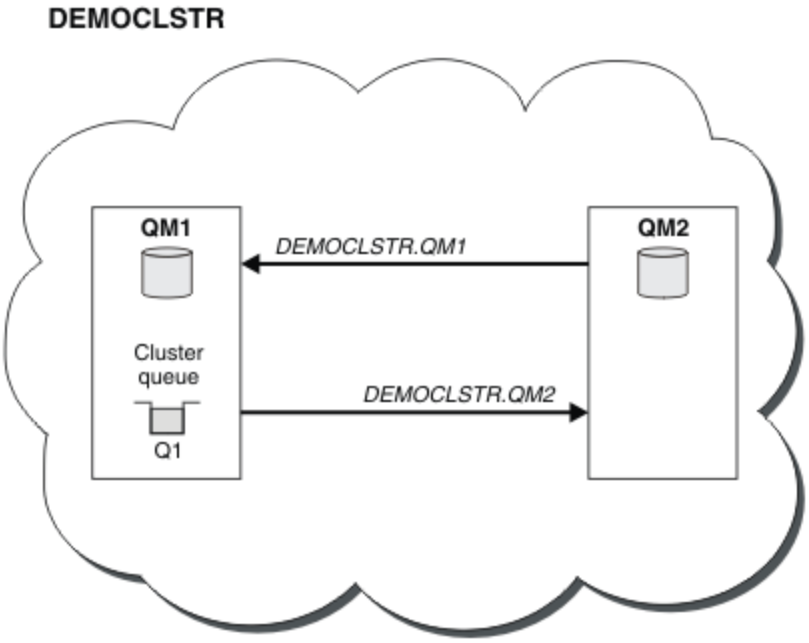


Figura 21. Un piccolo cluster di due gestori code

- I gestori code hanno nomi estesi come LONDON e NEWYORK. Gli stessi nomi vengono utilizzati nelle attività avanzate e di bilanciamento del carico di lavoro. In IBM WebSphere MQ per z/OS, i nomi dei gestori code sono limitati a quattro caratteri.
- I nomi dei gestori code implicano che ciascun gestore code si trova su una macchina separata. È possibile eseguire queste attività con tutti i gestori code sulla stessa macchina.
- Le attività utilizzano i comandi script IBM WebSphere MQ come vengono immessi dall'amministratore di sistema utilizzando i comandi **MQSC** . Esistono altri modi per immettere i comandi, incluso l'utilizzo di Esplora risorse di IBM WebSphere MQ più semplice. Il punto di utilizzo dei comandi script WebSphere MQ consiste nel dimostrare quali comandi IBM WebSphere MQ vengono utilizzati nelle attività.

Per istruzioni sull'impostazione di un cluster di esempio simile, consultare “Configurazione di un nuovo cluster” a pagina 188.

Operazioni successive

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

- “Come stabilire la comunicazione in un cluster” a pagina 186
- “Gestione dei cluster IBM WebSphere MQ” a pagina 188
- “Instradamento dei messaggi verso e dai cluster” a pagina 252
- “Utilizzo dei cluster per la gestione del carico di lavoro” a pagina 266

Per ulteriori informazioni che ti aiutano a configurare il tuo cluster, vedi “Suggerimenti per il clustering” a pagina 184.

Concetti correlati

Cluster

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 WebSphere 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 IBM WebSphere MQ tipica 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 in genere 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, da Version 7.5, le verifiche del controllo dell'accesso locale per le code del cluster remoto vengono effettuate rispetto a `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.

A partire da Version 7.1, gli amministratori hanno un altro modo per configurare il controllo accessi per le 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 del cluster remoto, 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 la stanza del gestore code, **ClusterQueueAccessControl** in `RQMName`. Il valore predefinito è `Xmitq`. È necessario creare profili per tutte le applicazioni esistenti delle code cluster che utilizzano code cluster. Se si modifica la stanza in `RQMName` senza creare profili, è probabile che le applicazioni abbiano esito negativo.

Suggerimento: Le modifiche apportate alla coda cluster che accede al check-in Version 7.1 non si applicano all'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.

Concetti correlati

“Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 288
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.

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 22 a pagina 164 mostra i componenti richiesti per l'accodamento distribuito.

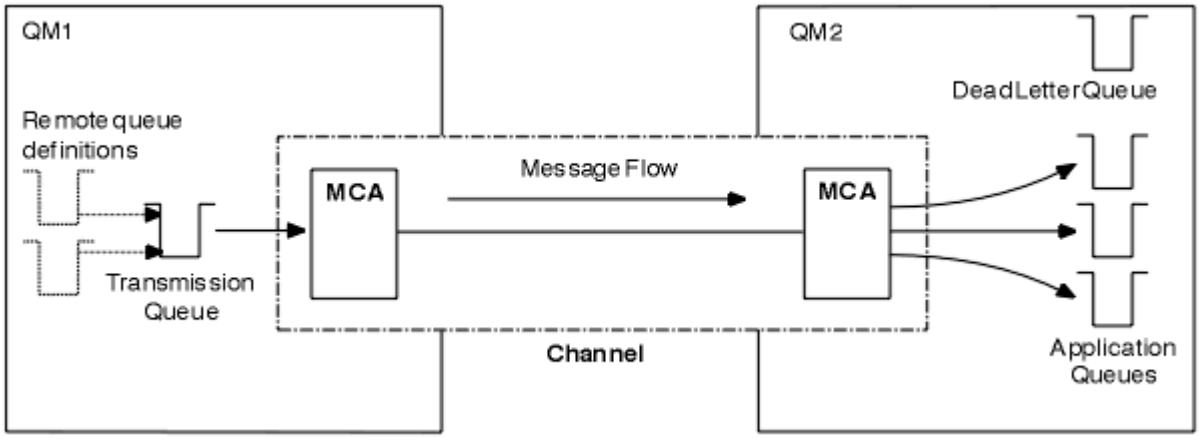


Figura 22. accodamento distribuito

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 23 a pagina 165, 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.

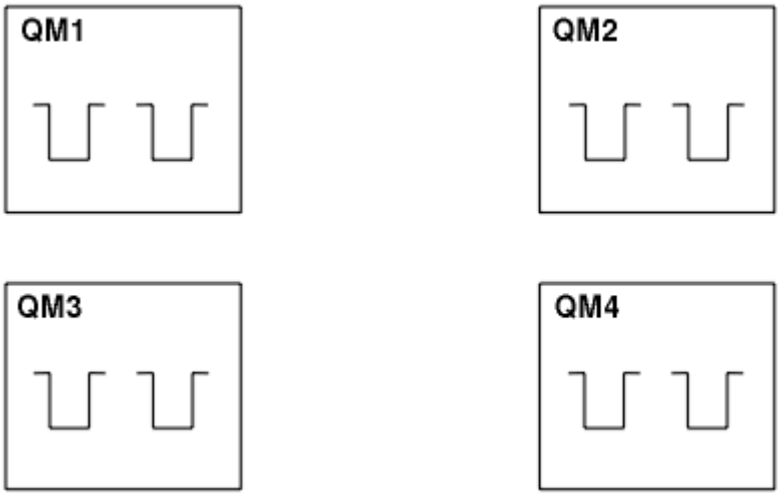


Figura 23. Una rete di quattro gestori code

Definizioni per impostare una rete utilizzando l'accodamento distribuito

Per impostare la rete mostrata in Figura 22 a pagina 164 utilizzando l'accodamento distribuito, è possibile disporre delle seguenti definizioni:

Tabella 24. 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 22 a pagina 164 utilizzando cluster sono necessarie le seguenti definizioni:

Tabella 25. 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 25. 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.

Componenti di un cluster

I cluster sono composti da gestore code, repository di cluster, canali cluster e code cluster.

Consultare i seguenti argomenti secondari per informazioni su ciascuno dei componenti cluster:

Concetti correlati

Cluster

“Confronto tra cluster e accodamento distribuito” a pagina 164
Confrontare i componenti che devono essere definiti per connettere i gestori code utilizzando l'accodamento distribuito e il cluster.

“Gestione dei cluster IBM WebSphere MQ” a pagina 188
È possibile creare, estendere e gestire cluster IBM WebSphere MQ .

Attività correlate

“Configurazione di un cluster di gestore code” a pagina 161
Utilizzare i link in questo argomento per scoprire come funzionano i cluster, come progettare una configurazione cluster e per ottenere un esempio di come impostare un cluster semplice.

“Configurazione di un nuovo cluster” a pagina 188
Seguire queste istruzioni per configurare il cluster di esempio. Istruzioni separate descrivono l'impostazione del cluster su TCP/IP, LU 6.2e con una o più code di trasmissione. Verificare il funzionamento del cluster inviando un messaggio da un gestore code all'altro.

Repository cluster

Un repository è una raccolta di informazioni sui gestori code che sono membri di un cluster.

Le informazioni sul repository includono i nomi dei gestori code, le loro ubicazioni, i loro canali, quali code ospitano e altre informazioni. Le informazioni vengono memorizzate sotto forma di messaggi su una coda denominata SYSTEM.CLUSTER.REPOSITORY.QUEUE. La coda è uno degli oggetti predefiniti. Viene definito quando si crea un gestore code WebSphere MQ , tranne che su WebSphere MQ per z/OS.

In genere, due gestori code in un cluster contengono un repository completo. Tutti i rimanenti gestori code contengono un repository parziale.

Repository completo e repository parziale

Un gestore code che ospita una serie completa di informazioni su ogni gestore code nel cluster ha un repository completo. Altri gestori code nel cluster dispongono di repository parziali contenenti un sottoinsieme di informazioni nei repository completi.

Un repository parziale contiene informazioni solo sui gestori code con cui il gestore code deve scambiare messaggi. I gestori code richiedono aggiornamenti alle informazioni di cui hanno bisogno, in modo che, in caso di modifiche, il gestore code del repository completo invii loro le nuove informazioni. Per gran parte del tempo, un repository parziale contiene tutte le informazioni che un gestore code deve eseguire all'interno del cluster. Quando un gestore code richiede ulteriori informazioni, interroga il repository completo e aggiorna quindi il repository parziale. I gestori code utilizzano una coda denominata SYSTEM.CLUSTER.COMMAND.QUEUE per richiedere e ricevere aggiornamenti ai repository. Questa coda è uno degli oggetti predefiniti.

Gestore code del cluster

Un gestore code cluster è un gestore code membro di un cluster.

Un gestore code può essere un membro di più di un cluster. Ogni gestore code cluster deve avere un nome univoco in tutti i cluster di cui è membro.

Un gestore code del cluster può ospitare code, che vengono pubblicizzate agli altri gestori code del cluster. Un gestore code del cluster non deve ospitare o pubblicizzare alcuna coda. Può inserire messaggi nel cluster e ricevere solo le risposte che sono indirizzate esplicitamente ad esso e non alle code pubblicizzate.

In WebSphere MQ per z/OS, un gestore code cluster può essere membro di un gruppo di condivisione code. In questo caso, condivide le definizioni di coda con altri gestori code nello stesso gruppo di condivisione code.

I gestori code del cluster sono autonomi. Hanno il controllo completo delle code e dei canali che definiscono. Le loro definizioni non possono essere modificate da altri gestori code (diversi dai gestori code nello stesso gruppo di condivisione code). I gestori code del repository non controllano le definizioni in altri gestori code nel cluster. Essi contengono una serie completa di tutte le definizioni, da utilizzare quando richiesto. Un cluster è una federazione di gestori code.

Dopo aver creato o modificato una definizione su un gestore code del cluster, le informazioni vengono inviate al gestore code del repository completo. Gli altri repository nel cluster vengono aggiornati successivamente.

Gestore code con repository completo

Un gestore code del repository completo è un gestore code del cluster che contiene una rappresentazione completa delle risorse del cluster. Per garantire la disponibilità, impostare due o più gestori code del repository completo in ciascun cluster. I gestori code del repository completo ricevono le informazioni inviate dagli altri gestori code nel cluster e aggiornano i relativi repository. Inviano messaggi l'uno all'altro per essere certi di essere entrambi aggiornati con nuove informazioni sul cluster.

Gestori code e repository

Ogni cluster ha almeno un gestore code (preferibilmente due) che contiene repository completi di informazioni sui gestori code, le code e i canali in un cluster. Questi repository contengono anche richieste dagli altri gestori code nel cluster per aggiornamenti alle informazioni.

Gli altri gestori code contengono un repository parziale, contenente informazioni sul sottoinsieme di code e gestori code con cui devono comunicare. I gestori code creano i propri repository parziali effettuando richieste quando devono accedere per la prima volta a un'altra coda o a un altro gestore code. Richiedono la notifica di eventuali nuove informazioni relative a tale coda o gestore code.

Ciascun gestore code memorizza le proprie informazioni sul repository in messaggi su una coda denominata SYSTEM.CLUSTER.REPOSITORY.QUEUE. I gestori code scambiano le informazioni del repository nei messaggi su una coda denominata SYSTEM.CLUSTER.COMMAND.QUEUE.

Ogni gestore code che unisce un cluster definisce un canale mittente del cluster, CLUSSDR, in uno dei repository. Apprende immediatamente quali altri gestori code nel cluster contengono repository completi. Da quel momento in poi, il gestore code può richiedere informazioni da uno qualsiasi dei repository. Quando il gestore code invia le informazioni al repository scelto, invia anche le informazioni a un altro repository (se presente).

Un repository completo viene aggiornato quando il gestore code che lo ospita riceve nuove informazioni da uno dei gestori code ad esso collegati. Le nuove informazioni vengono inviate anche a un altro repository, per ridurre il rischio che vengano ritardate se un gestore code del repository è fuori servizio. Poiché tutte le informazioni vengono inviate due volte, i repository devono eliminare i duplicati. Ogni elemento di informazioni contiene un numero di sequenza, che i repository utilizzano per identificare i duplicati. Tutti i repository vengono mantenuti in linea tra loro scambiando messaggi.

Code cluster

Una coda cluster è una coda ospitata da un gestore code cluster e resa disponibile ad altri gestori code del cluster.

Definire una coda cluster come una coda locale sul gestore code cluster in cui si trova la coda. Specificare il nome del cluster a cui appartiene la coda. Il seguente esempio mostra un comando **runmqsc** per definire una coda cluster con l'opzione CLUSTER :

```
DEFINE QLOCAL(Q1) CLUSTER(SALES)
```

Una definizione di coda cluster viene pubblicizzata in altri gestori code nel cluster. Gli altri gestori code nel cluster possono inserire i messaggi in una coda cluster senza la necessità di una definizione di coda remota corrispondente. Una coda cluster può essere pubblicizzata in più di un cluster utilizzando un elenco dei nomi di cluster.

Quando una coda viene pubblicizzata, qualsiasi gestore code del cluster può inserire dei messaggi al suo interno. Per inserire un messaggio, il gestore code deve scoprire, dai repository completi, la posizione in cui è ospitata la coda. Aggiunge quindi alcune informazioni di instradamento al messaggio e inserisce tale messaggio su una coda di trasmissione del cluster.

Una coda cluster può essere una coda che viene condivisa dai membri di un gruppo di condivisione code in IBM WebSphere MQ for z/OS.

Associazione

È possibile creare un cluster in cui più di un gestore code ospita un'istanza della stessa coda cluster. Assicurarsi che tutti i messaggi in sequenza vengano inviati alla stessa istanza della coda. È possibile associare una serie di messaggi a una particolare coda utilizzando l'opzione MQOO_BIND_ON_OPEN sulla chiamata MQOPEN .

Code di trasmissione cluster

Tranne su z/OS, un gestore code può memorizzare i messaggi per altri gestori code in un cluster su più code di trasmissione. È possibile configurare un gestore code per memorizzare messaggi su più code di trasmissione cluster in due diversi modi. Se si imposta l'attributo del gestore code DEFCLXQ su CHANNEL, viene automaticamente creata una diversa coda di trasmissione cluster da SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE per ogni canale mittente del cluster. Se si imposta l'opzione della coda di trasmissione CLCHNAME per trovare la corrispondenza con uno o più canali mittenti del cluster, il gestore code può memorizzare i messaggi per i canali corrispondenti su tale coda di trasmissione.

Attenzione: Se si sta utilizzando SYSTEM.CLUSTER.TRANSMIT.QUEUES dedicato con un gestore code che è stato aggiornato da una versione precedente del prodotto, assicurarsi che SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE abbia l'opzione SHARE/NOSHARE impostata su **SHARE**.

Un messaggio per una coda cluster su un gestore code differente viene posizionato su una coda di trasmissione cluster prima di essere inviato. Un canale mittente del cluster trasferisce i messaggi da una coda di trasmissione del cluster ai canali riceventi del cluster su altri gestori code. Per impostazione predefinita, una coda di trasmissione cluster definita dal sistema contiene tutti i messaggi che devono essere trasferiti ad altri gestori code cluster. La coda è denominata SYSTEM.CLUSTER.TRANSMIT.QUEUE. Un gestore code che fa parte di un cluster può inviare messaggi su questa coda di trasmissione del cluster a qualsiasi altro gestore code nello stesso cluster.

Una definizione per la singola coda SYSTEM.CLUSTER.TRANSMIT.QUEUE viene creata per impostazione predefinita su ogni gestore code ad eccezione di z/OS.

Su piattaforme diverse da z/OS, è possibile configurare un gestore code per trasferire i messaggi ad altri gestori code cluster utilizzando più code di trasmissione. È possibile definire manualmente ulteriori code di trasmissione del cluster oppure fare in modo che il gestore code crei automaticamente le code.

Per creare automaticamente le code dal gestore code, modificare l'attributo del gestore code DEFCLXQ da SCTQ a CHANNEL. Il risultato è che il gestore code crea una singola coda di trasmissione cluster per ogni canale mittente del cluster creato. Le code di trasmissione vengono create come code dinamiche permanenti dalla coda modello, SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE. Il nome di ogni coda dinamica permanente è SYSTEM.CLUSTER.TRANSMIT.*ChannelName*. Il nome del canale mittente del cluster a cui è associato ogni coda di trasmissione del cluster dinamico permanente è impostato nell'attributo della coda di trasmissione locale CLCHNAME. I messaggi per i gestori code con cluster remoti vengono posizionati sulla coda di trasmissione cluster dinamica permanente per il canale mittente del cluster associato, piuttosto che su SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Per creare le code di trasmissione del cluster manualmente, creare una coda locale con l'attributo USAGE impostato su XMITQe l'attributo CLCHNAME impostato su un nome di canale generico che si risolve in uno o più canali mittente del cluster; consultare ClusterChannelName. Se si creano manualmente le code di trasmissione del cluster, è possibile associare la coda di trasmissione a un singolo canale mittente del cluster o a più canali mittente del cluster. L'attributo CLCHNAME è un nome generico, che significa che è possibile inserire più caratteri jolly, "*", nel nome.

Fatta eccezione per i canali mittenti del cluster iniziali creati manualmente per collegare un gestore code a un repository completo, i canali mittenti del cluster vengono creati automaticamente. Vengono creati automaticamente quando è presente un messaggio da trasferire a un gestore code del cluster. Vengono creati con lo stesso nome del canale ricevente del cluster che riceve i messaggi cluster per quel cluster particolare sul gestore code di destinazione.

Se si segue una convenzione di denominazione per i canali riceventi del cluster, è possibile definire un valore generico per CLCHNAME che filtra i diversi tipi di messaggi del cluster in code di trasmissione differenti. Ad esempio, se si segue la convenzione di denominazione per i canali riceventi del cluster di *ClusterName*.*QmgrName*, il nome generico *ClusterName*.* filtra i messaggi per i diversi cluster su code di trasmissione differenti. È necessario definire le code di trasmissione manualmente e impostare CLCHNAME in ciascuna coda di trasmissione su *ClusterName*.*.

Le modifiche all'associazione delle code di trasmissione del cluster ai canali mittenti del cluster non hanno effetto immediato. La coda di trasmissione attualmente associata che un canale mittente del cluster sta gestendo potrebbe contenere messaggi in fase di trasferimento dal canale mittente del cluster. Solo quando nessun messaggio sulla coda di trasmissione attualmente associata viene elaborato da un canale mittente del cluster, il gestore code può modificare l'associazione del canale mittente del cluster di una coda di trasmissione diversa. Ciò può verificarsi quando nessun messaggio rimane sulla coda di trasmissione per essere elaborato dal canale mittente del cluster o quando l'elaborazione dei messaggi è sospesa e il canale mittente del cluster non ha alcun messaggio "incompleto" . Quando ciò si verifica, tutti i messaggi non elaborati per il canale mittente del cluster vengono trasferiti alla coda di trasmissione appena associata e l'associazione del canale mittente del cluster viene modificata.

È possibile creare una definizione di coda remota che si risolva in una coda di trasmissione cluster. Nella definizione, il gestore code QMX si trova nello stesso cluster del gestore code locale e non esiste alcuna coda di trasmissione, QMX.

```
DEFINE QREMOTE(A) RNAME(B) RQMNAME(QMX)
```

Durante la risoluzione del nome della coda, la coda di trasmissione del cluster ha la precedenza sulla coda di trasmissione predefinita. Un messaggio inserito in A viene memorizzato sulla coda di trasmissione cluster e quindi inviato alla coda remota B su QMX.

I gestori code possono anche comunicare con altri gestori code che non fanno parte del cluster. È necessario definire i canali e una coda di trasmissione per l'altro gestore code, come in un ambiente di accodamento distribuito.

Nota: Le applicazioni devono scrivere nelle code che si risolvono nella coda di trasmissione cluster e non devono scrivere direttamente nella coda di trasmissione cluster.

Definizione automatica delle code remote

Un gestore code in un cluster non necessita di una definizione di coda remota per le code remote nel cluster. Il gestore code del cluster trova l'ubicazione di una coda remota dal repository completo. Aggiunge le informazioni di instradamento al messaggio e le inserisce nella coda di trasmissione cluster. WebSphere MQ crea automaticamente una definizione equivalente a una definizione della coda remota in modo che il messaggio possa essere inviato.

Non è possibile modificare o eliminare una definizione di coda remota creata automaticamente. Tuttavia, utilizzando il comando DISPLAY QUEUE **runmqsc** con l'attributo CLUSINFO , è possibile visualizzare tutte le code locali su un gestore code e tutte le code cluster, incluse le code cluster su gestori code remoti. Ad esempio:

```
DISPLAY QUEUE(*) CLUSINFO
```

Riferimenti correlati

Nome ClusterChannel(MQCHAR20)

Canali cluster

È necessario definire i canali ricevente e mittente del cluster per i gestori code nel cluster. Considerazioni speciali si applicano ai repository completi.

All'interno dei cluster, i messaggi vengono distribuiti tra i gestori code del cluster su un tipo speciale di canale per cui sono necessarie le definizioni del canale ricevente del cluster e le definizioni del canale mittente del cluster.

Canale mittente del cluster: CLUSSDR

Definire manualmente un canale mittente del cluster per un repository completo in ogni gestore code nel cluster. La definizione mittente del cluster consente al gestore code di effettuare il contatto iniziale con il cluster. Denomina il gestore code del repository completo a cui il gestore code preferisce inviare le informazioni sul cluster. Il canale mittente del cluster viene utilizzato per notificare al repository eventuali

modifiche allo stato del gestore code. Ad esempio, se una coda viene aggiunta o rimossa. Essa viene utilizzata anche per trasmettere i messaggi.

I gestori code con repository completo hanno canali mittente cluster che fanno riferimento l'uno all'altro. Tali canali vengono utilizzati per comunicare le modifiche allo stato del cluster.

È poco importante a quale repository completo punta una definizione di canale CLUSSDR . Una volta stabilito il contatto iniziale, ulteriori oggetti del gestore code del cluster vengono definiti automaticamente, se necessario. Il gestore code può inviare informazioni sul cluster a ogni repository completo e messaggi a ogni gestore code.

Le definizioni CLUSSDR effettuate sui gestore code del repository completo sono speciali. Tutti gli aggiornamenti scambiati dai repository completi fluiscono esclusivamente su questi canali. L'amministratore controlla esplicitamente la rete di repository completi. L'amministratore deve definire un canale CLUSSDR da ogni gestore code del repository completo a ogni altro gestore code del repository completo nel cluster. L'amministratore deve creare manualmente le definizioni CLUSSDR sui gestori code del repository completo e non lasciarle definite automaticamente.

I canali mittenti del cluster devono essere definiti solo per collegare un repository parziale a un repository completo o per collegare insieme due repository completi. La configurazione manuale di un canale CLUSSDR che si riferisce a un repository parziale o a un gestore code non presente nel cluster, porta all'emissione di messaggi di errore, come AMQ9427 e AMQ9428 .

Anche se a volte ciò potrebbe essere inevitabile come situazione temporanea (ad esempio quando si modifica l'ubicazione di un repository completo), le definizioni errate dovrebbero essere eliminate il più presto possibile per impedire l'emissione di tali errori.

Canale ricevente del cluster: CLUSRCVR

Una definizione di canale ricevente del cluster definisce la fine di un canale su cui un gestore code del cluster può ricevere messaggi da altri gestori code nel cluster.

Un canale ricevente del cluster può anche trasportare informazioni sul cluster - informazioni destinate al repository locale. Definendo il canale ricevente del cluster, il gestore code mostra agli altri gestori code del cluster che è disponibile a ricevere messaggi. È necessario disporre di almeno un canale ricevente del cluster per ogni gestore code del cluster.

Una definizione CLUSRCVR consente ad altri gestori code di definire automaticamente le definizioni di canale CLUSSDR corrispondenti.

Concetti correlati

“Definizione automatica dei canali cluster” a pagina 171
Un gestore code deve avere una definizione per un canale mittente del cluster prima di poter inviare un messaggio a una destinazione remota. Dopo aver introdotto un gestore code in un cluster effettuando le definizioni CLUSSDR e CLUSRCVR iniziali, WebSphere MQ crea automaticamente le definizioni del canale mittente del cluster quando sono necessarie. Non è possibile modificare i canali mittenti del cluster definiti automaticamente. È possibile modificarne il funzionamento utilizzando un'uscita di definizione automatica del canale.

Definizione automatica dei canali cluster

Un gestore code deve avere una definizione per un canale mittente del cluster prima di poter inviare un messaggio a una destinazione remota. Dopo aver introdotto un gestore code in un cluster effettuando le definizioni CLUSSDR e CLUSRCVR iniziali, WebSphere MQ crea automaticamente le definizioni del canale mittente del cluster quando sono necessarie. Non è possibile modificare i canali mittenti del cluster definiti automaticamente. È possibile modificarne il funzionamento utilizzando un'uscita di definizione automatica del canale.

Quando vengono definiti sia l'estremità mittente del cluster che l'estremità ricevente del cluster di un canale, il canale viene avviato. Un canale definito automaticamente rimane attivo fino a quando non è più necessario e viene arrestato utilizzando le normali regole di intervallo di disconnessione.

I canali mittenti del cluster definiti automaticamente prendono i loro attributi dalla corrispondente definizione di canale ricevente del cluster sul gestore code di ricezione. Anche se è presente un canale mittente del cluster definito manualmente, i suoi attributi vengono modificati automaticamente per garantire che corrispondano alla definizione ricevente del cluster corrispondente. Si supponga, ad esempio, di definire un CLUSRCVR senza specificare un numero porta nel parametro CONNAME e definire manualmente un CLUSSDR che specifichi un numero porta. Quando il CLUSSDR definito automaticamente sostituisce quello definito manualmente, il numero porta (preso da CLUSRCVR) diventa vuoto. Viene utilizzato il numero di porta predefinito e il canale ha esito negativo.

Non è possibile modificare una definizione mittente del cluster definita automaticamente.

Non è possibile visualizzare automaticamente i canali definiti utilizzando il comando DISPLAY CHANNEL **runmqsc** . Per visualizzare i canali definiti automaticamente utilizzare il comando:

```
DISPLAY CLUSQMGR(qMgrName)
```

Per visualizzare lo stato del canale CLUSSDR definito automaticamente corrispondente alla definizione di canale CLUSRCVR creata, utilizzare il comando:

```
DISPLAY CHSTATUS(channelname)
```

È possibile utilizzare l'uscita di definizione automatica del canale WebSphere MQ se si desidera scrivere un programma di uscita utente per personalizzare un canale mittente del cluster o un canale ricevente del cluster. È possibile utilizzare l'uscita di definizione automatica del canale in un ambiente cluster per:

- Personalizzare le definizioni delle comunicazioni, ossia i nomi SNA LU6.2
- Aggiungere o rimuovere altre uscite, ad esempio uscite di sicurezza
- Modificare i nomi delle uscite canale. È necessario modificare il nome di un'uscita del canale CLUSSDR perché il nome dell'uscita del canale CLUSSDR viene generato automaticamente dalla definizione del canale CLUSRCVR . Il nome auto - generato potrebbe essere sbagliato, e quasi certamente è sbagliato se le due estremità del canale sono su piattaforme diverse. Il formato dei nomi di uscita è diverso su piattaforme differenti. Ad esempio, su Finestre è, SCYEXIT('*drive*:*path**library*(secexit)').

  I nomi delle uscite su piattaforme diverse da z/OS sono nel formato generale *percorso*/*libreria*(*funzione*). Se è presente *function* , vengono utilizzati fino a otto caratteri. Altrimenti, viene utilizzata la *libreria*, troncata a otto caratteri. Ad esempio,

  – /var/mqm/exits/myExit.so(MsgExit) converte in MSGEXIT
  – /var/mqm/exits/myExit converte in MYEXIT
  – /var/mqm/exits/myExit.so(ExitLongName) converte in EXITLONG

Per abilitare un canale in uscita (TCP) per utilizzare un particolare indirizzo IP, porta o intervallo di porte, utilizzare l'attributo del canale LOCLADDR. LOCLADDR è utile se si dispone di più di una scheda di rete e si desidera che un canale ne utilizzi una specifica per le comunicazioni in uscita.

Per specificare un indirizzo IP virtuale sui canali CLUSSDR , utilizzare l'indirizzo IP da LOCLADDR su un CLUSSDRdefinito manualmente. Per specificare l'intervallo di porte, utilizzare l'intervallo di porte da CLUSRCVR.

Se un cluster deve utilizzare LOCLADDR per ottenere i canali di comunicazione in uscita da collegare a un indirizzo IP specifico, è necessario scrivere un'uscita di definizione automatica del canale per forzare il valore LOCLADDR in uno dei relativi canali CLUSSDR definiti automaticamente ed è necessario specificarlo nel canale CLUSSDR definito manualmente.

non inserire un indirizzo IP nel campo LOCLADDR di un canale CLUSRCVR , a meno che tutti i gestori code non si trovino sullo stesso server. L'indirizzo IP LOCLADDR viene propagato ai canali CLUSSDR definiti automaticamente di tutti i gestori code che si connettono utilizzando il canale CLUSRCVR .

Inserire un numero di porta o un intervallo di porte in LOCLADDR di un canale CLUSRCVR , se si desidera che tutti i gestori code in un cluster utilizzino una porta specifica o un intervallo di porte, per tutte le relative comunicazioni in uscita

distributed Sulle piattaforme distribuite, è possibile impostare un valore di indirizzo locale predefinito che verrà utilizzato per tutti i canali mittenti che non hanno un indirizzo locale definito. Il valore predefinito viene definito impostando la variabile di ambiente MQ_LCLADDR prima di avviare il gestore code. Il formato del valore corrisponde a quello dell'attributo MQSC LOCLADDR.

Le definizioni di canale mittente del cluster definite automaticamente non sono oggetti canale reali. Su piattaforme diverse da z/OS, OAM (object authority manager) non è a conoscenza della relativa esistenza. Se si tenta di immettere comandi di avvio, arresto, ping, reimpostazione o risoluzione su canali mittenti del cluster definiti automaticamente, l'OAM controlla se si è autorizzati ad eseguire la stessa azione sul canale ricevente del cluster per il cluster.

Se il cluster deve utilizzare PROPCTL per rimuovere le intestazioni dell'applicazione come RFH2 dai messaggi che vanno da un gestore code di WebSphere MQ Versione 7 a un gestore code su un livello precedente di WebSphere MQ, è necessario scrivere un'uscita di definizione automatica del canale che forza PROPCTL su un valore NONE. L'uscita è necessaria perché i canali mittenti del cluster hanno la loro definizione basata sui canali riceventi del cluster corrispondenti. Poiché il canale ricevente del cluster di livello precedente non ha un attributo PROPCTL, l'attributo è impostato su COMPAT dal canale mittente del cluster automatico. L'attributo è impostato su COMPAT indipendentemente da quanto impostato sul canale mittente del cluster manuale.

Riferimenti correlati

Indirizzo locale (LOCLADDR)

Oggetti cluster predefiniti

Creare gli oggetti cluster predefiniti quando si utilizzano i cluster WebSphere MQ . Sono inclusi nella serie di oggetti predefiniti creati automaticamente quando si definisce un gestore code.

È possibile modificare le definizioni di canale predefinite come qualsiasi altra definizione di canale, eseguendo i comandi MQSC o PCF.

Non modificare le definizioni di coda predefinite, tranne per SYSTEM.CLUSTER.HISTORY.QUEUE.

SYSTEM.CLUSTER.COMMAND.QUEUE
Ogni gestore code in un cluster ha una coda locale denominata SYSTEM.CLUSTER.COMMAND.QUEUE che viene utilizzata per trasferire i messaggi al repository completo. Il messaggio contiene qualsiasi informazione nuova o modificata sul gestore code o qualsiasi richiesta di informazioni su altri gestori code. SYSTEM.CLUSTER.COMMAND.QUEUE è normalmente vuoto.

SYSTEM.CLUSTER.HISTORY.QUEUE
Ogni gestore code in un cluster ha una coda locale denominata SYSTEM.CLUSTER.HISTORY.QUEUE. SYSTEM.CLUSTER.HISTORY.QUEUE viene utilizzato per memorizzare la cronologia delle informazioni sullo stato del cluster per scopi di servizio.

Nelle impostazioni dell'oggetto predefinito, SYSTEM.CLUSTER.HISTORY.QUEUE è impostata su PUT(ENABLED). Per eliminare la raccolta cronologica, modificare l'impostazione in PUT(DISABLED).

SYSTEM.CLUSTER.REPOSITORY.QUEUE
Ogni gestore code in un cluster ha una coda locale denominata SYSTEM.CLUSTER.REPOSITORY.QUEUE. Questa coda viene utilizzata per memorizzare tutte le informazioni complete del repository. Questa coda non è normalmente vuota.

SYSTEM.CLUSTER.TRANSMIT.QUEUE
Ogni Gestore code ha una definizione per una coda locale denominata SYSTEM.CLUSTER.TRANSMIT.QUEUE. SYSTEM.CLUSTER.TRANSMIT.QUEUE è la coda di trasmissione predefinita per tutti i messaggi a tutte le code e i gestori code all'interno dei cluster. È possibile modificare la coda di trasmissione predefinita per ogni canale mittente del cluster in SYSTEM.CLUSTER.TRANSMIT.*ChannelName*, modificando l'attributo del gestore code DEFXMITQ. Non è possibile eliminare SYSTEM.CLUSTER.TRANSMIT.QUEUE. Viene utilizzato anche per definire i controlli di autorizzazione se la coda di trasmissione predefinita utilizzata è SYSTEM.CLUSTER.TRANSMIT.QUEUE o SYSTEM.CLUSTER.TRANSMIT.*ChannelName*.

SYSTEM.DEF.CLUSRCVR
Ogni cluster ha una definizione di canale CLUSRCVR predefinita denominata SYSTEM.DEF.CLUSRCVR. SYSTEM.DEF.CLUSRCVR viene utilizzato per fornire i valori predefiniti per gli attributi che non vengono specificati quando si crea un canale ricevente del cluster su un gestore code nel cluster.

SYSTEM.DEF.CLUSSDR
Ogni cluster ha una definizione di canale CLUSSDR predefinita denominata SYSTEM.DEF.CLUSSDR. SYSTEM.DEF.CLUSSDR viene utilizzato per fornire valori predefiniti per gli attributi che non vengono specificati quando si crea un canale mittente del cluster su un gestore code nel cluster.

Code di trasmissione cluster e canali mittente cluster

I messaggi tra i gestori code con cluster vengono memorizzati nelle code di trasmissione cluster e inoltrati dai canali mittenti del cluster.

Quando si visualizza il canale mittente del cluster, viene visualizzato che è associato a una coda di trasmissione. In qualsiasi momento, un canale mittente del cluster è associato a una coda di trasmissione. Se si modifica la configurazione del canale, questa potrebbe passare a una coda di trasmissione diversa al successivo avvio. Eseguire questo comando MQSC per visualizzare le code di trasmissione a cui sono associati i canali mittenti del cluster:

```
DISPLAY CHSTATUS(*) WHERE(CHLTYPE EQ CLUSSDR)
```

```
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                 CHLTYPE(CLUSSDR)
   CONNAME(9.146.163.190(1416))    CURRENT
   RQMNAME(QM2)                    STATUS(STOPPED)
   SUBSTATE( )                     XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

La coda di trasmissione visualizzata nello stato del canale salvato di un canale mittente del cluster arrestato potrebbe cambiare quando il canale viene riavviato. “Selezione di code di trasmissione predefinite per canali mittente del cluster” a pagina 175 descrive il processo di selezione di una coda di trasmissione predefinita; “Selezione di code di trasmissione definite manualmente dai canali mittente del cluster” a pagina 175 descrive il processo di selezione di una coda di trasmissione definita manualmente.

Quando un canale mittente del cluster viene avviato, ricontrolla la sua associazione con le code di trasmissione. Se la configurazione delle code di trasmissione o i valori predefiniti del gestore code vengono modificati, è possibile che il canale venga riassociato a una coda di trasmissione differente. Se il canale viene riavviato con una coda di trasmissione differente come risultato di una modifica della configurazione, viene eseguito un processo di trasferimento dei messaggi alla coda di trasmissione appena associata. “Come funziona il processo di commutazione del canale mittente del cluster in una coda di trasmissione differente” a pagina 176 descrive il processo di trasferimento di un canale mittente del cluster da una coda di trasmissione ad un altro.

Il comportamento dei canali mittente del cluster è diverso da quello dei canali mittente e server. Rimangono associate alla stessa coda di trasmissione fino a quando l'attributo del canale **XMITQ** non viene modificato. Se si modifica l'attributo della coda di trasmissione su un canale mittente o server e lo si riavvia, i messaggi non vengono trasferiti dalla vecchia coda di trasmissione a quella nuova.

Un'altra differenza tra i canali mittente del cluster e i canali mittente o server è che più canali mittente del cluster possono aprire una coda di trasmissione del cluster, ma solo un canale mittente o server può aprire una coda di trasmissione normale. Fino a quando le connessioni cluster Version 7.5 non hanno condiviso la singola coda di trasmissione cluster, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Da Version 7.5 in poi, è possibile che i canali mittente del cluster non condividano le code di trasmissione. L'esclusività non viene applicata; è un risultato della configurazione. È possibile configurare il percorso di un messaggio in un cluster in modo che non condivida alcuna coda di trasmissione o canale con i messaggi che fluiscono tra altre applicazioni. Consultare “Clustering: pianificazione della configurazione delle code di trasmissione del cluster” a pagina 291 e “Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 209.

Selezione di code di trasmissione predefinite per canali mittente del cluster

Una coda di trasmissione del cluster è una coda predefinita del sistema, con un nome che inizia con SYSTEM.CLUSTER.TRANSMIT, oppure una coda definita manualmente. Un canale mittente del cluster viene associato a una coda di trasmissione del cluster in uno dei due modi: dal meccanismo della coda di trasmissione del cluster predefinito o dalla configurazione manuale.

La coda di trasmissione del cluster predefinita è impostata come attributo del gestore code, **DEFCLXQ**. Il valore è SCTQ o CHANNEL. I gestori code nuovi e migrati sono impostati su SCTQ. È possibile modificare il valore in CHANNEL.

Se SCTQ è impostato, la coda di trasmissione del cluster predefinita è SYSTEM.CLUSTER.TRANSMIT.QUEUE. Ogni canale mittente del cluster può aprire questa coda. I canali mittenti del cluster che aprono la coda sono quelli che non sono associati alle code di trasmissione del cluster definite manualmente.

Se CHANNEL è impostato, il gestore code può creare una coda di trasmissione dinamica permanente separata per ogni canale mittente del cluster. Ogni coda è denominata SYSTEM.CLUSTER.TRANSMIT.*ChannelName* e viene creata dalla coda modello, SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE. Ogni canale mittente del cluster non associato a una code di trasmissione cluster definita manualmente è associato a una coda di trasmissione cluster dinamica permanente. La coda viene creata dal gestore code quando richiede una coda di trasmissione cluster separata per la destinazione cluster servita da questo canale mittente del cluster e non esiste alcuna coda.

Alcune destinazioni cluster possono essere servite da canali mittenti del cluster associati a code di trasmissione definite manualmente e altre dalla coda o dalle code predefinite. Nell'associazione dei canali mittenti del raggruppamento con le code di trasmissione, le code di trasmissione definite manualmente hanno sempre la precedenza sulle code di trasmissione predefinite.

La precedenza delle code di trasmissione cluster è illustrata in Figura 24 a pagina 175. L'unico canale mittente del cluster non associato ad una coda di trasmissione cluster definita manualmente è CS.QM1. Non è associato a una coda di trasmissione definita manualmente, perché nessuno dei nomi di canale nell'attributo **CLCHNAME** delle code di trasmissione corrisponde a CS.QM1.

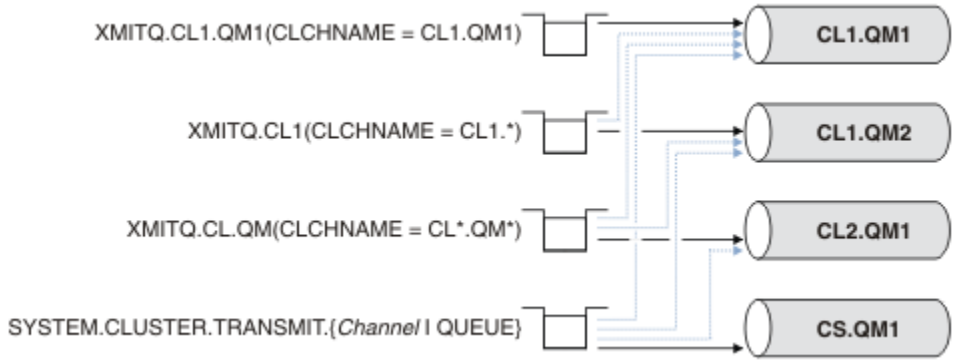


Figura 24. Precedenza coda di trasmissione / canale mittente del cluster

Selezione di code di trasmissione definite manualmente dai canali mittente del cluster

Una coda definita manualmente ha l'attributo della coda di trasmissione **USAGE** impostato su XMITQe l'attributo del nome del canale cluster **CLCHNAME** impostato su un nome canale specifico o generico.

Se il nome nell'attributo della coda **CLCHNAME** corrisponde a un nome canale mittente del cluster, il canale è associato alla coda. Il nome è una corrispondenza esatta, se il nome non contiene caratteri jolly, oppure la corrispondenza migliore, se il nome contiene caratteri jolly.

Se le definizioni **CLCHNAME** su più code di trasmissione corrispondono allo stesso canale mittente del cluster, si dice che le definizioni si sovrappongono. Per risolvere l'ambiguità, esiste un ordine di

precedenza tra le corrispondenze. Le corrispondenze esatte hanno sempre la precedenza. Figura 24 a pagina 175 mostra le associazioni tra le code di trasmissione e i canali mittente del cluster. Le frecce nere mostrano le associazioni effettive e le frecce grigie, le associazioni potenziali. L'ordine di precedenza delle code di trasmissione in Figura 24 a pagina 175 è:

XMITQ.CL1.QM1
La coda di trasmissione XMITQ.CL1.QM1 ha il proprio attributo **CLCHNAME** impostato su CL1.QM1. La definizione dell'attributo **CLCHNAME** , CL1.QM1, non ha caratteri jolly e ha la precedenza su qualsiasi altro attributo CLCHNAME , definito su altre code di trasmissione, che corrispondono ai caratteri jolly. Il gestore code memorizza qualsiasi messaggio cluster che deve essere trasferito dal canale mittente del cluster CL1.QM1 sulla coda di trasmissione XMITQ.CL1.QM1 . L'unica eccezione è se per più code di trasmissione il relativo attributo **CLCHNAME** è impostato su CL1.QM1. In tal caso, il gestore code memorizza i messaggi per il canale mittente del cluster CL1.QM1 su una qualsiasi di tali code. Seleziona una coda in modo arbitrario all'avvio del canale. Potrebbe selezionare una coda differente quando il canale viene riavviato.

XMITQ.CL1
La coda di trasmissione XMITQ.CL1 ha il proprio attributo **CLCHNAME** impostato su CL1.*. La definizione dell'attributo **CLCHNAME** , CL1.*, ha un carattere jolly finale, che corrisponde al nome di qualsiasi canale mittente del cluster che inizia con CL1.. Il gestore code memorizza qualsiasi messaggio cluster che deve essere trasferito da qualsiasi canale mittente del cluster il cui nome inizia con CL1. nella coda di trasmissione XMITQ.CL1, a meno che non vi sia una coda di trasmissione con una corrispondenza più specifica, come la coda XMITQ.CL1.QM1. Un carattere jolly finale rende la definizione meno specifica di una definizione senza caratteri jolly e più specifica di una definizione con più caratteri jolly o caratteri jolly seguiti da più caratteri finali.

XMITQ.CL.QM
XMITQ.CL.QM è il nome della coda di trasmissione con il suo attributo **CLCHNAME** impostato su CL*.QM*. La definizione di CL*.QM* ha due caratteri jolly, che corrispondono al nome di qualsiasi canale mittente del cluster che inizia con CL. e che include o termina con QM. La corrispondenza è meno specifica di una corrispondenza con un carattere jolly.

SYSTEM.CLUSTER.TRANSMIT.*channelName*|QUEUE
Se nessuna coda di trasmissione ha un attributo **CLCHNAME** che corrisponde al nome del canale mittente del cluster che il gestore code deve utilizzare, il gestore code utilizza la coda di trasmissione del cluster predefinita. La coda di trasmissione del cluster predefinita è la coda di trasmissione del cluster del sistema singolo, SYSTEM.CLUSTER.TRANSMIT.QUEUE, o una coda di trasmissione del cluster del sistema creata dal gestore code per uno specifico canale mittente del cluster, SYSTEM.CLUSTER.TRANSMIT.*channelName*. La coda predefinita dipende dall'impostazione del gestore code **DEFXMITQ** .

Suggerimento: A meno che non si abbia una chiara necessità di sovrapposizioni di definizioni, evitarle in quanto possono portare a configurazioni complicate e difficili da comprendere.

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

Per modificare l'associazione dei canali mittenti del cluster con le code di trasmissione del cluster, modificare il parametro **CLCHNAME** di qualsiasi coda di trasmissione o il parametro del gestore code **DEFCLXQ** in qualsiasi momento. Nulla accade immediatamente. Le modifiche si verificano solo quando viene avviato un canale. Quando viene avviato, verifica se continuare ad inoltrare i messaggi dalla stessa coda di trasmissione. Tre tipi di modifica modificano l'associazione di un canale mittente del cluster con una coda di trasmissione.

1. Ridefinire il parametro **CLCHNAME** della coda di trasmissione a cui è attualmente associato il canale mittente del cluster in modo che sia meno specifico o vuoto oppure eliminare la coda di trasmissione del cluster quando il canale viene arrestato.

   Alcune altre code di trasmissione del cluster potrebbero ora essere una migliore corrispondenza per il nome del canale. Oppure, se nessun' altra coda di trasmissione corrisponde al nome del canale mittente del cluster, l'associazione deve tornare alla coda di trasmissione predefinita.

2. Ridefinizione del parametro **CLCHNAME** di qualsiasi altra coda di trasmissione cluster o aggiunta di una coda di trasmissione cluster.

   Il parametro **CLCHNAME** di un'altra coda di trasmissione potrebbe ora essere una corrispondenza migliore per il canale mittente del cluster rispetto alla coda di trasmissione a cui è attualmente associato il canale mittente del cluster. Se il canale mittente del cluster è attualmente associato a una coda di trasmissione cluster predefinita, potrebbe essere associato a una coda di trasmissione cluster definita manualmente.
3. Se il canale mittente del cluster è attualmente associato a una coda di trasmissione del cluster predefinita, modificare il parametro del gestore code **DEFCLXQ** .

Se l'associazione di un canale mittente del cluster cambia, quando il canale viene avviato passa la sua associazione alla nuova coda di trasmissione. Durante lo switch, garantisce che nessun messaggio venga perso. I messaggi vengono trasferiti alla nuova coda di trasmissione nell'ordine in cui il canale trasferisce i messaggi al gestore code remoto.

Attenzione: In comune con qualsiasi inoltro di messaggi in un cluster, è necessario inserire i messaggi in gruppi per garantire che i messaggi che devono essere consegnati in ordine vengano consegnati in ordine. In rare occasioni, i messaggi possono essere fuori ordine in un cluster.

Il processo di commutazione passa attraverso i seguenti passi transazionali. Se il processo di commutazione viene interrotto, la fase transazionale corrente viene ripresa quando il canale viene riavviato.

Passo 1 - Elaborazione dei messaggi dalla coda di trasmissione originale
Il canale mittente del cluster è associato alla nuova coda di trasmissione, che potrebbe condividere con altri canali mittente del cluster. I messaggi per il canale mittente del cluster continuano ad essere inseriti nella coda di trasmissione originale. Un processo di commutazione di transizione trasferisce i messaggi dalla coda di trasmissione originale alla nuova coda di trasmissione. Il canale mittente del cluster inoltra i messaggi dalla nuova coda di trasmissione al canale ricevente del cluster. Lo stato del canale mostra il canale mittente del cluster ancora associato alla vecchia coda di trasmissione.

Il processo di commutazione continua a trasferire anche i messaggi appena arrivati. Questo passo continua fino a quando il numero di messaggi rimanenti che devono essere inoltrati dal processo di commutazione non raggiunge lo zero. Quando il numero di messaggi raggiunge lo zero, la procedura passa al punto 2.
Durante il passo 1, l'attività del disco per il canale aumenta. I messaggi persistenti vengono sottoposti a commit dalla prima coda di trasmissione e sulla seconda coda di trasmissione. Questa attività disco è in aggiunta ai messaggi di cui viene eseguito il commit quando vengono inseriti e rimossi dalla coda di trasmissione come parte del trasferimento dei messaggi normalmente. Idealmente, nessun messaggio arriva durante il processo di commutazione, in modo che la transizione possa avvenire il più rapidamente possibile. Se i messaggi arrivano, vengono elaborati dal processo di commutazione.

Fase 2 - Elaborazione dei messaggi dalla nuova coda di trasmissione
Non appena non rimane alcun messaggio nella coda di trasmissione originale per il canale mittente del cluster, i nuovi messaggi vengono inseriti direttamente sulla nuova coda di trasmissione. Lo stato del canale indica che il canale mittente del cluster è associato alla nuova coda di trasmissione.
Il seguente messaggio viene scritto nel log degli errori gestore code: "AMQ7341 `La coda di trasmissione per il canale` *`ChannelName`* `è` *`QueueName`*."

Attributi code di trasmissione cluster e code di trasmissione cluster multipli

È possibile inoltrare i messaggi del cluster a diversi gestori code che memorizzano i messaggi su una singola coda di trasmissione del cluster o su più code. Con una coda, si ha una serie di attributi della coda di trasmissione cluster da impostare e interrogare, con più code, si hanno più serie. Per alcuni attributi, avere più insiemi è un vantaggio: ad esempio, l'interrogazione della profondità della coda indica quanti messaggi sono in attesa di essere inoltrati da uno o più canali, piuttosto che da tutti i canali. Per altri attributi, la presenza di più insiemi è uno svantaggio: ad esempio, probabilmente non si desidera configurare le stesse autorizzazioni di accesso per ogni coda di trasmissione del cluster. Per questo motivo, le autorizzazioni di accesso vengono sempre verificate rispetto al profilo per

SYSTEM.CLUSTER.TRANSMIT.QUEUEe non rispetto ai profili per una particolare coda di trasmissione cluster. Se si desidera applicare controlli di sicurezza più granulari, consultare “Controllo accessi e code di trasmissione di più cluster” a pagina 163.

Più canali mittente del cluster e più code di trasmissione

Un gestore code memorizza un messaggio su una coda di trasmissione cluster prima di inoltrarlo su un canale mittente del cluster. Seleziona un canale mittente del cluster connesso alla destinazione per il messaggio. Potrebbe avere una scelta di canali mittente del cluster che si connettono tutti alla stessa destinazione. La destinazione potrebbe essere la stessa coda fisica, connessa da più canali mittente del cluster a un singolo gestore code. La destinazione potrebbe essere anche molte code fisiche con lo stesso nome di coda, ospitate su gestori code differenti nello stesso cluster. Dove è una scelta di canali mittenti del cluster connessi a una destinazione, l'algoritmo di bilanciamento del carico di lavoro ne sceglie uno. La scelta dipende da una serie di fattori; consultare L'algoritmo di gestione del carico di lavoro cluster.

In Figura 25 a pagina 179, CL1.QM1, CL1.QM2 e CS.QM1 sono tutti canali che potrebbero portare alla stessa destinazione. Ad esempio, se si definisce Q1 in CL1 su QM1 e QM2 , CL1.QM1 e CL1.QM2 forniscono entrambi instradamenti alla stessa destinazione, Q1, su due gestori code differenti. Se il canale CS.QM1 si trova anche in CL1, è anche un canale che può essere utilizzato da un messaggio per Q1 . L'appartenenza al cluster di CS.QM1 potrebbe essere definita da un elenco nomi cluster, motivo per cui il nome del canale non include un nome cluster nella sua costruzione. In base ai parametri di bilanciamento del workload e all'applicazione di invio, alcuni messaggi per Q1 potrebbero essere posizionati su ognuna delle code di trasmissione, XMITQ.CL1.QM1, XMITQ.CL1 e SYSTEM.CLUSTER.TRANSMIT.CS.QM1.

Se si intende separare il traffico di messaggi, in modo che i messaggi per la stessa destinazione non condividano le code o i canali con i messaggi per destinazioni differenti, è necessario considerare prima come dividere il traffico su canali mittenti del cluster differenti e quindi come separare i messaggi per un determinato canale in una coda di trasmissione differente. Le code cluster sullo stesso cluster, sullo stesso gestore code, normalmente condividono gli stessi canali cluster. La definizione di più code di trasmissione del cluster da sola non è sufficiente per separare il traffico dei messaggi del cluster su code differenti. A meno che non si separano messaggi per code di destinazione differenti su canali differenti, i messaggi condividono la stessa coda di trasmissione cluster.

Un modo semplice per separare i canali utilizzati dai messaggi è creare più cluster. Su qualsiasi gestore code in ogni cluster, definire solo una coda cluster. Quindi, se si definisce un canale ricevente del cluster differente per ogni combinazione cluster / gestore code, i messaggi per ogni coda cluster non condividono un canale cluster con i messaggi per altre code cluster. Se si definiscono code di trasmissione separate per i canali cluster, il gestore code di invio memorizza i messaggi solo per una coda cluster su ciascuna coda di trasmissione. Ad esempio, se si desidera che due code cluster non condividano le risorse, è possibile posizionarle in cluster differenti sullo stesso gestore code o su gestori code differenti nello stesso cluster.

La scelta della coda di trasmissione cluster non influisce sull'algoritmo di bilanciamento del carico di lavoro. L'algoritmo di bilanciamento del workload sceglie quale canale mittente del cluster inoltrare un messaggio. Colloca il messaggio nella coda di trasmissione gestita da tale canale. Se l'algoritmo di bilanciamento del carico di lavoro viene richiamato per scegliere nuovamente, ad esempio se il canale si arresta, potrebbe essere in grado di selezionare un canale differente per inoltrare il messaggio. Se sceglie un canale differente e il nuovo canale inoltra i messaggi da una diversa coda di trasmissione del cluster, l'algoritmo di bilanciamento del carico di lavoro trasferisce il messaggio all'altra coda di trasmissione.

In Figura 25 a pagina 179, due canali mittente del cluster, CS.QM1 e CS.QM2, sono associati alla coda di trasmissione del sistema predefinito. Quando l'algoritmo di bilanciamento del carico di lavoro memorizza un messaggio su SYSTEM.CLUSTER.TRANSMIT.QUEUEo qualsiasi altra coda di trasmissione del cluster, il nome del canale mittente del cluster che deve inoltrare il messaggio viene memorizzato nell'ID di correlazione del messaggio. Ogni canale inoltra solo i messaggi che corrispondono all'ID di correlazione con il nome canale.

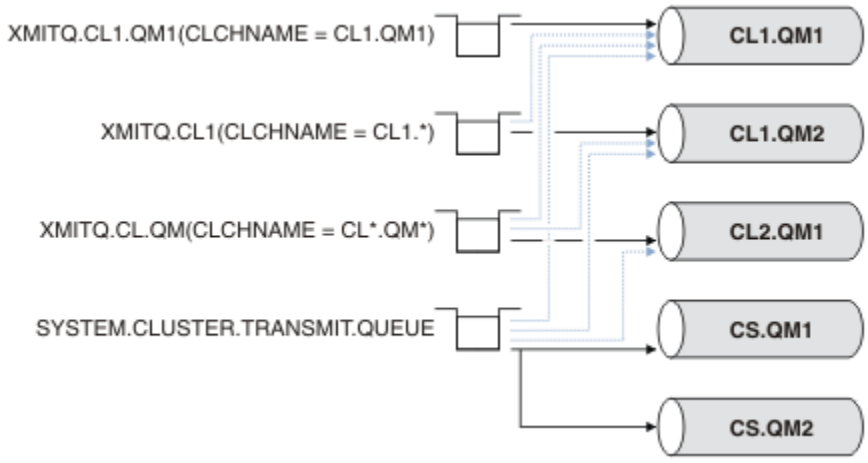


Figura 25. Più canali mittente cluster

Se `CS.QM1` si arresta, vengono esaminati i messaggi sulla coda di trasmissione per quel canale mittente del cluster. I messaggi che possono essere inoltrati da un'altra canale vengono rielaborati dall'algoritmo di bilanciamento del carico di lavoro. Il loro ID di correlazione viene reimpostato su un nome canale mittente del cluster alternativo. Se il canale mittente del cluster alternativo è `CS.QM2`, il messaggio rimane su `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Se il canale alternativo è `CL1.QM1`, l'algoritmo di bilanciamento del workload trasferisce il messaggio a `XMITQ.CL1.QM1`. Quando il canale mittente del cluster viene riavviato, i nuovi messaggi e i messaggi che non sono stati contrassegnati per un canale mittente del cluster differente, vengono nuovamente trasferiti dal canale.

È possibile modificare l'associazione tra le code di trasmissione e i canali mittenti del cluster su un sistema in esecuzione. È possibile modificare un parametro `CLCHNAME` su una coda di trasmissione oppure modificare il parametro del gestore code **DEFCLXQ** . Quando un canale interessato dalla modifica viene riavviato, avvia il processo di commutazione della coda di trasmissione; consultare “Come funziona il processo di commutazione del canale mittente del cluster in una coda di trasmissione differente” a pagina 176.

Il processo per commutare la coda di trasmissione inizia quando il canale viene riavviato. Il processo di ribilanciamento del carico di lavoro inizia quando il canale viene arrestato. I due processi possono essere eseguiti in parallelo.

Il semplice caso è quando l'arresto di un canale mittente del cluster non fa in modo che il processo di ribilanciamento modifichi il canale mittente del cluster che deve inoltrare i messaggi sulla coda. In questo caso, nessun altro canale mittente del cluster può inoltrare i messaggi alla destinazione corretta. Senza alcun canale mittente del cluster alternativo per inoltrare i messaggi alla relativa destinazione, i messaggi rimangono contrassegnati per lo stesso canale mittente del cluster dopo l'arresto del canale mittente del cluster. Quando il canale viene avviato, se uno switch è in sospeso, il processo di commutazione sposta i messaggi in una coda di trasmissione differente in cui vengono elaborati dallo stesso canale mittente del cluster.

Il caso più complesso è quello in cui più di un canale mittente del cluster può elaborare alcuni messaggi nella stessa destinazione. Arrestare e riavviare il canale mittente del cluster per attivare lo switch della coda di trasmissione. In molti casi, al momento del riavvio del canale, l'algoritmo di bilanciamento del carico di lavoro ha già spostato i messaggi dalla coda di trasmissione originale a code di trasmissione differenti servite da canali mittenti del cluster differenti. Solo i messaggi che non possono essere inoltrati da un diverso canale mittente del cluster rimangono da trasferire alla nuova coda di trasmissione. In alcuni casi, se il canale viene riavviato rapidamente, rimangono alcuni messaggi che potrebbero essere trasferiti dall'algoritmo di bilanciamento del carico di lavoro. In tal caso, alcuni messaggi rimanenti vengono commutati dal processo di bilanciamento del workload e altri dal processo di commutazione della coda di trasmissione.

Concetti correlati

“Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 288

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.

“Calcolo della dimensione del log” a pagina 407
Stima della dimensione del log necessaria per un gestore code.

Attività correlate

“Clustering: pianificazione della configurazione delle code di trasmissione del cluster” a pagina 291
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. La configurazione di più code di trasmissione cluster si applica a piattaforme diverse da z/OS.

“Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221
Seguire le istruzioni nell'attività per creare cluster sovrapposti con un gestore code del gateway. Utilizzare i cluster come punto iniziale per i seguenti esempi di isolamento dei messaggi in un'applicazione da messaggi in altre applicazioni in un cluster.

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 201
Seguire queste istruzioni per aggiungere il gestore code al cluster creato. I messaggi per le code cluster e gli argomenti vengono trasferiti utilizzando più code di trasmissione cluster.

“Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 206
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una coda di trasmissione cluster aggiuntiva per separare il traffico di messaggi a un singolo gestore code in un cluster.

“Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 209
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza un cluster aggiuntivo per isolare i messaggi in una particolare coda cluster.

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.

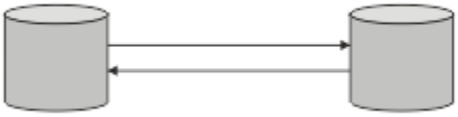


Figura 26. Due repository completi collegati.

Ogni altro gestore code nel cluster conserva un'immagine dello 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 non sono più in servizio, 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 scelti per contenere repository completi devono essere affidabili e gestiti. Scegli 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 tali sistemi richiedano solo la manutenzione 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 passano 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 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 .

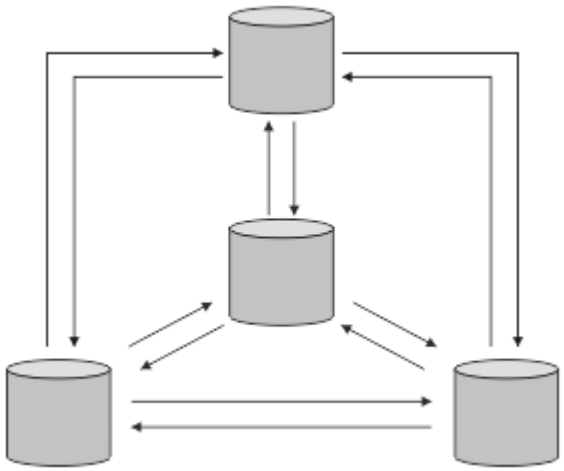


Figura 27. Più di due repository completi connessi

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 182.

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 con un massimo di 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 nel cluster prendono il loro nome dal canale ricevente del cluster corrispondente configurato sul gestore code ricevente nel cluster e devono quindi 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 che utilizza 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 , è preferibile definire canali discreti per ogni cluster in ogni caso.

Convenzioni di denominazione del canale 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.

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 28 a pagina 184, 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. WebSphere MQ seleziona i canali da 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 28 a pagina 184. WebSphere MQ sposta i messaggi nella coda 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.

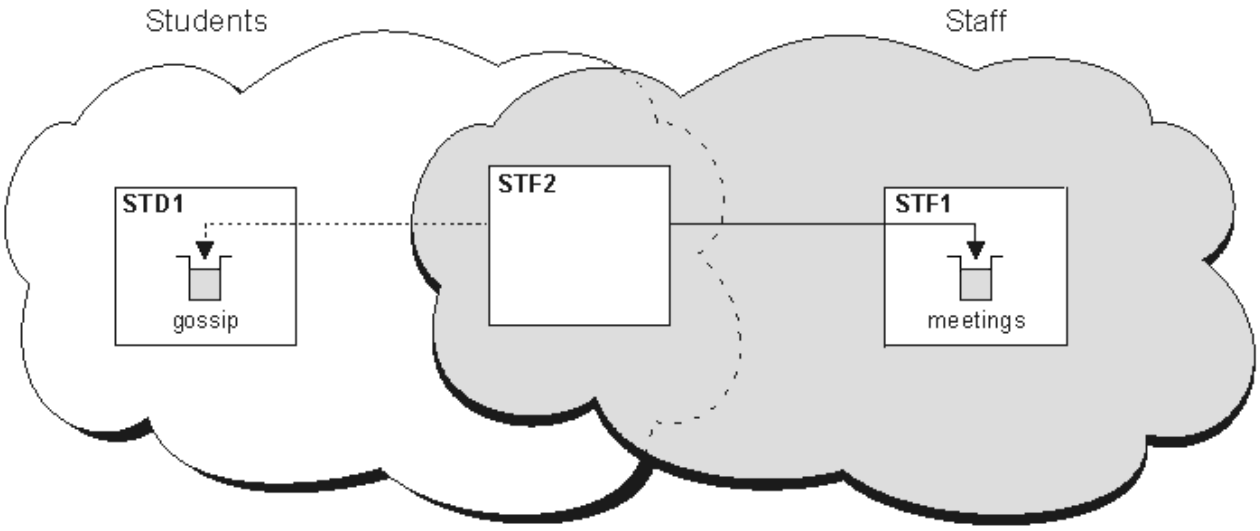


Figura 28. Classi di servizio

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.

- WebSphere MQ Explorer non può gestire direttamente i gestori code WebSphere MQ per z/OS con versioni precedenti alla Versione 6.0.
- 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 WebSphere MQ Explorer, che presenta i gestori code in una struttura ad albero, la vista per i cluster di grandi dimensioni potrebbe essere ingombrante.
- WebSphere MQ Explorer può gestire un cluster con gestori code del repository su WebSphere MQ per z/OS Versione 6 o successiva. Non è necessario nominare un repository aggiuntivo su un sistema separato. Per versioni precedenti di WebSphere MQ su z/OS, WebSphere MQ Explorer non può gestire un cluster con gestori code del repository. È necessario denominare un repository aggiuntivo su un sistema che WebSphere MQ Explorer può amministrare.
- 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 WebSphere MQ per AIX, IBM i, HP-UX, Solaris, Linuxe Windows. 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 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 WebSphere 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

Funzionamento dei cluster

“Confronto tra cluster e accodamento distribuito” a pagina 164
Confrontare i componenti che devono essere definiti per connettere i gestori code utilizzando l'accodamento distribuito e il cluster.

“Componenti di un cluster” a pagina 166
I cluster sono composti da gestore code, repository di cluster, canali cluster e code cluster.

“Gestione dei cluster IBM WebSphere MQ” a pagina 188
È possibile creare, estendere e gestire cluster IBM WebSphere MQ .

Attività correlate

“Configurazione di un cluster di gestore code” a pagina 161
Utilizzare i link in questo argomento per scoprire come funzionano i cluster, come progettare una configurazione cluster e per ottenere un esempio di come impostare un cluster semplice.

“Configurazione di un nuovo cluster” a pagina 188
Seguire queste istruzioni per configurare il cluster di esempio. Istruzioni separate descrivono l'impostazione del cluster su TCP/IP, LU 6.2e con una o più code di trasmissione. Verificare il funzionamento del cluster inviando un messaggio da un gestore code all'altro.

Come stabilire la comunicazione in un cluster

Un iniziatore di canale è necessario per avviare un canale di comunicazione quando è presente un messaggio da consegnare. Un listener del canale attende di avviare l'altra estremità di un canale per ricevere il messaggio.

Prima di iniziare

Per stabilire la comunicazione tra i gestori code in un cluster, configurare un collegamento utilizzando uno dei protocolli di comunicazione supportati. I protocolli supportati sono TCP o LU 6.2 su qualsiasi piattaforma e NetBIOS o SPX su sistemi Windows . Come parte di questa configurazione, hai anche bisogno degli iniziatori di canali e dei listener di canali proprio come si fa con l'accodamento distribuito.

Informazioni su questa attività

Tutti i gestori code cluster hanno bisogno di un iniziatore di canali per monitorare la coda di iniziazione definita dal sistema `SYSTEM.CHANNEL.INITQ`. `SYSTEM.CHANNEL.INITQ` è la coda di iniziazione per tutte le code di trasmissione, inclusa la coda di trasmissione cluster.

Ogni gestore code deve avere un listener del canale. Un programma del listener del canale attende le richieste di rete in entrata e avvia il canale ricevente appropriato quando è necessario. L'implementazione dei listener del canale è specifica della piattaforma, tuttavia ci sono alcune caratteristiche comuni.
Su tutte le piattaforme WebSphere MQ , il listener può essere avviato utilizzando il comando START `LISTENER` . Su sistemi WebSphere MQ per IBM i, Windows, UNIX and Linux , è possibile avviare automaticamente il listener contemporaneamente al gestore code. Per avviare automaticamente il listener, impostare l'attributo `CONTROL` dell'oggetto `LISTENER` su `QMGR` o `STARTONLY`.

Procedura

1. Avviare l'iniziatore di canali.
   - UNIX Linux Windows

     IBM WebSphere MQ per Windows, sistemi UNIX and Linux
     Quando si avvia un gestore code, se l'attributo del gestore code `SCHINIT` è impostato su `QMGR`, viene avviato automaticamente un iniziatore di canali. Altrimenti, può essere avviato utilizzando il comando **runmqsc** `START CHINIT` o il comando di controllo **runmqchi** .
2. Avviare il listener del canale.
   - Windows

     IBM WebSphere MQ per Windows
     Utilizzare il programma listener del canale fornito da WebSphere MQo le funzioni fornite dal sistema operativo.

     Per avviare il listener del canale WebSphere MQ utilizzare il comando `RUNMQLSR` . Ad esempio:

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

   - UNIX Linux

     IBM WebSphere MQ su sistemi UNIX and Linux
     Utilizzare il programma del listener del canale fornito da WebSphere MQo le funzioni fornite dal sistema operativo; ad esempio, **inetd** per le comunicazioni TCP.

     Per avviare il listener del canale WebSphere MQ utilizzare il comando **runmqlsr** . Ad esempio:

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

     Per utilizzare **inetd** per avviare i canali, configurare due file:

a. Modificare il file `/etc/services`. È necessario essere collegati come superuser o root. Se la seguente riga non è nel file, aggiungerla come mostrato:

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

dove 1414 è il numero di porta richiesto da IBM WebSphere MQ. È possibile modificare il numero di porta, ma deve corrispondere al numero di porta specificato all'estremità di invio.

b. Modificare il file `/etc/inetd.conf`. Se non si dispone della seguente riga in tale file, aggiungerla come mostrato:

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

dove *MQ_INSTALLATION_PATH* viene sostituito dalla directory di alto livello in cui è installato WebSphere MQ .

Gli aggiornamenti diventano attivi dopo che **inetd** ha riletto i file di configurazione. Immettere i comandi riportati di seguito dall'ID utente root:

Su AIX:

```
refresh -s inetd
```

Su HP-UX:

```
inetd -c
```

Su Solaris o Linux:

a. Individuare l'ID processo di **inetd** con il seguente comando:

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

b. Eseguire il comando appropriato, come riportato di seguito:

– Per Solaris 9 e Linux:

```
kill -1 inetd processid
```

– Per Solaris 10 o versioni successive:

```
inetconv
```

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 WebSphere 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: Per i cluster di grandi dimensioni, può essere disruttivo se molti gestori code inviano automaticamente tutte le informazioni su se stessi contemporaneamente. Consultare "L'aggiornamento in un cluster di grandi dimensioni può influire sulle prestazioni e sulla disponibilità del cluster" a pagina 311.

Concetti correlati

"Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER" a pagina 310
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.

Gestione dei cluster IBM WebSphere MQ

È possibile creare, estendere e gestire cluster IBM WebSphere MQ .

Per i dettagli su come gestire i cluster IBM WebSphere MQ , consultare i seguenti argomenti secondari:

Concetti correlati

Cluster

Funzionamento dei cluster

"Confronto tra cluster e accodamento distribuito" a pagina 164
Confrontare i componenti che devono essere definiti per connettere i gestori code utilizzando l'accodamento distribuito e il cluster.

"Componenti di un cluster" a pagina 166
I cluster sono composti da gestore code, repository di cluster, canali cluster e code cluster.

Attività correlate

"Configurazione di un cluster di gestore code" a pagina 161
Utilizzare i link in questo argomento per scoprire come funzionano i cluster, come progettare una configurazione cluster e per ottenere un esempio di come impostare un cluster semplice.

"Configurazione di un nuovo cluster" a pagina 188
Seguire queste istruzioni per configurare il cluster di esempio. Istruzioni separate descrivono l'impostazione del cluster su TCP/IP, LU 6.2e con una o più code di trasmissione. Verificare il funzionamento del cluster inviando un messaggio da un gestore code all'altro.

Configurazione di un nuovo cluster

Seguire queste istruzioni per configurare il cluster di esempio. Istruzioni separate descrivono l'impostazione del cluster su TCP/IP, LU 6.2e con una o più code di trasmissione. Verificare il funzionamento del cluster inviando un messaggio da un gestore code all'altro.

Prima di iniziare

- Invece di attenersi alle seguenti istruzioni, è possibile utilizzare una delle procedure guidate fornite con IBM WebSphere MQ Explorer per creare un cluster come quello creato da questa attività. Fare clic con il tastino destro del mouse sulla cartella Cluster di gestori code, quindi fare clic su **Nuovo** > **Cluster di gestori code**e seguire le istruzioni fornite nella procedura guidata.
- Per informazioni di background che potrebbero aiutare l'utente a comprendere i passi intrapresi per configurare un cluster, consultare "Code cluster" a pagina 168, Canali e Listener.

Informazioni su questa attività

Si sta configurando una nuova rete IBM WebSphere MQ per un chain store. Il negozio ha due filiali, una a Londra e una a New York. I dati e le applicazioni per ogni negozio sono ospitati da sistemi che eseguono gestori code separati. I due gestori code sono denominati LONDON e NEWYORK. L'applicazione di inventario viene eseguita sul sistema a New York, connesso al gestore code NEWYORK. L'applicazione è guidata dall'arrivo dei messaggi sulla coda INVENTQ , ospitata da NEWYORK. I due gestori code, LONDON e NEWYORK, devono essere collegati in un cluster denominato INVENTORY in modo che possano entrambi inserire messaggi in INVENTQ.

Figura 29 a pagina 189 mostra l'aspetto di questo cluster.

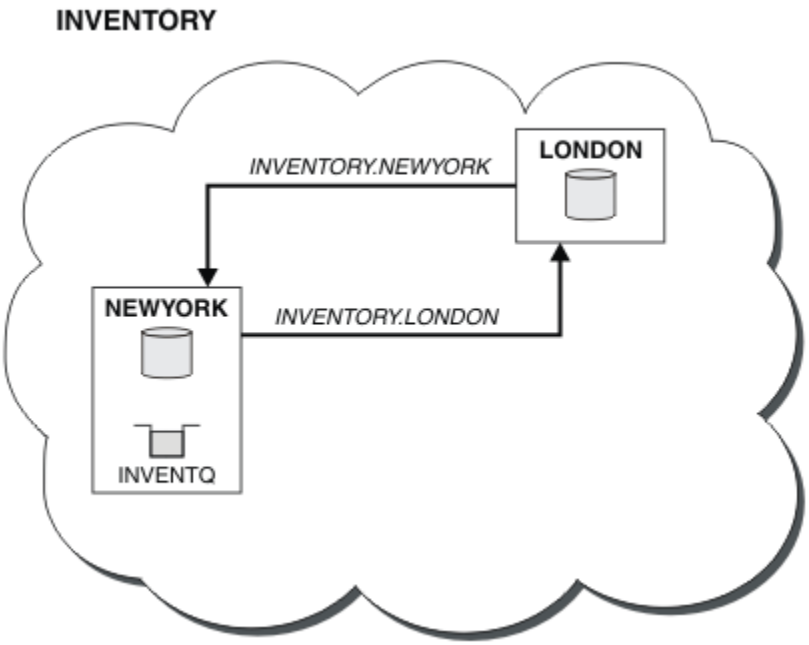


Figura 29. Il cluster INVENTORY con due gestori code

È possibile configurare ciascun gestore code nel cluster che non si trova su z/OS per inviare messaggi ad altri gestori code nel cluster utilizzando code di trasmissione cluster differenti.

Le istruzioni per impostare il cluster variano in base al protocollo di trasporto, al numero di code di trasmissione o alla piattaforma. Hai una scelta di tre combinazioni. La procedura di verifica rimane la stessa per tutte le combinazioni.

Procedura

- "Impostazione di un cluster utilizzando TCP/IP con una coda di trasmissione singola per gestore code" a pagina 190
- "Configurazione di un cluster su TCP/IP utilizzando più code di trasmissione per gestore code" a pagina 193
- "Configurazione di un cluster utilizzando LU 6.2 su z/OS" a pagina 195
- "Verifica del cluster" a pagina 197

Risultati

Figura 29 a pagina 189 mostra la configurazione del cluster INVENTORY in base a questa attività.

Chiaramente, INVENTORY è un piccolo cluster. Tuttavia, è utile come prova di concetto. La cosa importante da capire su questo cluster è l'ambito che offre per il miglioramento futuro.

Concetti correlati

Cluster

Funzionamento dei cluster

“Confronto tra cluster e accodamento distribuito” a pagina 164
Confrontare i componenti che devono essere definiti per connettere i gestori code utilizzando l'accodamento distribuito e il cluster.

“Componenti di un cluster” a pagina 166
I cluster sono composti da gestore code, repository di cluster, canali cluster e code cluster.

“Gestione dei cluster IBM WebSphere MQ” a pagina 188
È possibile creare, estendere e gestire cluster IBM WebSphere MQ .

Attività correlate

“Configurazione di un cluster di gestore code” a pagina 161
Utilizzare i link in questo argomento per scoprire come funzionano i cluster, come progettare una configurazione cluster e per ottenere un esempio di come impostare un cluster semplice.

Impostazione di un cluster utilizzando TCP/IP con una coda di trasmissione singola per gestore code

Prima di iniziare

- Su AIX, HP-UX, IBM i, Linux, Solaris, and Windows, l'attributo del gestore code, **DEFCLXQ**, deve essere lasciato come valore predefinito, SCTQ.

Informazioni su questa attività

Seguire questa procedura per impostare un cluster su AIX, HP-UX, IBM i, Linux, Solaris, and Windows utilizzando il TCP/IP del protocollo di trasporto.

Procedura

1. Decidere l'organizzazione del cluster e il relativo nome.

   Si è deciso di collegare i due gestori code, LONDON e NEWYORK, in un cluster. Un cluster con solo due gestori code offre solo vantaggi marginali su una rete che utilizza l'accodamento distribuito. Si tratta di un buon modo per iniziare e offre un margine di espansione futura. Quando si aprono nuove filiali del negozio, è possibile aggiungere facilmente i gestori code al cluster. L'aggiunta di nuovi gestori code non interrompe la rete esistente; consultare “Aggiunta di un gestore code a un cluster” a pagina 199.

   Per il momento, l'unica applicazione in esecuzione è l'applicazione di inventario. Il nome cluster è INVENTORY.
2. Decidere quali gestori code devono contenere repository completi.

   In qualsiasi cluster è necessario denominare almeno un gestore code, o preferibilmente due, per conservare i repository completi. In questo esempio, ci sono solo due gestori code, LONDON e NEWYORK, che contengono repository completi.

   a. È possibile eseguire i passi rimanenti in qualsiasi ordine.

   b. Man mano che si procede con la procedura, i messaggi di avvertenza potrebbero essere scritti nel log del gestore code. I messaggi sono il risultato di definizioni mancanti che devono essere ancora aggiunte.

   ```
   Examples of the responses to the commands are shown in a box
   like this after each step in this task.
   These examples show the responses returned by WebSphere MQ for AIX.
   The responses vary on other platforms.
   ```

   c. Prima di procedere con questi passi, assicurarsi che i gestori code siano avviati.

3. Modificare le definizioni del gestore code per aggiungere le definizioni del repository.

   Su ogni gestore code che deve contenere un repository completo, modificare la definizione del gestore code locale utilizzando il comando ALTER QMGR e specificando l'attributo REPOS :

   ```
   ALTER QMGR REPOS(INVENTORY)
   ```

   ```
   1 : ALTER QMGR REPOS(INVENTORY)
   AMQ8005: Websphere MQ queue manager changed.
   ```

   Ad esempio, se si immette:

   a. `runmqsc LONDON`

   b. `ALTER QMGR REPOS(INVENTORY)`

   LONDON viene modificato in repository completo.

4. Definire i listener.

   Definire un listener che accetti richieste di rete da altri gestori code per ogni gestore code nel cluster. Sui gestori code LONDON , immettere il seguente comando:

   ```
   DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR)
   ```

   Nota: Quando si definisce un listener, è necessario definire un numero di porta se si utilizzano gli indirizzi IP nel campo CONNAME e il numero di porta non è la porta predefinita (1414). Ad esempio:

   ```
   DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(1415)
   ```

   L'attributo CONTROL assicura che il listener venga avviato e arrestato quando il gestore code lo fa.

   Il listener non viene avviato quando è definito, quindi deve essere avviato manualmente la prima volta con il seguente comando MQSC:

   ```
   START LISTENER(LONDON_LS)
   ```

   Immettere comandi simili per tutti gli altri gestori code nel cluster, modificando il nome listener per ciascun gestore code.

   Esistono diversi modi per definire questi listener, come mostrato in Listener.

5. Definire il canale CLUSRCVR per il gestore code LONDON .

   Su ogni gestore code in un cluster, definire un canale ricevente del cluster su cui il gestore code può ricevere messaggi. CLUSRCVR definisce il nome connessione del gestore code. Il nome della connessione è memorizzato nei repository, a cui possono fare riferimento altri gestori code. La parola chiave CLUSTER mostra la disponibilità del gestore code a ricevere messaggi da altri gestori code nel cluster.

   In questo esempio, il nome del canale è `INVENTORY.LONDON`e il nome della connessione (`CONNAME`) è l'indirizzo di rete della macchina su cui si trova il gestore code, ovvero `LONDON.CHSTORE.COM`. L'indirizzo di rete può essere immesso come un nome host DNS alfanumerico o come un indirizzo IP in formato decimale puntato IPv4 . Ad esempio, `192.0.2.0`o formato esadecimale IPv6 ; ad esempio `2001:DB8:0204:acff:fe97:2c34:fde0:3485`. Il numero di porta non è specificato, quindi viene utilizzata la porta predefinita (1414).

   ```
   DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('TCP Cluster-receiver channel for queue manager LONDON')
   ```

```
1 : DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
AMQ8014: Websphere MQ channel created.
07/09/98  12:56:35  No repositories for cluster 'INVENTORY'
```

6. Definire il canale CLUSRCVR per il gestore code NEWYORK .

   Se il listener del canale sta utilizzando la porta predefinita, in genere 1414, e il cluster non include un gestore code su z/OS, è possibile omettere CONNAME

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CLUSTER(INVENTORY)
   DESCR('TCP Cluster-receiver channel for queue manager NEWYORK')
   ```

7. Definire il canale CLUSSDR sul gestore code LONDON .

   Su ogni gestore code in un cluster, definire un canale mittente del cluster. Il gestore code invia messaggi a un gestore code del repository completo sul canale mittente del cluster. In questo caso, ci sono solo due gestori code, entrambi con repository completi. Ciascuno di essi deve avere una definizione CLUSSDR che punti al canale CLUSRCVR definito sull'altro gestore code. I nomi canale forniti nelle definizioni CLUSSDR devono corrispondere ai nomi canale nelle definizioni CLUSRCVR corrispondenti. Quando un gestore code dispone di definizioni sia per un canale ricevente del cluster che per un canale mittente del cluster nello stesso cluster, il canale mittente del cluster viene avviato.

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
   ```

```
1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
AMQ8014: Websphere MQ channel created.
07/09/98  13:00:18    Channel program started.
```

8. Definire il canale CLUSSDR sul gestore code NEWYORK .

   ```
   DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('TCP Cluster-sender channel from NEWYORK to repository at LONDON')
   ```

9. Definire la coda cluster INVENTQ

   Definire la coda INVENTQ sul gestore code NEWYORK , specificando la parola chiave CLUSTER .

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

```
1 : DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
AMQ8006: Websphere MQ queue created.
```

   La parola chiave CLUSTER fa sì che la coda venga annunciata al cluster. Una volta definita, la coda diventa disponibile per gli altri gestori code nel cluster. Possono inviargli messaggi senza dover creare una definizione di coda remota.

   Tutte le definizioni sono complete. Su tutte le piattaforme, avviare un programma listener su ciascun gestore code. Il programma listener attende le richieste di rete in arrivo e avvia il canale ricevente del cluster quando è necessario.

Configurazione di un cluster su TCP/IP utilizzando più code di trasmissione per gestore code

Informazioni su questa attività

Seguire questa procedura per impostare un cluster su AIX, HP-UX, IBM i, Linux, Solaris, and Windows utilizzando il TCP/IP del protocollo di trasporto. I gestori code del repository sono configurati per utilizzare una coda di trasmissione cluster differente per inviare messaggi l'uno all'altro e ad altri gestori code nel cluster. Se si aggiungono gestori code al cluster che devono anche utilizzare code di trasmissione differenti, seguire l'attività, "Aggiunta di un gestore code a un cluster: code di trasmissione separate" a pagina 201. Non è possibile configurare un gestore code su z/OS per utilizzare code di trasmissione cluster separate.

Procedura

1. Decidere l'organizzazione del cluster e il relativo nome.

   Si è deciso di collegare i due gestori code, LONDON e NEWYORK, in un cluster. Un cluster con solo due gestori code offre solo vantaggi marginali su una rete che utilizza l'accodamento distribuito. Si tratta di un buon modo per iniziare e offre un margine di espansione futura. Quando si aprono nuove filiali del negozio, è possibile aggiungere facilmente i gestori code al cluster. L'aggiunta di nuovi gestori code non interrompe la rete esistente; consultare "Aggiunta di un gestore code a un cluster" a pagina 199.

   Per il momento, l'unica applicazione in esecuzione è l'applicazione di inventario. Il nome cluster è INVENTORY.
2. Decidere quali gestori code devono contenere repository completi.

   In qualsiasi cluster è necessario denominare almeno un gestore code, o preferibilmente due, per conservare i repository completi. In questo esempio, ci sono solo due gestori code, LONDON e NEWYORK, che contengono repository completi.

   a. È possibile eseguire i passi rimanenti in qualsiasi ordine.

   b. Man mano che si procede con la procedura, i messaggi di avvertenza potrebbero essere scritti nel log del gestore code. I messaggi sono il risultato di definizioni mancanti che devono essere ancora aggiunte.

   ```
   Examples of the responses to the commands are shown in a box
   like this after each step in this task.
   These examples show the responses returned by WebSphere MQ for AIX.
   The responses vary on other platforms.
   ```

   c. Prima di procedere con questi passi, assicurarsi che i gestori code siano avviati.
3. Modificare le definizioni del gestore code per aggiungere le definizioni del repository.

   Su ogni gestore code che deve contenere un repository completo, modificare la definizione del gestore code locale utilizzando il comando ALTER QMGR e specificando l'attributo REPOS :

   ```
   ALTER QMGR REPOS(INVENTORY)
   ```

   ```
   1 : ALTER QMGR REPOS(INVENTORY)
   AMQ8005: Websphere MQ queue manager changed.
   ```

   Ad esempio, se si immette:

   a. `runmqsc LONDON`

   b. `ALTER QMGR REPOS(INVENTORY)`

   LONDON viene modificato in repository completo.

4. Modificare le definizioni del gestore code per creare code di trasmissione cluster separate per ciascuna destinazione.

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

   Su ogni gestore code che si aggiunge al cluster decidere se utilizzare o meno code di trasmissione separate. Consultare gli argomenti “Aggiunta di un gestore code a un cluster” a pagina 199 e “Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 201.

5. Definire i listener.

   Definire un listener che accetti richieste di rete da altri gestori code per ogni gestore code nel cluster. Sui gestori code LONDON , immettere il seguente comando:

```
DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR)
```

   Nota: Quando si definisce un listener, è necessario definire un numero di porta se si utilizzano gli indirizzi IP nel campo CONNAME e il numero di porta non è la porta predefinita (1414). Ad esempio:

```
DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(1415)
```

   L'attributo CONTROL assicura che il listener venga avviato e arrestato quando il gestore code lo fa.

   Il listener non viene avviato quando è definito, quindi deve essere avviato manualmente la prima volta con il seguente comando MQSC:

```
START LISTENER(LONDON_LS)
```

   Immettere comandi simili per tutti gli altri gestori code nel cluster, modificando il nome listener per ciascun gestore code.

   Esistono diversi modi per definire questi listener, come mostrato in Listener.

6. Definire il canale CLUSRCVR per il gestore code LONDON .

   Su ogni gestore code in un cluster, definire un canale ricevente del cluster su cui il gestore code può ricevere messaggi. CLUSRCVR definisce il nome connessione del gestore code. Il nome della connessione è memorizzato nei repository, a cui possono fare riferimento altri gestori code. La parola chiave CLUSTER mostra la disponibilità del gestore code a ricevere messaggi da altri gestori code nel cluster.

   In questo esempio, il nome del canale è INVENTORY.LONDONe il nome della connessione (CONNAME) è l'indirizzo di rete della macchina su cui si trova il gestore code, ovvero LONDON.CHSTORE.COM. L'indirizzo di rete può essere immesso come un nome host DNS alfanumerico o come un indirizzo IP in formato decimale puntato IPv4 . Ad esempio, 192.0.2.0o formato esadecimale IPv6 ; ad esempio 2001:DB8:0204:acff:fe97:2c34:fde0:3485. Il numero di porta non è specificato, quindi viene utilizzata la porta predefinita (1414).

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
```

```
1 : DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
AMQ8014: Websphere MQ channel created.
07/09/98  12:56:35  No repositories for cluster 'INVENTORY'
```

7. Definire il canale CLUSRCVR per il gestore code NEWYORK .

   Se il listener del canale sta utilizzando la porta predefinita, in genere 1414, e il cluster non include un gestore code su z/OS, è possibile omettere CONNAME

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager NEWYORK')
```

8. Definire il canale CLUSSDR sul gestore code LONDON .

   Su ogni gestore code in un cluster, definire un canale mittente del cluster. Il gestore code invia messaggi a un gestore code del repository completo sul canale mittente del cluster. In questo caso, ci sono solo due gestori code, entrambi con repository completi. Ciascuno di essi deve avere una definizione CLUSSDR che punti al canale CLUSRCVR definito sull'altro gestore code. I nomi canale forniti nelle definizioni CLUSSDR devono corrispondere ai nomi canale nelle definizioni CLUSRCVR corrispondenti. Quando un gestore code dispone di definizioni sia per un canale ricevente del cluster che per un canale mittente del cluster nello stesso cluster, il canale mittente del cluster viene avviato.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
```

```
1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
AMQ8014: Websphere MQ channel created.
07/09/98  13:00:18    Channel program started.
```

9. Definire il canale CLUSSDR sul gestore code NEWYORK .

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from NEWYORK to repository at LONDON')
```

10. Definire la coda cluster INVENTQ

    Definire la coda INVENTQ sul gestore code NEWYORK , specificando la parola chiave CLUSTER .

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

```
1 : DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
AMQ8006: Websphere MQ queue created.
```

    La parola chiave CLUSTER fa sì che la coda venga annunciata al cluster. Una volta definita, la coda diventa disponibile per gli altri gestori code nel cluster. Possono inviargli messaggi senza dover creare una definizione di coda remota.

    Tutte le definizioni sono complete. Su tutte le piattaforme, avviare un programma listener su ciascun gestore code. Il programma listener attende le richieste di rete in arrivo e avvia il canale ricevente del cluster quando è necessario.

Configurazione di un cluster utilizzando LU 6.2 su z/OS

Procedura

1. Decidere l'organizzazione del cluster e il relativo nome.

   Si è deciso di collegare i due gestori code, LONDON e NEWYORK, in un cluster. Un cluster con solo due gestori code offre solo vantaggi marginali su una rete che utilizza l'accodamento distribuito. Si tratta di un buon modo per iniziare e offre un margine di espansione futura. Quando si aprono nuove filiali del negozio, è possibile aggiungere facilmente i gestori code al cluster. L'aggiunta di nuovi gestori code non interrompe la rete esistente; consultare “Aggiunta di un gestore code a un cluster” a pagina 199.

   Per il momento, l'unica applicazione in esecuzione è l'applicazione di inventario. Il nome cluster è INVENTORY.
2. Decidere quali gestori code devono contenere repository completi.

   In qualsiasi cluster è necessario denominare almeno un gestore code, o preferibilmente due, per conservare i repository completi. In questo esempio, ci sono solo due gestori code, LONDON e NEWYORK, che contengono repository completi.

a. È possibile eseguire i passi rimanenti in qualsiasi ordine.

b. Man mano che si procede con i passi, potrebbero essere scritti messaggi di avvertenza nella console del sistema z/OS . I messaggi sono il risultato di definizioni mancanti che devono essere ancora aggiunte.

c. Prima di procedere con questi passi, assicurarsi che i gestori code siano avviati.

3. Modificare le definizioni del gestore code per aggiungere le definizioni del repository.

   Su ogni gestore code che deve contenere un repository completo, modificare la definizione del gestore code locale utilizzando il comando ALTER QMGR e specificando l'attributo REPOS :

```
ALTER QMGR REPOS(INVENTORY)
```

```
1 : ALTER QMGR REPOS(INVENTORY)
AMQ8005: Websphere MQ queue manager changed.
```

   Ad esempio, se si immette:

   a. `runmqsc LONDON`

   b. `ALTER QMGR REPOS(INVENTORY)`

   LONDON viene modificato in repository completo.

4. Definire i listener.

   Il listener non viene avviato quando è definito, quindi deve essere avviato manualmente la prima volta con il seguente comando MQSC:

```
START LISTENER(LONDON_LS)
```

   Immettere comandi simili per tutti gli altri gestori code nel cluster, modificando il nome listener per ciascun gestore code.

5. Definire il canale CLUSRCVR per il gestore code LONDON .

   Su ogni gestore code in un cluster, definire un canale ricevente del cluster su cui il gestore code può ricevere messaggi. CLUSRCVR definisce il nome connessione del gestore code. Il nome della connessione è memorizzato nei repository, a cui possono fare riferimento altri gestori code. La parola chiave CLUSTER mostra la disponibilità del gestore code a ricevere messaggi da altri gestori code nel cluster.

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(LU62)
CONNAME(LONDON.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-receiver channel for queue manager LONDON')
```

```
1 : DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(LU62)
CONNAME(LONDON.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-receiver channel for queue manager LONDON')
AMQ8014: Websphere MQ channel created.
07/09/98  12:56:35  No repositories for cluster 'INVENTORY'
```

6. Definire il canale CLUSRCVR per il gestore code NEWYORK .

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(LU62)
CONNAME(NEWYORK.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-receiver channel for queue manager NEWYORK')
```

7. Definire il canale CLUSSDR sul gestore code LONDON .

   Su ogni gestore code in un cluster, definire un canale mittente del cluster. Il gestore code invia messaggi a un gestore code del repository completo sul canale mittente del cluster. In questo caso, ci sono solo due gestori code, entrambi con repository completi. Ciascuno di essi deve avere una

definizione CLUSSDR che punti al canale CLUSRCVR definito sull'altro gestore code. I nomi canale forniti nelle definizioni CLUSSDR devono corrispondere ai nomi canale nelle definizioni CLUSRCVR corrispondenti. Quando un gestore code dispone di definizioni sia per un canale ricevente del cluster che per un canale mittente del cluster nello stesso cluster, il canale mittente del cluster viene avviato.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
CONNAME(CPIC) CLUSTER(INVENTORY)
DESCR('LU62 Cluster-sender channel from LONDON to repository at NEWYORK')
```

```
1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
CONNAME(NEWYORK.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-sender channel from LONDON to repository at NEWYORK')
AMQ8014: Websphere MQ channel created.
07/09/98  13:00:18    Channel program started.
```

8. Definire il canale CLUSSDR sul gestore code NEWYORK .

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
CONNAME(LONDON.LUNAME) CLUSTER(INVENTORY)
DESCR('LU62 Cluster-sender channel from NEWYORK to repository at LONDON')
```

9. Definire la coda cluster INVENTQ

   Definire la coda INVENTQ sul gestore code NEWYORK , specificando la parola chiave CLUSTER .

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

```
1 : DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
AMQ8006: Websphere MQ queue created.
```

   La parola chiave CLUSTER fa sì che la coda venga annunciata al cluster. Una volta definita, la coda diventa disponibile per gli altri gestori code nel cluster. Possono inviargli messaggi senza dover creare una definizione di coda remota.

   Tutte le definizioni sono complete. Su tutte le piattaforme, avviare un programma listener su ciascun gestore code. Il programma listener attende le richieste di rete in arrivo e avvia il canale ricevente del cluster quando è necessario.

Verifica del cluster

Informazioni su questa attività

È possibile verificare il cluster in uno o più dei seguenti modi:

1. Esecuzione dei comandi di gestione per visualizzare gli attributi del cluster e del canale.
2. Eseguire i programmi di esempio per inviare e ricevere messaggi su una coda cluster.
3. Scrivere i propri programmi per inviare un messaggio di richiesta ad una coda cluster e rispondere con un messaggio di risposta ad una coda di risposta non cluster.

Procedura

Immettere i comandi DISPLAY **runmqsc** per verificare il cluster.

Le risposte che si vedono dovrebbero essere come le risposte nei passi che seguono.

1. Dal gestore code NEWYORK , eseguire il comando **DISPLAY CLUSQMGR** :

```
dis clusqmgr(*)
```

```
1 : dis clusqmgr(*)
AMQ8441: Display Cluster Queue Manager details.
CLUSQMGR(NEWYORK)              CLUSTER(INVENTORY)
CHANNEL(INVENTORY.NEWYORK)
AMQ8441: Display Cluster Queue Manager details.
CLUSQMGR(LONDON)               CLUSTER(INVENTORY)
CHANNEL(INVENTORY.LONDON)
```

2. Dal gestore code NEWYORK , eseguire il comando **DISPLAY CHANNEL STATUS** :

```
dis chstatus(*)
```

```
1 : dis chstatus(*)
AMQ8417: Display Channel Status details.
CHANNEL(INVENTORY.NEWYORK)     XMITQ( )
CONNAME(192.0.2.0)             CURRENT
CHLTYPE(CLUSRCVR)              STATUS(RUNNING)
RQMNAME(LONDON)
AMQ8417: Display Channel Status details.
CHANNEL(INVENTORY.LONDON)      XMITQ(SYSTEM.CLUSTER.TRANSMIT.INVENTORY.LONDON)
CONNAME(192.0.2.1)             CURRENT
CHLTYPE(CLUSSDR)               STATUS(RUNNING)
RQMNAME(LONDON)
```

Inviare messaggi tra i due gestori code, utilizzando **amqsput**.

3. Su LONDON eseguire il comando **amqsput INVENTQ LONDON**.

   Immettere alcuni messaggi, seguiti da una riga vuota.

4. Su NEWYORK eseguire il comando **amqsget INVENTQ NEWYORK**.

   Ora vengono visualizzati i messaggi immessi su LONDON. Dopo 15 secondi il programma termina.

Inviare i messaggi tra i due gestori code utilizzando i propri programmi.

Nei seguenti passi, LONDON inserisce un messaggio in INVENTQ alle NEWYORK e riceve una risposta sulla coda LONDON_reply.

5. Su LONDON , inserire un messaggio nella coda cluster.
   a) Definire una coda locale denominata LONDON_reply.
   b) Impostare le opzioni MQOPEN su MQOO_OUTPUT.
   c) Emettere la chiamata MQOPEN per aprire la coda INVENTQ.
   d) Impostare il nome *ReplyToQ* nel descrittore del messaggio su LONDON_reply.
   e) Emettere la chiamata MQPUT per inserire il messaggio.
   f) Eseguire il commit del messaggio.
6. Su NEWYORK , ricevere il messaggio sulla coda cluster e inserire una risposta nella coda di risposta.
   a) Impostare le opzioni MQOPEN su MQOO_BROWSE.
   b) Emettere la chiamata MQOPEN per aprire la coda INVENTQ.
   c) Emettere la chiamata MQGET per ottenere un messaggio da INVENTQ.
   d) Richiamare il nome *ReplyToQ* dal descrittore del messaggio.
   e) Inserire il nome *ReplyToQ* nel campo ObjectName del descrittore oggetto.
   f) Impostare le opzioni MQOPEN su MQOO_OUTPUT.
   g) Emettere la chiamata MQOPEN per aprire LONDON_reply sul gestore code LONDON.
   h) Emettere la chiamata MQPUT per inserire il messaggio in LONDON_reply.
7. Su LONDON ricevere la risposta.
   a) Impostare le opzioni MQOPEN su MQOO_BROWSE.
   b) Emettere la chiamata MQOPEN per aprire la coda LONDON_reply.
   c) Emettere la chiamata MQGET per richiamare il messaggio da LONDON_reply.

Aggiunta di un gestore code a un cluster

Seguire queste istruzioni per aggiungere il gestore code al cluster creato. I messaggi per le code e gli argomenti del cluster vengono trasferiti utilizzando la singola coda di trasmissione del cluster SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Il cluster INVENTORY è configurato come descritto in "Configurazione di un nuovo cluster" a pagina 188. Contiene due gestori code, LONDON e NEWYORK, che contengono entrambi repository completi.
- Il gestore code PARIS appartiene all'installazione primaria. Se non lo è, è necessario eseguire il comando **setmqenv** per impostare l'ambiente di comandi per l'installazione a cui appartiene PARIS .
- La connettività TCP esiste tra tutti e tre i sistemi e il gestore code è configurato con un listener TCP che viene avviato sotto il controllo del gestore code.

Informazioni su questa attività

1. Una nuova filiale della catena di negozi è in fase di configurazione a Parigi e si desidera aggiungere al cluster un gestore code denominato PARIS .
2. Il gestore code PARIS invia aggiornamenti di inventario all'applicazione in esecuzione sul sistema a New York inserendo i messaggi nella coda INVENTQ .

Attenersi alla seguente procedura per aggiungere un gestore code a un cluster.

Procedura

1. Decidere quale repository completo PARIS fa riferimento per primo.

   Ogni gestore code in un cluster deve fare riferimento a uno o più repository completi. Raccoglie le informazioni sul cluster da un repository completo e quindi crea il proprio repository parziale. Scegliere uno dei repository come repository completo. Non appena un nuovo gestore code viene aggiunto al cluster, viene immediatamente a conoscenza dell'altro repository. Le informazioni relative alle modifiche a un gestore code vengono inviate direttamente a due repository. In questo esempio, si collega PARIS al gestore code LONDON, solo per motivi geografici.

   Nota: Eseguire i passi rimanenti in qualsiasi ordine, dopo l'avvio del gestore code PARIS .
2. Definire un canale CLUSRCVR sul gestore code PARIS.

   Ogni gestore code in un cluster deve definire un canale ricevente del cluster su cui può ricevere i messaggi. Su PARIS, definire:

   ```
   DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(PARIS.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for queue manager PARIS')
   ```

   Il canale ricevente del cluster annuncia la disponibilità del gestore code a ricevere messaggi da altri gestori code nel cluster INVENTORY. Non è necessario creare definizioni su altri gestori code per l'invio al canale ricevente del cluster INVENTORY.PARIS. Le altre definizioni vengono effettuate automaticamente quando necessario.
3. Definire un canale CLUSSDR nel gestore code PARIS.

   Ogni gestore code in un cluster deve definire un canale mittente del cluster su cui inviare i messaggi al repository completo iniziale.

Su PARIS, creare la seguente definizione per un canale denominato INVENTORY.LONDON al gestore code con indirizzo di rete LONDON.CHSTORE.COM.

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from PARIS to repository at LONDON')
```

4. Opzionale: Se questo gestore code si sta unendo nuovamente a un cluster, completare alcuni passi aggiuntivi.
   a) Se si sta aggiungendo un gestore code a un cluster che è stato precedentemente rimosso dallo stesso cluster, verificare che venga visualizzato come membro del cluster. In caso contrario, completare i seguenti passi aggiuntivi:
      i) Immettere il comando **REFRESH CLUSTER** sul gestore code che si sta aggiungendo. Questa fase arresta i canali del cluster e fornisce alla tua cache del cluster locale una nuova serie di numeri di sequenza che sono sicuri di essere aggiornati nel resto del cluster.

```
REFRESH CLUSTER(INVENTORY) REPOS(YES)
```

      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 gli aggiornamenti di stato a tutti i gestori code interessati. Consultare Refreshing in a large cluster can affect performance and availability of the cluster.
      ii) Riavviare il canale CLUSSDR (ad esempio, utilizzando il comando START CHANNEL).
      iii) Riavviare il canale CLUSRCVR.
   b) Se il cluster è un cluster di pubblicazione / sottoscrizione e il gestore code di unione ha delle sottoscrizioni, immettere il seguente comando per assicurarsi che le sottoscrizioni proxy siano correttamente sincronizzate nel cluster:

```
REFRESH QMGR TYPE(PROXYSUB)
```

Risultati

La seguente figura mostra il cluster configurato da questa attività.

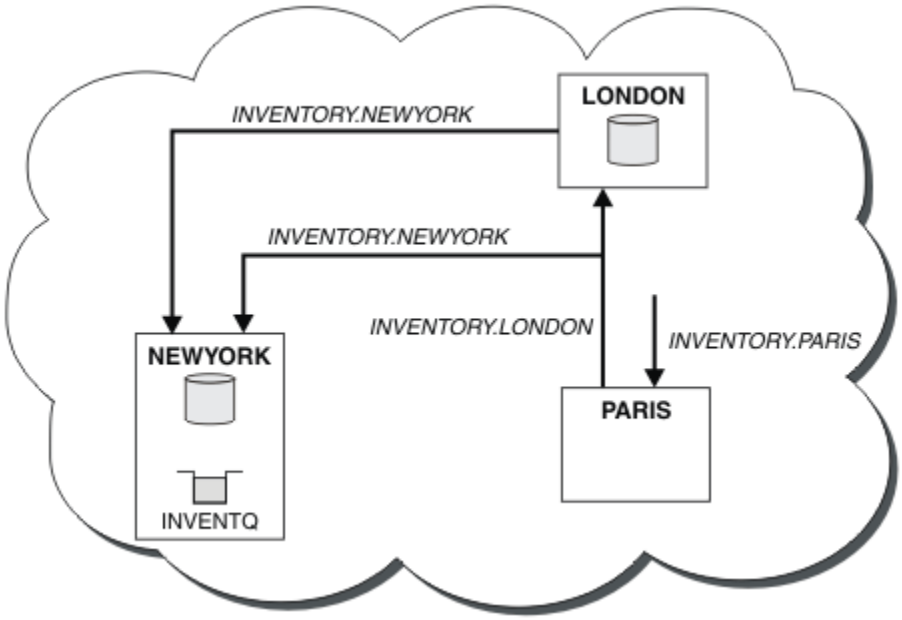


Figura 30. Il cluster INVENTORY con tre gestori code

Creando solo due definizioni, una CLUSRCVR e una CLUSSDR , è stato aggiunto il gestore code PARIS al cluster.

Ora il gestore code PARIS apprende, dal repository completo in LONDON, che la coda INVENTQ è ospitata dal gestore code NEWYORK. Quando un'applicazione ospitata dal sistema a Parigi tenta di inserire i messaggi in INVENTQ, PARIS definisce automaticamente un canale mittente del cluster per connettersi al canale ricevente del cluster INVENTORY.NEWYORK. L'applicazione può ricevere risposte quando il nome del gestore code è specificato come gestore code di destinazione e viene fornita una coda di risposta.

Aggiunta di un gestore code a un cluster: code di trasmissione separate

Seguire queste istruzioni per aggiungere il gestore code al cluster creato. I messaggi per le code cluster e gli argomenti vengono trasferiti utilizzando più code di trasmissione cluster.

Prima di iniziare

- Il gestore code viene definito su una piattaforma diversa da z/OS.
- Il gestore code non è un membro di alcun cluster.
- Il cluster esiste; esiste un repository completo a cui questo gestore code può connettersi direttamente e il repository è disponibile. Per la procedura per creare il cluster, consultare "Configurazione di un nuovo cluster" a pagina 188.

Informazioni su questa attività

Questa attività è un'alternativa a "Aggiunta di un gestore code a un cluster" a pagina 199, in cui si aggiunge un gestore code a un cluster che posiziona i messaggi cluster su una singola coda di trasmissione.

In questa attività, si aggiunge un gestore code a un cluster che crea automaticamente code di trasmissione cluster separate per ogni canale mittente del cluster.

Per mantenere il numero di definizioni di code piccole, il valore predefinito è di utilizzare una singola coda di trasmissione. L'utilizzo di code di trasmissione separate è vantaggioso se si desidera monitorare il traffico destinato a gestori code e cluster differenti. Si potrebbe anche voler separare il traffico verso destinazioni differenti per raggiungere gli obiettivi di isolamento o di prestazioni.

Procedura

1. Modificare il tipo di coda di trasmissione del canale cluster predefinito.

   Modificare il gestore code PARIS:

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

   Ogni volta che il gestore code crea un canale mittente del cluster per inviare un messaggio a un gestore code, crea una coda di trasmissione del cluster. La coda di trasmissione viene utilizzata solo da questo canale mittente del cluster. La coda di trasmissione è permanente - dinamica. Viene creato dalla coda modello, SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE, con il nome SYSTEM.CLUSTER.TRANSMIT.*ChannelName*.

   Attenzione: Se si sta utilizzando SYSTEM.CLUSTER.TRANSMIT.QUEUES dedicato con un gestore code che è stato aggiornato da una versione precedente del prodotto, assicurarsi che SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE abbia l'opzione SHARE/NOSHARE impostata su **SHARE**.
2. Decidere quale repository completo PARIS fa riferimento per primo.

   Ogni gestore code in un cluster deve fare riferimento a uno o più repository completi. Raccoglie le informazioni sul cluster da un repository completo e quindi crea il proprio repository parziale. Scegliere uno dei repository come repository completo. Non appena un nuovo gestore code viene aggiunto al cluster, viene immediatamente a conoscenza dell'altro repository. Le informazioni relative

alle modifiche a un gestore code vengono inviate direttamente a due repository. In questo esempio, si collega PARIS al gestore code LONDON, solo per motivi geografici.

Nota: Eseguire i passi rimanenti in qualsiasi ordine, dopo l'avvio del gestore code PARIS .

3. Definire un canale CLUSRCVR sul gestore code PARIS.

   Ogni gestore code in un cluster deve definire un canale ricevente del cluster su cui può ricevere i messaggi. Su PARIS, definire:

   ```
   DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(PARIS.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for queue manager PARIS')
   ```

   Il canale ricevente del cluster annuncia la disponibilità del gestore code a ricevere messaggi da altri gestori code nel cluster INVENTORY. Non è necessario creare definizioni su altri gestori code per l'invio al canale ricevente del cluster INVENTORY.PARIS. Le altre definizioni vengono effettuate automaticamente quando necessario.

4. Definire un canale CLUSSDR nel gestore code PARIS.

   Ogni gestore code in un cluster deve definire un canale mittente del cluster su cui inviare i messaggi al repository completo iniziale.

   Su PARIS, creare la seguente definizione per un canale denominato INVENTORY.LONDON al gestore code con indirizzo di rete LONDON.CHSTORE.COM.

   ```
   DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from PARIS to repository at LONDON')
   ```

   Il gestore code crea automaticamente la coda di trasmissione del cluster dinamico permanente SYSTEM.CLUSTER.TRANSMIT.INVENTORY.LONDON dalla coda modello SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE. Imposta l'attributo CLCHNAME della coda di trasmissione su INVENTORY.LONDON.

Risultati

La seguente figura mostra il cluster configurato da questa attività.

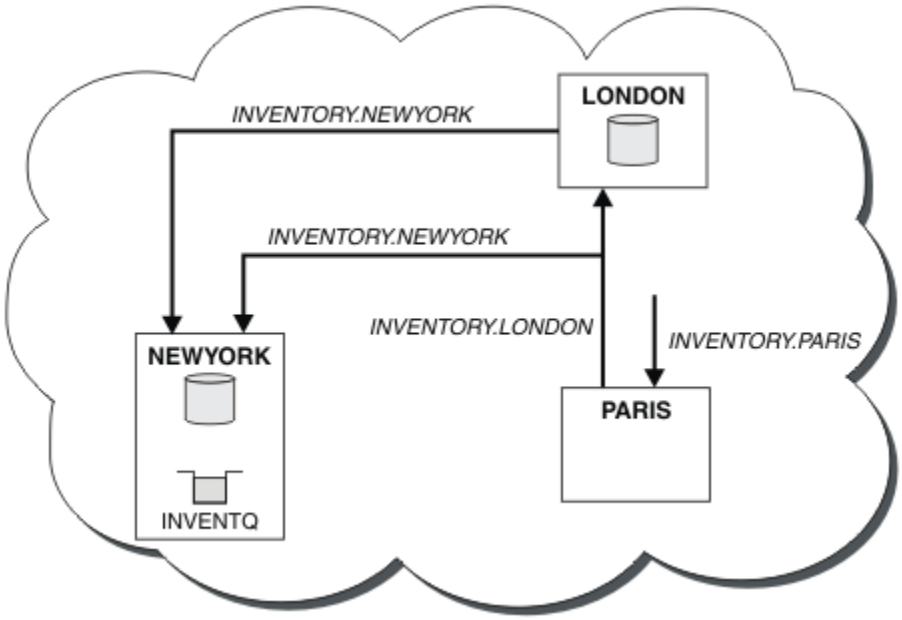


Figura 31. Il cluster INVENTORY con tre gestori code

Creando solo due definizioni, una CLUSRCVR e una CLUSSDR , è stato aggiunto il gestore code PARIS al cluster.

Ora il gestore code PARIS apprende, dal repository completo in LONDON, che la coda INVENTQ è ospitata dal gestore code NEWYORK. Quando un'applicazione ospitata dal sistema a Parigi tenta di inserire i messaggi in INVENTQ, PARIS definisce automaticamente un canale mittente del cluster per connettersi al canale ricevente del cluster INVENTORY.NEWYORK. L'applicazione può ricevere risposte quando il nome del gestore code è specificato come gestore code di destinazione e viene fornita una coda di risposta.

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

Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una definizione remota della coda cluster e un canale mittente e una coda di trasmissione separati.

Prima di iniziare

Creare i cluster sovrapposti mostrati in Figura 37 a pagina 221 in “Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221 seguendo i passi in tale attività.

Informazioni su questa attività

La soluzione utilizza l'accodamento distribuito per separare i messaggi per l'applicazione Server App dal traffico di altri messaggi sul gestore code gateway. È necessario definire una definizione di coda remota con cluster su QM1 per deviare i messaggi su una coda di trasmissione e su un canale diversi. La definizione della coda remota deve includere un riferimento alla specifica coda di trasmissione che memorizza i messaggi solo per Q1 su QM3. In Figura 32 a pagina 204, l'alias della coda cluster Q1A è integrato da una definizione della coda remota Q1Re sono aggiunti una coda di trasmissione e un canale mittente.

In questa soluzione, tutti i messaggi di risposta vengono restituiti utilizzando il comune SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Il vantaggio di questa soluzione è che è facile separare il traffico per più code di destinazione sullo stesso gestore code, nello stesso cluster. Lo svantaggio della soluzione è che non è possibile utilizzare il bilanciamento del carico di lavoro del cluster tra più copie di Q1 su gestori code differenti. Per superare questo svantaggio, consultare “Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 206. È inoltre necessario gestire la commutazione da una coda di trasmissione all'altra.

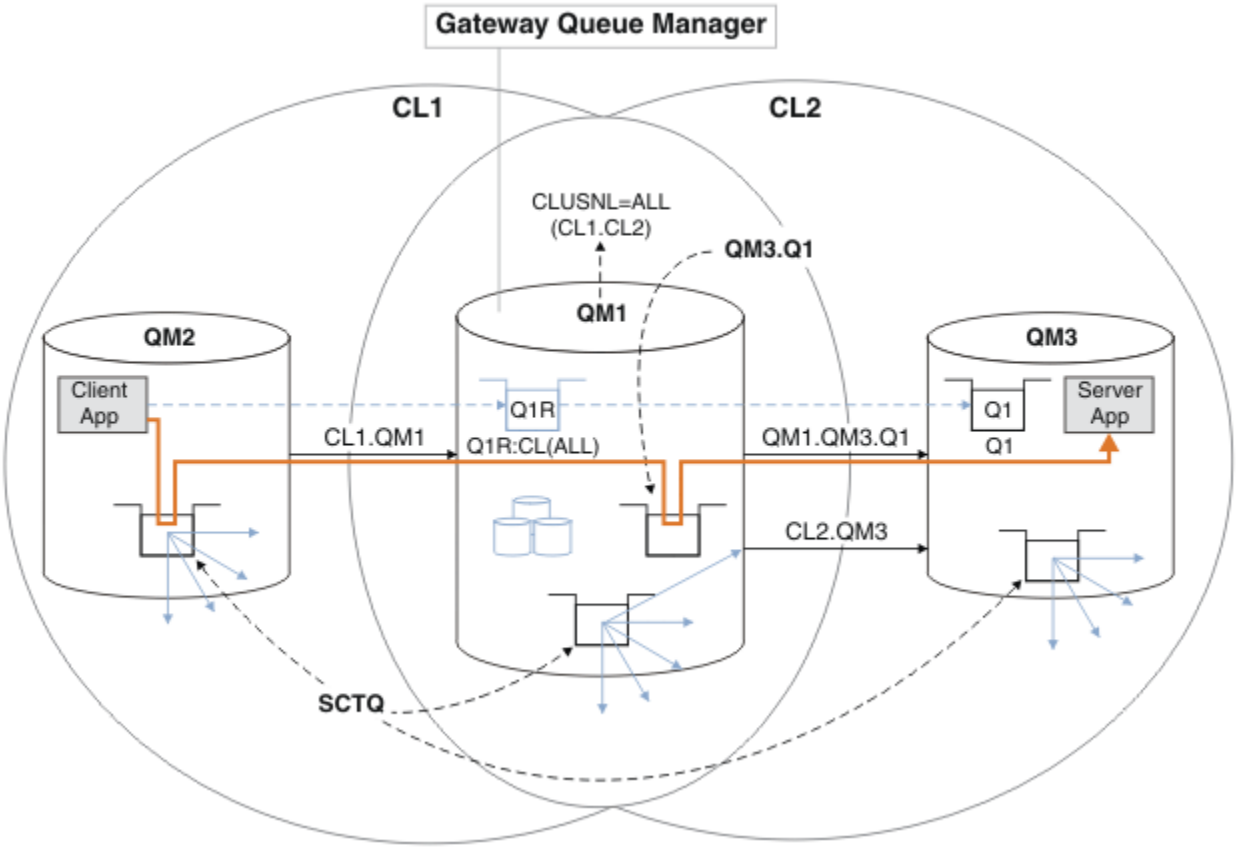


Figura 32. Applicazione client-server distribuita all'architettura del cluster hub e spoke utilizzando definizioni di coda remota

Procedura

1. Creare un canale per separare il traffico di messaggi per Q1 dal gestore code gateway
   a) Creare un canale mittente sul gestore code del gateway, QM1, sul gestore code di destinazione, QM3.

   ```
   DEFINE CHANNEL(QM1.QM3.Q1) CHLTYPE(SDR) CONNAME(QM3HostName(1413)) XMITQ(QM3.Q1) REPLACE
   ```

   b) Creare un canale ricevente sul gestore code di destinazione, QM3.

   ```
   DEFINE CHANNEL(QM1.QM3.Q1) CHLTYPE(RCVR) REPLACE
   ```

2. Creare una coda di trasmissione sul gestore code del gateway per il traffico di messaggi verso Q1

   ```
   DEFINE QLOCAL(QM3.Q1) USAGE(XMITQ) REPLACE
   START CHANNEL(QM1.QM3.Q1)
   ```

   L'avvio del canale associato alla coda di trasmissione associa la coda di trasmissione al canale. Il canale viene avviato automaticamente, una volta che la coda di trasmissione è stata associata al canale.
3. Integrare la definizione dell'alias della coda con cluster per Q1 sul gestore code del gateway con una definizione della coda remota con cluster.

   ```
   DEFINE QREMOTE CLUSNL(ALL) RNAME(Q1) RQMNAME(QM3) XMITQ(QM3.Q1) REPLACE
   ```

Operazioni successive

Verificare la configurazione inviando un messaggio a Q1 su QM3 da QM2 utilizzando la definizione remota della coda cluster Q1R sul gestore code del gateway QM1.

1. Eseguire il programma di esempio **amqsput** su QM2 per inserire un messaggio.

```
C:\IBM\MQ>amqsput Q1R QM2
Sample AMQSPUT0 start
target queue is Q1R
Sample request message from QM2 to Q1 using Q1R

Sample AMQSPUT0 end
```

2. Eseguire il programma di esempio **amqsget** per richiamare il messaggio da Q1 on QM3

```
C:\IBM\MQ>amqsget Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1R>
no more messages
Sample AMQSGET0 end
```

Concetti correlati

“Controllo accessi e code di trasmissione di più cluster” a pagina 163
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.QUEUEo la verifica rispetto ai profili locali per la coda del cluster o il gestore code del cluster.

“Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 288
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

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 201
Seguire queste istruzioni per aggiungere il gestore code al cluster creato. I messaggi per le code cluster e gli argomenti vengono trasferiti utilizzando più code di trasmissione cluster.

“Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221
Seguire le istruzioni nell'attività per creare cluster sovrapposti con un gestore code del gateway. Utilizzare i cluster come punto iniziale per i seguenti esempi di isolamento dei messaggi in un'applicazione da messaggi in altre applicazioni in un cluster.

“Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway” a pagina 203
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una definizione remota della coda cluster e un canale mittente e una coda di trasmissione separati.

“Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi” a pagina 226
È possibile modificare il modo predefinito in cui un gestore code memorizza i messaggi per una coda cluster o un argomento su una coda di trasmissione. La modifica del valore predefinito fornisce un modo per isolare i messaggi cluster su 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” a pagina 206
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una coda di trasmissione cluster aggiuntiva per separare il traffico di messaggi a un singolo gestore code in un cluster.

“Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 209

Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza un cluster aggiuntivo per isolare i messaggi in una particolare coda cluster.

"Clustering: pianificazione della configurazione delle code di trasmissione del cluster" a pagina 291
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. La configurazione di più code di trasmissione cluster si applica a piattaforme diverse da z/OS.

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

Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una coda di trasmissione cluster aggiuntiva per separare il traffico di messaggi a un singolo gestore code in un cluster.

Prima di iniziare

1. Il gestore code del gateway deve essere su Version 7.5o versione successiva e su una piattaforma diversa da z/OS.
2. Creare i cluster sovrapposti mostrati in Figura 37 a pagina 221 in "Creazione di cluster a due sovrapposizioni con un gestore code del gateway" a pagina 221 seguendo i passi in tale attività.

Informazioni su questa attività

Sul gestore code del gateway, QM1, aggiungere una coda di trasmissione e impostarne l'attributo di coda CLCHNAME. Impostare CLCHNAME sul nome del canale ricevente del cluster su QM3; consultare Figura 33 a pagina 207.

Questa soluzione presenta una serie di vantaggi rispetto alla soluzione descritta in "Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway" a pagina 203:

- Richiede meno definizioni aggiuntive.
- Supporta il bilanciamento del carico di lavoro tra più copie della coda di destinazione, Q1, su gestori code differenti nello stesso cluster, CL2.
- Il gestore code del gateway passa automaticamente alla nuova configurazione quando il canale viene riavviato senza perdere alcun messaggio.
- Il gestore code del gateway continua ad inoltrare i messaggi nello stesso ordine in cui li ha ricevuti. Ciò avviene anche se lo switch si verifica con i messaggi per la coda Q1 a QM3 ancora su SYSTEM.CLUSTER.TRANSMIT.QUEUE.

La configurazione per isolare il traffico di messaggi cluster in Figura 33 a pagina 207 non risulta in un isolamento del traffico tanto grande quanto la configurazione che utilizza le code remote in "Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway" a pagina 203. Se il gestore code QM3 in CL2 ospita diverse code cluster e applicazioni server, tutte queste code condividono il canale cluster, CL2.QM3, connettendo QM1 a QM3. I flussi aggiuntivi sono illustrati in Figura 33 a pagina 207 dalla freccia grigia che rappresenta il potenziale traffico di messaggi cluster da SYSTEM.CLUSTER.TRANSMIT.QUEUE al canale mittente del cluster CL2.QM3.

Il rimedio consiste nel limitare il gestore code ad ospitare una coda cluster in uno specifico cluster. Se il gestore code ospita già un certo numero di code cluster, per soddisfare questa limitazione è necessario creare un altro gestore code o un altro cluster; consultare "Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway" a pagina 209.

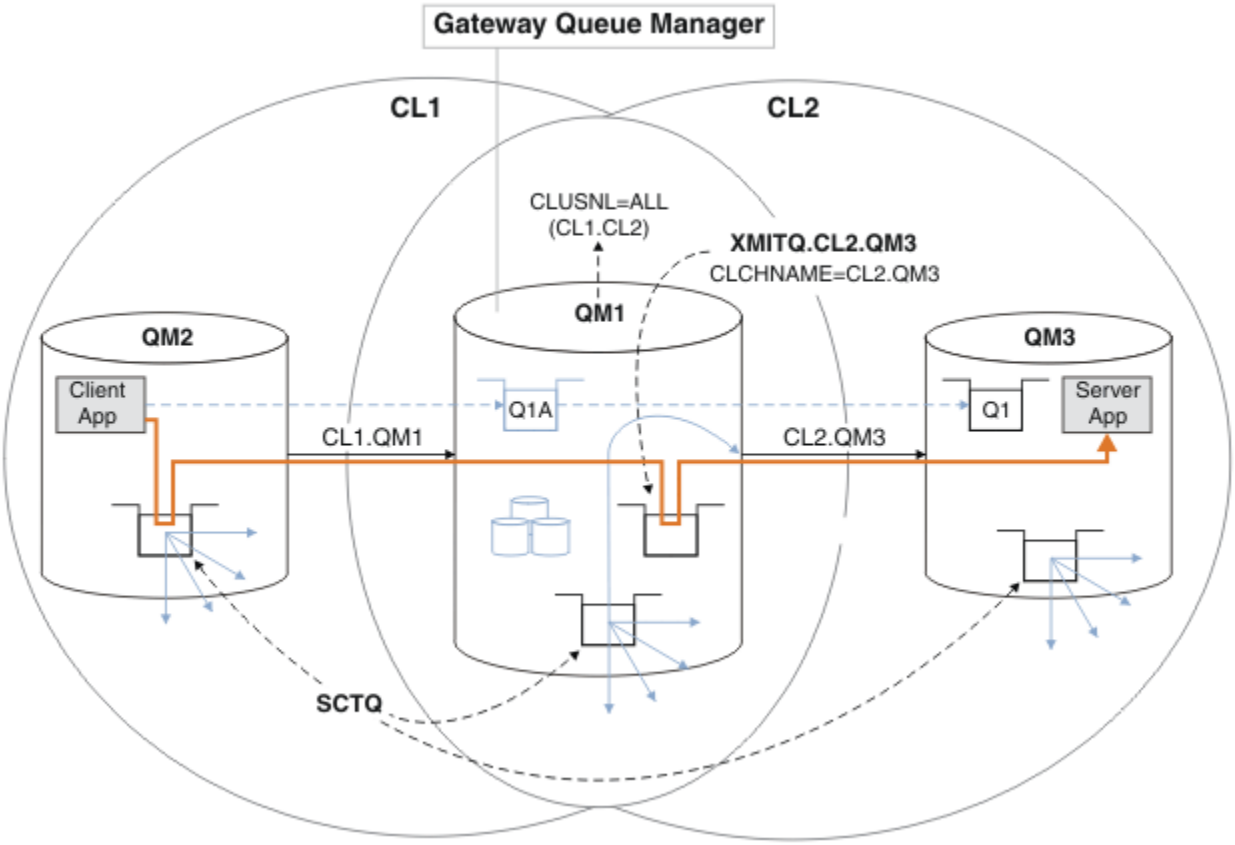


Figura 33. Applicazione client-server distribuita all'architettura hub e spoke utilizzando una coda di trasmissione cluster aggiuntiva.

Procedura

1. Creare un'ulteriore coda di trasmissione del cluster per il canale mittente del cluster `CL2.QM3` sul gestore code del gateway, `QM1`.

```
*... on QM1
DEFINE QLOCAL(XMITQ.CL2.QM3) USAGE(XMITQ) CLCHNAME(CL2.QM3)
```

2. Passare all'utilizzo della coda di trasmissione, `XMITQ.CL2.QM3`.
   a) Arrestare il canale mittente del cluster `CL2.QM3`.

```
*... On QM1
STOP CHANNEL(CL2.QM3)
```

   La risposta è che il comando è accettato:

```
AMQ8019: Stop WebSphere MQ channel accepted.
```

   b) Verificare che il canale `CL2.QM3` sia arrestato

   Se il canale non si arresta, è possibile eseguire nuovamente il comando **STOP CHANNEL** con l'opzione FORCE . Un esempio di impostazione dell'opzione FORCE è se il canale non si arresta e non è possibile riavviare l'altro gestore code per sincronizzare il canale.

```
*... On QM1
start
```

   La risposta è un riepilogo dello stato del canale

```
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM3)              CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1413))      CURRENT
   RQMNAME(QM3)                  STATUS(STOPPED)
   SUBSTATE(MQGET)               XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

c) Avviare il canale, CL2.QM3.

```
*... On QM1
START CHANNEL(CL2.QM3)
```

La risposta è che il comando è accettato:

```
AMQ8018: Start WebSphere MQ channel accepted.
```

d) Verificare che il canale sia stato avviato.

```
*... On QM1
DISPLAY CHSTATUS(CL2.QM3)
```

La risposta è un riepilogo dello stato del canale:

```
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM3)                  CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1413))          CURRENT
   RQMNAME(QM3)                      STATUS(RUNNING)
   SUBSTATE(MQGET)                   XMITQ(XMITQ.CL2.QM3)
```

e) Controllare che la coda di trasmissione sia stata commutata.

Monitorare il file di registrazione errori del gestore code del gateway per il messaggio "AMQ7341 La coda di trasmissione per il canale CL2.QM3 è XMITQ.CL2.QM3".

Operazioni successive

Verificare la coda di trasmissione separata inviando un messaggio da QM2 a Q1 on QM3 utilizzando la definizione dell'alias della coda Q1A

1. Eseguire il programma di esempio **amqsput** su QM2 per inserire un messaggio.

```
C:\IBM\MQ>amqsput Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

Sample AMQSPUT0 end
```

2. Eseguire il programma di esempio **amqsget** per richiamare il messaggio da Q1 on QM3

```
C:\IBM\MQ>amqsget Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1A>
no more messages
Sample AMQSGET0 end
```

Concetti correlati

“Controllo accessi e code di trasmissione di più cluster” a pagina 163
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.QUEUEo la verifica rispetto ai profili locali per la coda del cluster o il gestore code del cluster.

“Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 288
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.

“Code di trasmissione cluster e canali mittente cluster” a pagina 174
I messaggi tra i gestori code con cluster vengono memorizzati nelle code di trasmissione cluster e inoltrati dai canali mittenti del cluster.

Attività correlate

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 201
Seguire queste istruzioni per aggiungere il gestore code al cluster creato. I messaggi per le code cluster e gli argomenti vengono trasferiti utilizzando più code di trasmissione cluster.

“Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221
Seguire le istruzioni nell'attività per creare cluster sovrapposti con un gestore code del gateway. Utilizzare i cluster come punto iniziale per i seguenti esempi di isolamento dei messaggi in un'applicazione da messaggi in altre applicazioni in un cluster.

“Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway” a pagina 203
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una definizione remota della coda cluster e un canale mittente e una coda di trasmissione separati.

“Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi” a pagina 226
È possibile modificare il modo predefinito in cui un gestore code memorizza i messaggi per una coda cluster o un argomento su una coda di trasmissione. La modifica del valore predefinito fornisce un modo per isolare i messaggi cluster su 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” a pagina 206
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una coda di trasmissione cluster aggiuntiva per separare il traffico di messaggi a un singolo gestore code in un cluster.

“Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 209
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza un cluster aggiuntivo per isolare i messaggi in una particolare coda cluster.

“Clustering: pianificazione della configurazione delle code di trasmissione del cluster” a pagina 291
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. La configurazione di più code di trasmissione cluster si applica a piattaforme diverse da z/OS.

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

Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza un cluster aggiuntivo per isolare i messaggi in una particolare coda cluster.

Prima di iniziare

I passi nell'attivit ... vengono scritti per modificare la configurazione illustrata in Figura 33 a pagina 207.

1. Il gestore code del gateway deve essere su Version 7.5o versione successiva e su una piattaforma diversa da z/OS.
2. Creare i cluster sovrapposti mostrati in Figura 37 a pagina 221 in "Creazione di cluster a due sovrapposizioni con un gestore code del gateway" a pagina 221 seguendo i passi in tale attività.
3. Eseguire le operazioni in Figura 33 a pagina 207in "Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway" a pagina 206 per creare la soluzione senza il cluster aggiuntivo. Utilizzarlo come base per i passaggi in questa attività.

Informazioni su questa attività

La soluzione per isolare il traffico di messaggi a una singola applicazione in "Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway" a pagina 206 funziona se la coda del cluster di destinazione è l'unica coda del cluster su un gestore code. Se non lo è, hai due scelte. Spostare la coda in un gestore code differente oppure creare un cluster che isoli la coda da altre code cluster sul gestore code.

Questa attività consente di aggiungere un cluster per isolare la coda di destinazione. Il cluster viene aggiunto solo per tale scopo. In pratica, affrontare l'attività di isolare sistematicamente alcune applicazioni quando si stanno progettando i cluster e gli schemi di denominazione dei cluster. L'aggiunta di un cluster ogni volta che una coda richiede l'isolamento potrebbe finire con molti cluster da gestire. In questa attività, si modifica la configurazione in "Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway" a pagina 206 aggiungendo un cluster `CL3` per isolare `Q1` su `QM3`. Le applicazioni continuano ad essere eseguite per tutta la durata della modifica.

Le nuove definizioni e quelle modificate vengono evidenziate in Figura 34 a pagina 211. Il riepilogo delle modifiche è il seguente: creare un cluster, il che significa che è necessario creare anche un nuovo repository cluster completo. Nell'esempio, `QM3` è uno dei repository completi per `CL3`. Creare i canali mittente cluster e ricevente cluster per `QM1`per aggiungere il gestore code gateway al nuovo cluster. Modificare la definizione di `Q1` per passare a `CL3`. Modificare l'elenco nomi del cluster sul gestore code del gateway e aggiungere una coda di trasmissione del cluster per utilizzare il nuovo canale cluster. Infine, passare l'alias della coda `Q1A` al nuovo elenco nomi cluster.

IBM WebSphere MQ non può trasferire automaticamente i messaggi dalla coda di trasmissione `XMITQ.CL2.QM3` aggiunta in "Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway" a pagina 206 alla nuova coda di trasmissione `XMITQ.CL3.QM3`. Può trasferire automaticamente i messaggi solo se entrambe le code di trasmissione sono servite dallo stesso canale mittente del cluster. Invece, l'attività descrive un modo per eseguire lo switch manualmente, che potrebbe essere appropriato per l'utente. Una volta completato il trasferimento, è possibile ripristinare l'uso della coda di trasmissione del cluster predefinita per altre code del cluster `CL2` su `QM3`. In alternativa, è possibile continuare a utilizzare `XMITQ.CL2.QM3`. Se si decide di ripristinare una coda di trasmissione del cluster predefinita, il gestore code del gateway gestisce automaticamente lo switch.

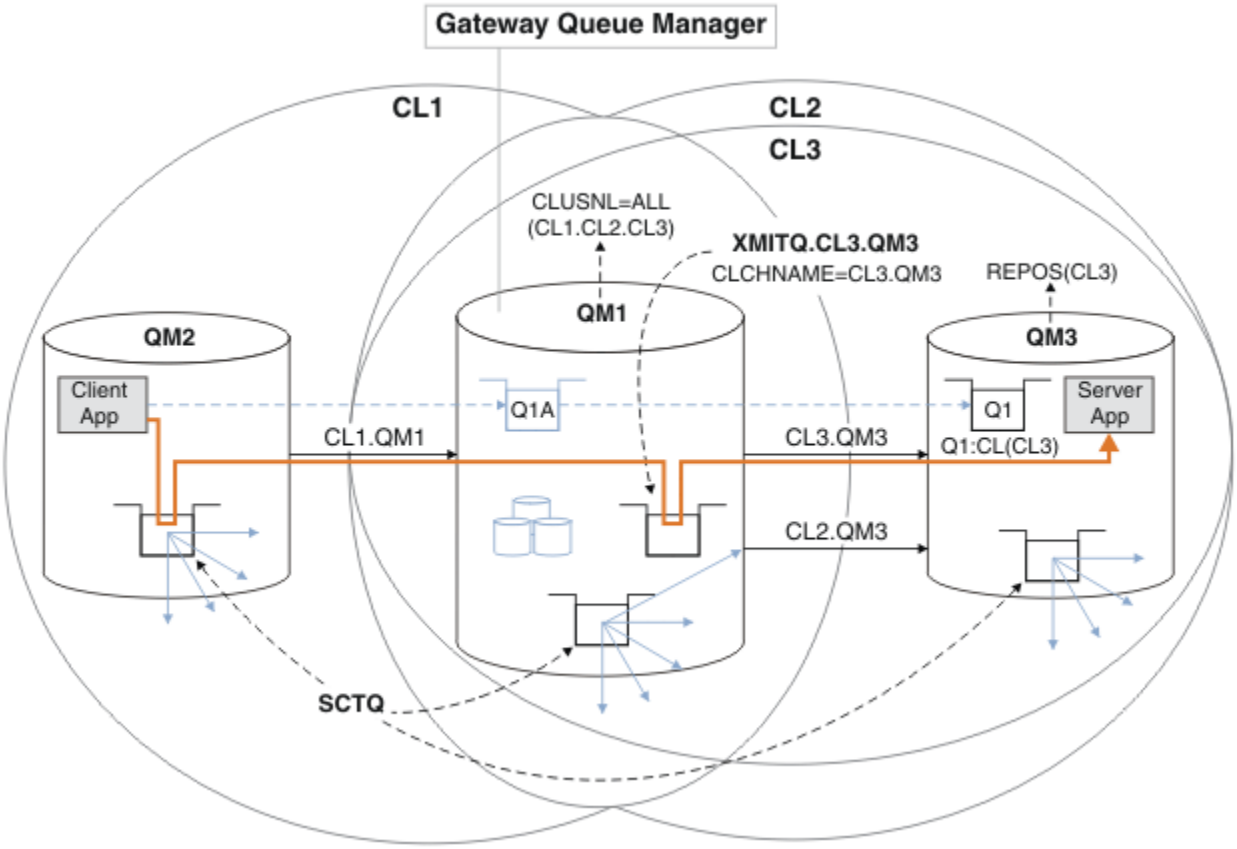


Figura 34. Utilizzo di un ulteriore cluster per separare il traffico di messaggi nel gestore code del gateway che va a una delle diverse code del cluster sullo stesso gestore code

Procedura

1. Modificare i gestori code QM3 e QM5 per renderli repository sia per CL2 che per CL3.

   Per rendere un gestore code membro di più cluster, deve utilizzare un elenco di nomi cluster per identificare i cluster di cui è membro.

   ```
   *... On QM3 and QM5
   DEFINE NAMELIST(CL23) NAMES(CL2, CL3) REPLACE
   ALTER QMGR REPOS(' ') REPOSNL(CL23)
   ```

2. Definire i canali tra i gestori code QM3 e QM5 per CL3.

   ```
   *... On QM3
   DEFINE CHANNEL(CL3.QM5) CHLTYPE(CLUSSDR)  CONNAME('localhost(1415)') CLUSTER(CL3) REPLACE
   DEFINE CHANNEL(CL3.QM3) CHLTYPE(CLUSRCVR) CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE

   *... On QM5
   DEFINE CHANNEL(CL3.QM3) CHLTYPE(CLUSSDR)  CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE
   DEFINE CHANNEL(CL3.QM5) CHLTYPE(CLUSRCVR) CONNAME('localhost(1415)') CLUSTER(CL3) REPLACE
   ```

3. Aggiungere il gestore code del gateway a CL3.

   Aggiungere il gestore code del gateway aggiungendo QM1 a CL3 come repository parziale. Creare un repository parziale aggiungendo i canali mittente cluster e ricevente cluster a QM1.

   Aggiungere inoltre CL3 all'elenco dei nomi di tutti i cluster connessi al gestore code del gateway.

   ```
   *... On QM1
   DEFINE CHANNEL(CL3.QM3) CHLTYPE(CLUSSDR)  CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE
   DEFINE CHANNEL(CL3.QM1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1411)') CLUSTER(CL3) REPLACE
   ALTER NAMELIST(ALL) NAMES(CL1, CL2, CL3)
   ```

4. Aggiungere una coda di trasmissione cluster al gestore code del gateway, QM1, per i messaggi che vanno a CL3 su QM3.

   Inizialmente, arrestare il canale mittente del cluster che trasferisce i messaggi dalla coda di trasmissione finché non si è pronti a commutare le code di trasmissione.

   ```
   *... On QM1
   DEFINE QLOCAL(XMITQ.CL3.QM3) USAGE(XMITQ) CLCHNAME(CL3.QM3) GET(DISABLED) REPLACE
   ```

5. Eliminare i messaggi dalla coda di trasmissione del cluster esistente XMITQ.CL2.QM3.

   Questa sottoprocedura è intesa a preservare l'ordine dei messaggi in Q1 in modo che corrisponda all'ordine in cui sono arrivati al gestore code del gateway. Con i cluster, l'ordinamento dei messaggi non è completamente garantito, ma è probabile. Se è richiesto l'ordine garantito dei messaggi, le applicazioni devono definirne l'ordine. Consultare L'ordine in cui i messaggi vengono richiamati da una coda.

   a) Modificare la coda di destinazione Q1 su QM3 da CL2 a CL3.

   ```
   *... On QM3
   ALTER QLOCAL(Q1) CLUSTER(CL3)
   ```

   b) Monitorare XMITQ.CL3.QM3 fino a quando i messaggi non iniziano ad essere consegnati.

   I messaggi vengono consegnati a XMITQ.CL3.QM3 quando il passaggio di Q1 a CL3 viene propagato al gestore code del gateway.

   ```
   *... On QM1
   DISPLAY QUEUE(XMITQ.CL3.QM3) CURDEPTH
   ```

   c) Monitorare XMITQ.CL2.QM3 fino a quando non ha alcun messaggio in attesa di essere consegnato a Q1 su QM3.

   Nota: XMITQ.CL2.QM3 potrebbe memorizzare messaggi per altre code su QM3 che sono membri di CL2, nel qual caso la profondità potrebbe non andare a zero.

   ```
   *... On QM1
   DISPLAY QUEUE(XMITQ.CL2.QM3) CURDEPTH
   ```

   d) Abilitare il richiamo dalla nuova coda di trasmissione del cluster, XMITQ.CL3.QM3

   ```
   *... On QM1
   ALTER QLOCAL(XMITQ.CL3.QM3) GET(ENABLED)
   ```

6. Rimuovere la vecchia coda di trasmissione del cluster, XMITQ.CL2.QM3, se non è più richiesta.

   I messaggi per le code del cluster in CL2 su QM3 ritornano all'utilizzo della coda di trasmissione del cluster predefinita sul gestore code del gateway, QM1. La coda di trasmissione cluster predefinita è SYSTEM.CLUSTER.TRANSMIT.QUEUEo SYSTEM.CLUSTER.TRANSMIT.CL2.QM3. La scelta dipende dal fatto che il valore dell'attributo del gestore code **DEFCLXQ** su QM1 sia SCTQ o CHANNEL. Il gestore code trasferisce i messaggi da XMITQ.CL2.QM3 automaticamente al successivo avvio del canale mittente del cluster CL2.QM3 .

   a) Modificare la coda di trasmissione, XMITQ.CL2.QM3, da coda di trasmissione cluster a coda di trasmissione normale.

   Ciò interrompe l'associazione della coda di trasmissione con qualsiasi canale mittente del cluster. In risposta, IBM WebSphere MQ trasferisce automaticamente i messaggi da XMITQ.CL2.QM3 nella coda di trasmissione del cluster predefinita al successivo avvio del canale mittente del cluster. Fino a quel momento, i messaggi per CL2 su QM3 continuano a essere posizionati su XMITQ.CL2.QM3.

   ```
   *... On QM1
   ALTER QLOCAL(XMITQ.CL2.QM3) CLCHNAME(' ')
   ```

b) Arrestare il canale mittente del cluster CL2.QM3.

L'arresto e il riavvio del canale mittente del cluster avvia il trasferimento dei messaggi da XMITQ.CL2.QM3 nella coda di trasmissione del cluster predefinita. In genere si arresta e si avvia il canale manualmente per avviare il trasferimento. Il trasferimento viene avviato automaticamente se il canale viene riavviato dopo la chiusura alla scadenza del suo intervallo di disconnessione.

```
*... On QM1
STOP CHANNEL(CL2.QM3)
```

La risposta è che il comando è accettato:

```
AMQ8019: Stop WebSphere MQ channel accepted.
```

c) Verificare che il canale CL2.QM3 sia arrestato

Se il canale non si arresta, è possibile eseguire nuovamente il comando **STOP CHANNEL** con l'opzione FORCE . Un esempio di impostazione dell'opzione FORCE è se il canale non si arresta e non è possibile riavviare l'altro gestore code per sincronizzare il canale.

```
*... On QM1
DISPLAY CHSTATUS(CL2.QM3)
```

La risposta è un riepilogo dello stato del canale

```
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM3)                        CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1413))                CURRENT
   RQMNAME(QM3)                            STATUS(STOPPED)
   SUBSTATE(MQGET)                         XMITQ(XMITQ.CL2.QM3)
```

d) Avviare il canale, CL2.QM3.

```
*... On QM1
START CHANNEL(CL2.QM3)
```

La risposta è che il comando è accettato:

```
AMQ8018: Start WebSphere MQ channel accepted.
```

e) Verificare che il canale sia stato avviato.

```
*... On QM1
DISPLAY CHSTATUS(CL2.QM3)
```

La risposta è un riepilogo dello stato del canale:

```
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM3)           CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1413))   CURRENT
   RQMNAME(QM3)               STATUS(RUNNING)
   SUBSTATE(MQGET)            XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE|CL2.QM3)
```

f) Monitorare il file di registrazione errori del gestore code del gateway per il messaggio "AMQ7341 La coda di trasmissione per il canale CL2.QM3 è SYSTEM.CLUSTER.TRANSMIT.*QUEUE | CL2.QM3*".

g) Eliminare la coda di trasmissione cluster, XMITQ.CL2.QM3.

```
*... On QM1
DELETE QLOCAL(XMITQ.CL2.QM3)
```

Operazioni successive

Verificare la coda con cluster separata inviando un messaggio da QM2 a Q1 su QM3 utilizzando la definizione alias della coda Q1A

1. Eseguire il programma di esempio **amqsput** su QM2 per inserire un messaggio.

```
C:\IBM\MQ>amqsput Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

Sample AMQSPUT0 end
```

2. Eseguire il programma di esempio **amqsget** per richiamare il messaggio da Q1 on QM3

```
C:\IBM\MQ>amqsget Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1A>
no more messages
Sample AMQSGET0 end
```

Concetti correlati

“Controllo accessi e code di trasmissione di più cluster” a pagina 163
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.QUEUEo la verifica rispetto ai profili locali per la coda del cluster o il gestore code del cluster.

“Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 288
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.

“Code di trasmissione cluster e canali mittente cluster” a pagina 174
I messaggi tra i gestori code con cluster vengono memorizzati nelle code di trasmissione cluster e inoltrati dai canali mittenti del cluster.

Attività correlate

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 201
Seguire queste istruzioni per aggiungere il gestore code al cluster creato. I messaggi per le code cluster e gli argomenti vengono trasferiti utilizzando più code di trasmissione cluster.

“Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221
Seguire le istruzioni nell'attività per creare cluster sovrapposti con un gestore code del gateway. Utilizzare i cluster come punto iniziale per i seguenti esempi di isolamento dei messaggi in un'applicazione da messaggi in altre applicazioni in un cluster.

“Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway” a pagina 203
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una definizione remota della coda cluster e un canale mittente e una coda di trasmissione separati.

“Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi” a pagina 226
È possibile modificare il modo predefinito in cui un gestore code memorizza i messaggi per una coda cluster o un argomento su una coda di trasmissione. La modifica del valore predefinito fornisce un modo per isolare i messaggi cluster su 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” a pagina 206

Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una coda di trasmissione cluster aggiuntiva per separare il traffico di messaggi a un singolo gestore code in un cluster.

"Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway" a pagina 209
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza un cluster aggiuntivo per isolare i messaggi in una particolare coda cluster.

"Clustering: pianificazione della configurazione delle code di trasmissione del cluster" a pagina 291
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. La configurazione di più code di trasmissione cluster si applica a piattaforme diverse da z/OS.

Aggiunta di un gestore code a un cluster utilizzando DHCP

Aggiungere un gestore code a un cluster utilizzando DHCP. L'attività illustra l'omissione del valore CONNAME su una definizione CLUSRCVR .

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

L'attività dimostra due funzioni speciali:

- La capacità di omettere il valore CONNAME su una definizione CLUSRCVR .
- La capacità di utilizzare +QMNAME+ su una definizione CLUSSDR .

Nessuna funzione viene fornita su z/OS.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in "Configurazione di un nuovo cluster" a pagina 188. Contiene due gestori code, LONDON e NEWYORK, che contengono entrambi repository completi.
- Una nuova filiale della catena di negozi è in fase di configurazione a Parigi e si desidera aggiungere al cluster un gestore code denominato PARIS .
- Il gestore code PARIS invia aggiornamenti di inventario all'applicazione in esecuzione sul sistema a New York inserendo i messaggi nella coda INVENTQ.
- La connettività di rete esiste tra tutti e tre i sistemi.
- Il protocollo di rete è TCP.
- Il sistema del gestore code PARIS utilizza DHCP, il che significa che gli indirizzi IP potrebbero cambiare al riavvio del sistema.
- I canali tra i sistemi PARIS e LONDON vengono denominati in base a una convenzione di denominazione definita. La convenzione utilizza il nome del gestore code del repository completo su LONDON.
- Gli amministratori del gestore code PARIS non hanno informazioni sul nome del gestore code sul repository LONDON . Il nome del gestore code sul repository LONDON è soggetto a modifica.

Informazioni su questa attività

Effettuare le operazioni riportate di seguito per aggiungere un gestore code a un cluster utilizzando DHCP.

Procedura

1. Decidere quale repository completo PARIS fa riferimento per primo.

   Ogni gestore code in un cluster deve fare riferimento a uno o più repository completi. Raccoglie le informazioni sul cluster da un repository completo e quindi crea il proprio repository parziale. Scegliere uno dei repository come repository completo. Non appena un nuovo gestore code viene aggiunto al cluster, viene immediatamente a conoscenza dell'altro repository. Le informazioni relative alle modifiche a un gestore code vengono inviate direttamente a due repository. In questo esempio si sceglie di collegare PARIS al gestore code LONDON, solo per motivi geografici.

   Nota: Eseguire i passi rimanenti in qualsiasi ordine, dopo l'avvio del gestore code PARIS .

2. Definire un canale CLUSRCVR sul gestore code PARIS.

   Ogni gestore code in un cluster deve definire un canale ricevente del cluster su cui può ricevere messaggi. Su PARIS, definire:

   ```
   DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSRCVR)
   TRPTYPE(TCP) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for queue manager PARIS')
   ```

   Il canale ricevente del cluster annuncia la disponibilità del gestore code a ricevere messaggi da altri gestori code nel cluster INVENTORY. Non è necessario specificare CONNAME sul canale ricevente del cluster. È possibile richiedere a IBM WebSphere MQ di individuare il nome della connessione dal sistema, omettendo CONNAMEo specificando CONNAME(' '). IBM WebSphere MQ genera il valore CONNAME utilizzando l'indirizzo IP corrente del sistema; consultare CONNAME. Non è necessario creare definizioni su altri gestori code per l'invio al canale ricevente del cluster INVENTORY.PARIS. Le altre definizioni vengono effettuate automaticamente quando necessario.

3. Definire un canale CLUSSDR sul gestore code PARIS.

   Ogni gestore code in un cluster deve definire un canale mittente del cluster su cui inviare i messaggi al repository completo iniziale. Su PARIS, creare la seguente definizione per un canale denominato INVENTORY.+QMNAME+ al gestore code con indirizzo di rete LONDON.CHSTORE.COM.

   ```
   DEFINE CHANNEL(INVENTORY.+QMNAME+) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from PARIS to repository at LONDON')
   ```

4. Opzionale: Se questo gestore code si sta unendo nuovamente a un cluster, completare alcuni passi aggiuntivi.

   a) Se si sta aggiungendo un gestore code a un cluster che è stato precedentemente rimosso dallo stesso cluster, verificare che venga visualizzato come membro del cluster. In caso contrario, completare i seguenti passi aggiuntivi:

      i) Immettere il comando **REFRESH CLUSTER** sul gestore code che si sta aggiungendo. Questa fase arresta i canali del cluster e fornisce alla tua cache del cluster locale una nuova serie di numeri di sequenza che sono sicuri di essere aggiornati nel resto del cluster.

      ```
      REFRESH CLUSTER(INVENTORY) REPOS(YES)
      ```

      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 gli aggiornamenti di stato a tutti i gestori code interessati. Consultare Refreshing in a large cluster can affect performance and availability of the cluster.

      ii) Riavviare il canale CLUSSDR (ad esempio, utilizzando il comando START CHANNEL).

      iii) Riavviare il canale CLUSRCVR.

   b) Se il cluster è un cluster di pubblicazione / sottoscrizione e il gestore code di unione ha delle sottoscrizioni, immettere il seguente comando per assicurarsi che le sottoscrizioni proxy siano correttamente sincronizzate nel cluster:

```
REFRESH QMGR TYPE(PROXYSUB)
```

Risultati

Il cluster configurato da questa attività è lo stesso di “Aggiunta di un gestore code a un cluster” a pagina 199:

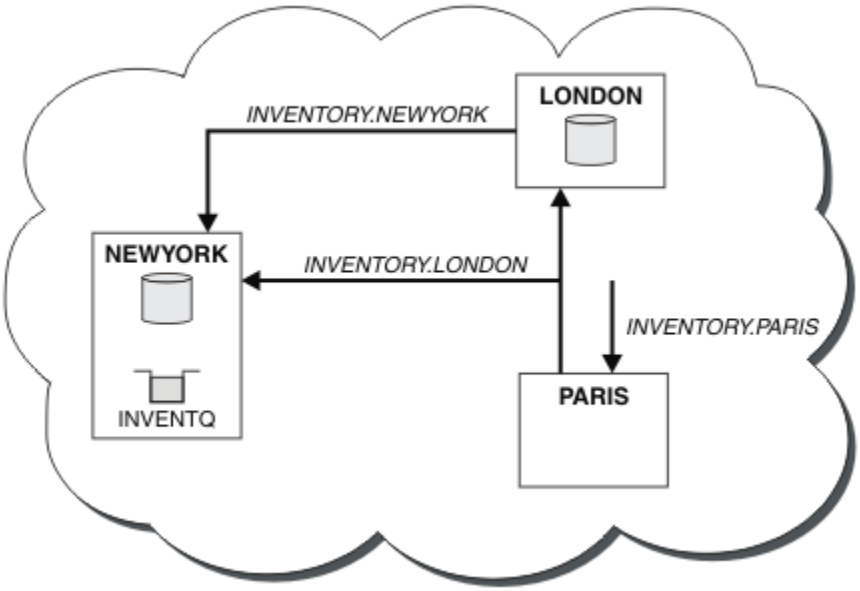


Figura 35. Il cluster INVENTORY con tre gestori code

Creando solo due definizioni, una CLUSRCVR e una definizione CLUSSDR , è stato aggiunto il gestore code PARIS al cluster.

Sul gestore code PARIS , viene avviato il CLUSSDR contenente la stringa +QMNAME+ . Sul sistema LONDON IBM WebSphere MQ risolve +QMNAME+ nel nome del gestore code (LONDON). IBM WebSphere MQ mette quindi in corrispondenza la definizione di un canale denominato INVENTORY.LONDON con la corrispondente definizione CLUSRCVR .

WebSphere MQ restituisce il nome del canale risolto al gestore code PARIS . In PARIS, la definizione di canale CLUSSDR per il canale denominato INVENTORY.+QMNAME+ viene sostituita da una definizione CLUSSDR generata internamente per INVENTORY.LONDON. Questa definizione contiene il nome del canale risolto, ma in caso contrario è uguale alla definizione +QMNAME+ creata. I repository del cluster vengono aggiornati anche con la definizione del canale con il nome del canale appena risolto.

Nota:

1. Il canale creato con il nome +QMNAME+ diventa immediatamente inattivo. Non viene mai utilizzato per trasmettere dati.
2. Le uscite del canale potrebbero vedere la modifica del nome del canale tra una chiamata e la successiva.

Ora il gestore code PARIS apprende, dal repository in LONDON, che la coda INVENTQ è ospitata dal gestore code NEWYORK. Quando un'applicazione ospitata dal sistema a Parigi tenta di inserire i messaggi in INVENTQ, PARIS definisce automaticamente un canale mittente del cluster per connettersi al canale ricevente del cluster INVENTORY.NEWYORK. L'applicazione può ricevere risposte quando il nome del gestore code è specificato come gestore code di destinazione e viene fornita una coda di risposta.

Riferimenti correlati

Definire il canale

Aggiunta di un gestore code su cui è presente una coda

Aggiungere un altro gestore code al cluster, per ospitare un'altra coda INVENTQ . Le richieste vengono inviate alternativamente alle code su ciascun gestore code. Non è necessario apportare modifiche all'host INVENTQ esistente.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in “Aggiunta di un gestore code a un cluster” a pagina 199. Contiene tre gestori code; LONDON e NEWYORK contengono entrambi repository completi, PARIS contiene un repository parziale. L'applicazione di inventario viene eseguita sul sistema a New York, connesso al gestore code NEWYORK . L'applicazione è guidata dall'arrivo di messaggi sulla coda INVENTQ .
- Un nuovo negozio è in fase di allestire a Toronto. Per fornire ulteriore capacità, si desidera eseguire l'applicazione di inventario sul sistema a Toronto e New York.
- La connettività di rete esiste tra tutti e quattro i sistemi.
- Il protocollo di rete è TCP.

Nota: Il gestore code TORONTO contiene solo un repository parziale. Se si desidera aggiungere un gestore code del repository completo a un cluster, fare riferimento a “Spostamento di un repository completo in un altro gestore code” a pagina 233.

Informazioni su questa attività

Effettuare le operazioni riportate di seguito per aggiungere un gestore code su cui è presente una coda.

Procedura

1. Decidere quale repository completo TORONTO fa riferimento per primo.

   Ogni gestore code in un cluster deve fare riferimento a uno o più repository completi. Raccoglie le informazioni sul cluster da un repository completo e quindi crea il proprio repository parziale. Non è di particolare importanza quale repository si sceglie. In questo esempio, si sceglie NEWYORK. Una volta che il nuovo gestore code si è unito al cluster, comunica con entrambi i repository.

2. Definire il canale CLUSRCVR .

   Ogni gestore code in un cluster deve definire un canale ricevente del cluster su cui può ricevere messaggi. Su TORONTO, definire un canale CLUSRCVR :

   ```
   DEFINE CHANNEL(INVENTORY.TORONTO) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(TORONTO.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for TORONTO')
   ```

   Il gestore code TORONTO annuncia la propria disponibilità a ricevere messaggi da altri gestori code nel cluster INVENTORY utilizzando il canale ricevente del cluster.

3. Definire un canale CLUSSDR nel gestore code TORONTO.

   Ogni gestore code di un cluster deve definire un canale mittente del cluster su cui può inviare messaggi al primo repository completo. In questo caso scegliere NEWYORK. TORONTO necessita della seguente definizione:

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from TORONTO to repository at NEWYORK')
   ```

4. Opzionale: Se questo gestore code si sta unendo nuovamente a un cluster, completare alcuni passi aggiuntivi.
   a) Se si sta aggiungendo un gestore code a un cluster che è stato precedentemente rimosso dallo stesso cluster, verificare che venga visualizzato come membro del cluster. In caso contrario, completare i seguenti passi aggiuntivi:
      i) Immettere il comando **REFRESH CLUSTER** sul gestore code che si sta aggiungendo. Questa fase arresta i canali del cluster e fornisce alla tua cache del cluster locale una nuova serie di numeri di sequenza che sono sicuri di essere aggiornati nel resto del cluster.

         ```
         REFRESH CLUSTER(INVENTORY) REPOS(YES)
         ```

         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 gli aggiornamenti di stato a tutti i gestori code interessati. Consultare Refreshing in a large cluster can affect performance and availability of the cluster.
      ii) Riavviare il canale CLUSSDR (ad esempio, utilizzando il comando START CHANNEL).
      iii) Riavviare il canale CLUSRCVR.
   b) Se il cluster è un cluster di pubblicazione / sottoscrizione e il gestore code di unione ha delle sottoscrizioni, immettere il seguente comando per assicurarsi che le sottoscrizioni proxy siano correttamente sincronizzate nel cluster:

      ```
      REFRESH QMGR TYPE(PROXYSUB)
      ```
5. Esaminare l'applicazione inventario per le affinità dei messaggi.

   Prima di procedere, assicurarsi che l'applicazione di inventario non abbia alcuna dipendenza dalla sequenza di elaborazione dei messaggi e installare l'applicazione sul sistema a Toronto.
6. Definire la coda del cluster INVENTQ.

   La coda INVENTQ , che è già ospitata dal gestore code NEWYORK , deve essere ospitata anche da TORONTO. Definirlo sul gestore code TORONTO nel modo seguente:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

Risultati

Figura 36 a pagina 220 mostra il cluster INVENTORY configurato da questa attività.

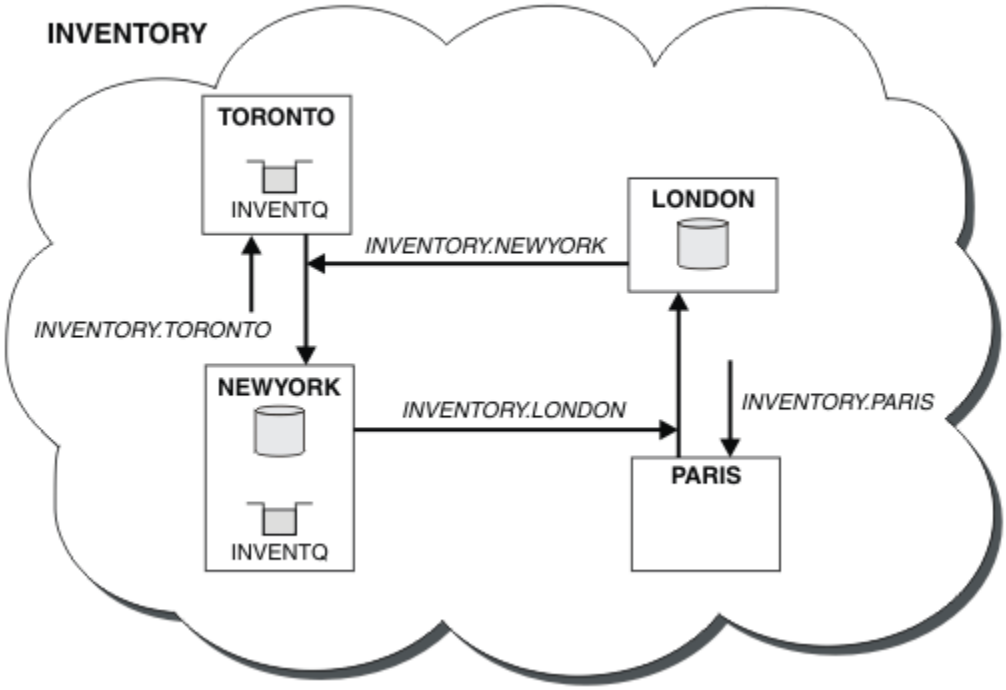


Figura 36. Il cluster INVENTORY con quattro gestori code

La coda INVENTQ e l'applicazione di inventario si trovano ora su due gestori code nel cluster. Ciò aumenta la loro disponibilità, velocizza la velocità di trasmissione dei messaggi e consente la distribuzione del carico di lavoro tra i due gestori code. I messaggi inseriti in INVENTQ da TORONTO o NEWYORK vengono gestiti dall'istanza sul gestore code locale quando possibile. I messaggi immessi da LONDON o PARIS vengono instradati alternativamente a TORONTO o NEWYORK, in modo che il carico di lavoro sia bilanciato.

Questa modifica al cluster è stata effettuata senza che fosse necessario modificare le definizioni sui gestori code NEWYORK, LONDONe PARIS. I repository completi in questi gestori code vengono aggiornati automaticamente con le informazioni necessarie per inviare messaggi a INVENTQ all'indirizzo TORONTO. L'applicazione di inventario continua a funzionare se uno dei gestori code NEWYORK o TORONTO diventa non disponibile e dispone di capacità sufficiente. L'applicazione di inventario deve essere in grado di funzionare correttamente se è ospitata in entrambe le ubicazioni.

Come si può vedere dal risultato di questa attività, è possibile avere la stessa applicazione in esecuzione su più di un gestore code. È possibile eseguire il clustering per distribuire il carico di lavoro in modo uniforme.

Un'applicazione potrebbe non essere in grado di elaborare i record in entrambe le collocazioni. Ad esempio, si supponga di decidere di aggiungere una query di account del cliente e aggiornare l'applicazione in esecuzione in LONDON e NEWYORK. Un record di account può essere conservato solo in un posto. È possibile decidere di controllare la distribuzione delle richieste utilizzando una tecnica di partizionamento dati. È possibile suddividere la distribuzione dei record. È possibile disporre la metà dei record, ad esempio per i numeri di conto 00000 - 49999, da tenere in LONDON. L'altra metà, nell'intervallo 50000 - 99999, è contenuta in NEWYORK. È quindi possibile scrivere un programma di uscita del carico di lavoro del cluster per esaminare il campo account in tutti i messaggi e instradare i messaggi al gestore code appropriato.

Operazioni successive

Ora che sono state completate tutte le definizioni, se non è stato ancora fatto, avviare l'iniziatore di canali su IBM WebSphere MQ for z/OS. Su tutte le piattaforme, avviare un programma listener sul Gestore code TORONTO. Il programma listener attende le richieste di rete in arrivo e avvia il canale ricevente del cluster quando è necessario.

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

Seguire le istruzioni nell'attività per creare cluster sovrapposti con un gestore code del gateway. Utilizzare i cluster come punto iniziale per i seguenti esempi di isolamento dei messaggi in un'applicazione da messaggi in altre applicazioni in un cluster.

Informazioni su questa attività

La configurazione cluster di esempio utilizzata per illustrare l'isolazione del traffico di messaggi cluster viene mostrata in Figura 37 a pagina 221. L'esempio è descritto in “Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 288.

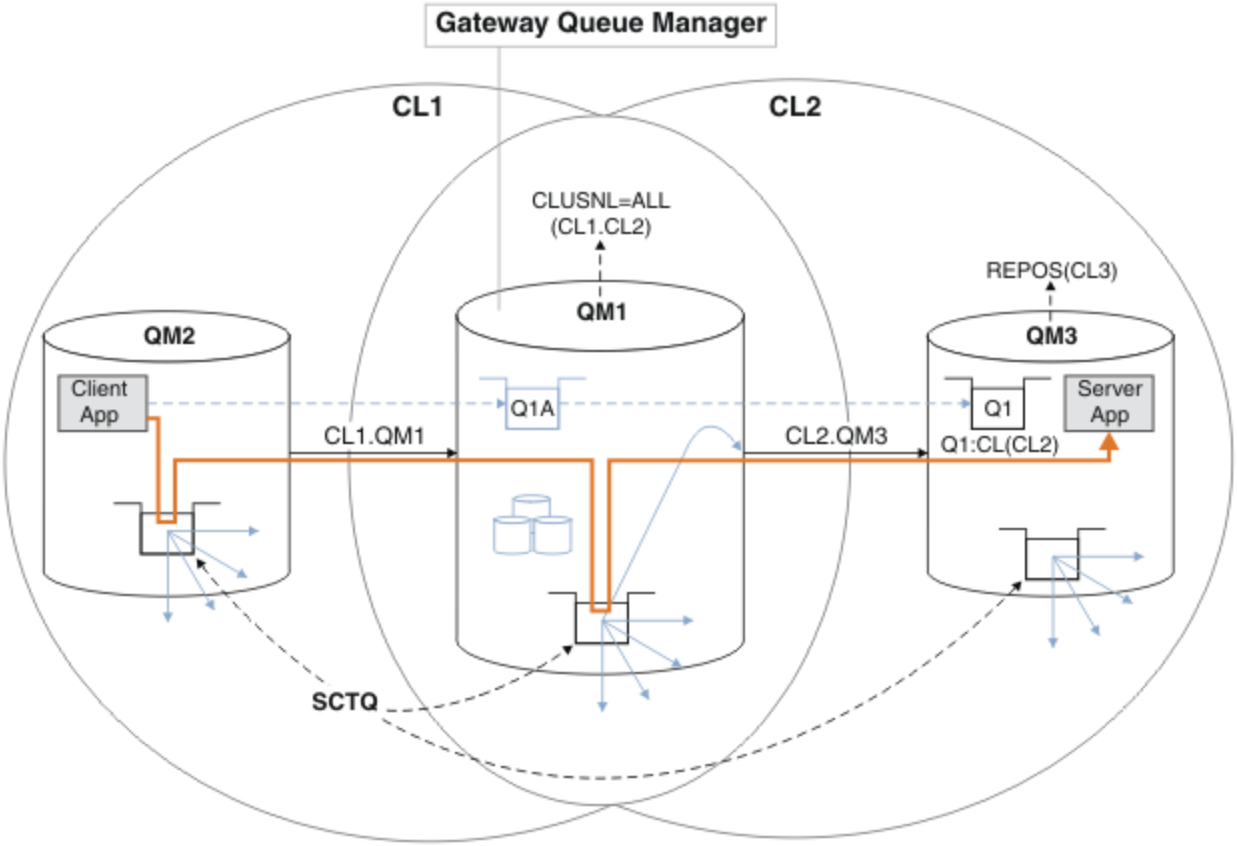


Figura 37. Applicazione client-server distribuita all'architettura hub e spoke utilizzando i cluster IBM WebSphere MQ

Per rendere il numero di passi per costruire l'esempio il meno possibile, la configurazione è semplice, piuttosto che realistica. L'esempio potrebbe rappresentare l'integrazione di due cluster creati da due organizzazioni separate. Per uno scenario più realistico, consultare “Clustering: pianificazione della configurazione delle code di trasmissione del cluster” a pagina 291.

Seguire la procedura per costruire i cluster. I cluster vengono utilizzati nei seguenti esempi di isolamento del traffico di messaggi dall'applicazione client all'applicazione server.

Le istruzioni aggiungono un paio di gestori code aggiuntivi in modo che ogni cluster abbia due repository. Il gestore code del gateway non viene utilizzato come repository per motivi di prestazioni.

Procedura

1. Creare e avviare i gestori code QM1, QM2, QM3, QM4, QM5.

```
crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE QMn
strmqm QmgrName
```

Nota: QM4 e QM5 sono i repository completi di backup per i cluster.

2. Definire e avviare i listener per ciascun gestore code.

```
*... On QMn
DEFINE LISTENER(TCP141n) TRPTYPE(TCP) IPADDR(hostname) PORT(141n) CONTROL(QMGR) REPLACE
START LISTENER(TCP141n)
```

3. Creare un elenco di nomi cluster per tutti i cluster.

```
*... On QM1
DEFINE NAMELIST(ALL) NAMES(CL1, CL2) REPLACE
```

4. Creare repository completi QM2 e QM4 per CL1, QM3 e QM5 per CL2.

   a) Per CL1:

```
*... On QM2 and QM4
ALTER QMGR REPOS(CL1) DEFCLXQ(SCTQ)
```

   b) Per CL2:

```
*... On QM3 and QM5
ALTER QMGR REPOS(CL2) DEFCLXQ(SCTQ)
```

5. Aggiungere i canali mittente del cluster e ricevente del cluster per ciascun gestore code e cluster.

   Eseguire i comandi riportati di seguito su QM2, QM3, QM4 e QM5, dove *c*, *n*e *m* assumono i valori mostrati in Tabella 26 a pagina 222 per ciascun gestore code:

Tabella 26. Valori di parametro per la creazione di cluster 1 e 2

Gestore code	**Cluster** ***c***	**Altro repository** ***n***	**Questo repository** ***m***
QM2	1	4	2
QM4	1	2	4
QM3	2	5	3
QM5	2	3	5

```
*... On QMm
DEFINE CHANNEL(CLc.QMn) CHLTYPE(CLUSSDR)  CONNAME('localhost(141n)') CLUSTER(CLc) REPLACE
DEFINE CHANNEL(CLc.QMm) CHLTYPE(CLUSRCVR) CONNAME('localhost(141m)') CLUSTER(CLc) REPLACE
```

6. Aggiungere il gestore code del gateway, QM1, a ciascuno dei cluster.

```
*... On QM1
DEFINE CHANNEL(CL1.QM2) CHLTYPE(CLUSSDR)  CONNAME('localhost(1412)') CLUSTER(CL1) REPLACE
DEFINE CHANNEL(CL1.QM1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1411)') CLUSTER(CL1) REPLACE
DEFINE CHANNEL(CL2.QM3) CHLTYPE(CLUSSDR)  CONNAME('localhost(1413)') CLUSTER(CL2) REPLACE
DEFINE CHANNEL(CL2.QM1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1411)') CLUSTER(CL2) REPLACE
```

7. Aggiungere la coda locale Q1 al gestore code QM3 nel cluster CL2.

```
*... On QM3
DEFINE QLOCAL(Q1) CLUSTER(CL2) REPLACE
```

8. Aggiungere l'alias del gestore code con cluster Q1A al gestore code del gateway.

```
*... On QM1
DEFINE QALIAS(Q1A)  CLUSNL(ALL) TARGET(Q1) TARGTYPE(QUEUE) DEFBIND(NOTFIXED) REPLACE
```

Nota: Le applicazioni che utilizzano l'alias del gestore code su qualsiasi altro gestore code, ma QM1, devono specificare DEFBIND(NOTFIXED) quando aprono la coda alias. **DEFBIND** specifica se le informazioni di instradamento nell'intestazione del messaggio sono fisse quando la coda viene aperta dall'applicazione. Se è impostato sul valore predefinito, OPEN, i messaggi vengono instradati

a Q1@QM1. Q1@QM1 non esiste, quindi i messaggi provenienti da altri gestori code finiscono su una coda di messaggi non recapitabili. Impostando l'attributo della coda su DEFBIND(NOTFIXED), le applicazioni come **amqsput**, che per impostazione predefinita utilizzano l'impostazione della coda di **DEFBIND**, si comportano correttamente.

9. Aggiungere le definizioni di alias del gestore code del cluster per tutti i gestori code del cluster al gestore code del gateway QM1.

```
*... On QM1
DEFINE QREMOTE(QM2) RNAME(' ') RQMNAME(QM2) CLUSNL(ALL) REPLACE
DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSNL(ALL) REPLACE
```

Suggerimento: Le definizioni di alias del gestore code sul gestore code del gateway trasferiscono i messaggi che fanno riferimento a un gestore code in un altro cluster; consultare Alias del gestore code cluster.

Operazioni successive

1. Verificare la definizione alias della coda inviando un messaggio da QM2 a Q1 su QM3 utilizzando la definizione alias della coda Q1A.

   a. Eseguire il programma di esempio **amqsput** su QM2 per inserire un messaggio.

   ```
   C:\IBM\MQ>amqsput Q1A QM2
   Sample AMQSPUT0 start
   target queue is Q1A
   Sample request message from QM2 to Q1 using Q1A

   Sample AMQSPUT0 end
   ```

   b. Eseguire il programma di esempio **amqsget** per richiamare il messaggio da Q1 on QM3

   ```
   C:\IBM\MQ>amqsget Q1 QM3
   Sample AMQSGET0 start
   message <Sample request message from QM2 to Q1 using Q1A>
   no more messages
   Sample AMQSGET0 end
   ```

2. Verificare le definizioni alias del gestore code inviando un messaggio di richiesta e ricevendo un messaggio di risposta su una coda di risposta dinamica temporanea.

   Il diagramma mostra il percorso utilizzato dal messaggio di risposta per tornare a una coda dinamica temporanea, denominata RQ. L'applicazione server, connessa a QM3, apre la coda di risposta utilizzando il nome del gestore code QM2. Il nome del gestore code QM2 è definito come alias del gestore code in cluster su QM1. QM3 instrada il messaggio di risposta a QM1. QM1 instrada il messaggio a QM2.

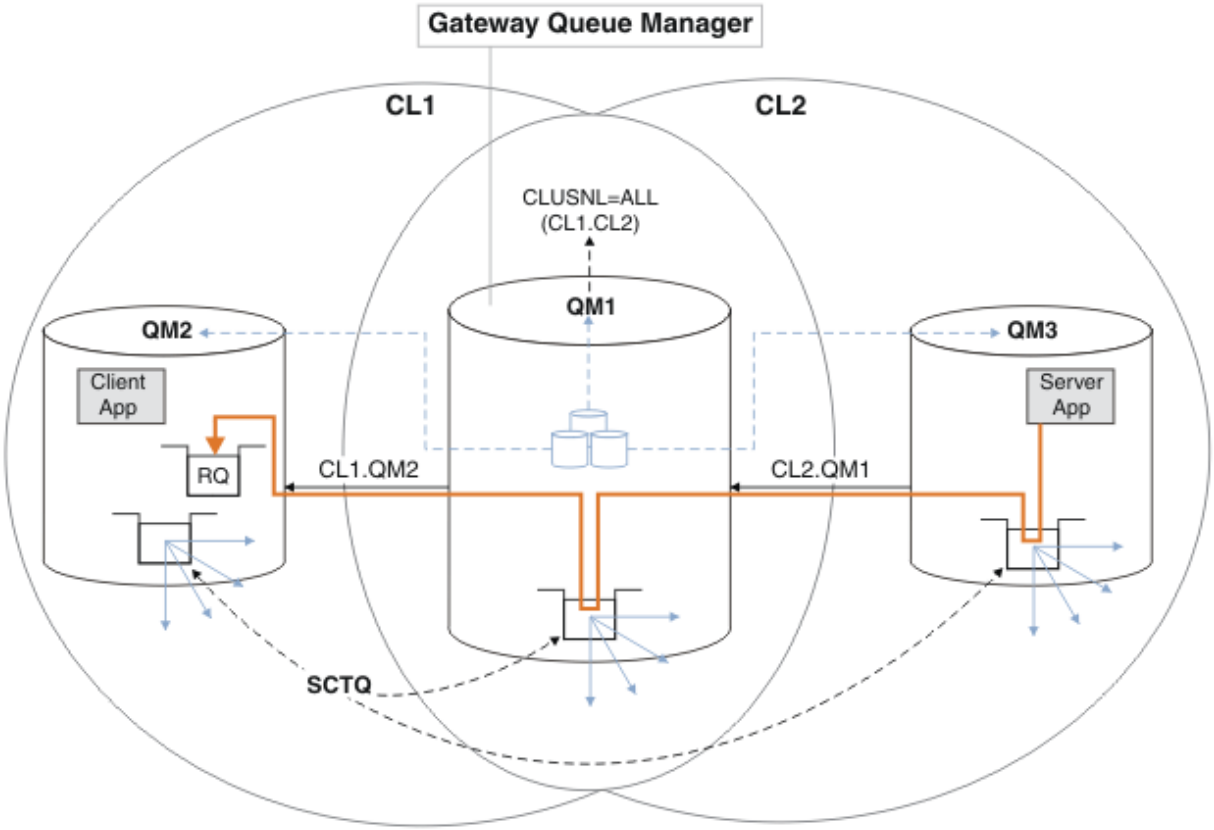


Figura 38. Utilizzo di un alias del gestore code per restituire il messaggio di risposta a un cluster differente

Il modo in cui funziona l'instradamento è il seguente. Ogni gestore code in ogni cluster ha una definizione di alias del gestore code su QM1. Gli alias sono raggruppati in tutti i cluster. Le frecce tratteggiate grigie da ciascuno degli alias a un gestore code mostrano che ogni alias del gestore code viene risolto in un gestore code reale in almeno uno di questi cluster. In questo caso, l'alias QM2 è raggruppato in cluster CL1 e CL2e viene risolto nel gestore code reale QM2 in CL1. L'applicazione server crea il messaggio di risposta utilizzando il nome della coda di risposta RQe il nome del gestore code di risposta QM2. Il messaggio viene instradato a QM1 perché la definizione alias del gestore code QM2 è definita su QM1 nel cluster CL2 e il gestore code QM2 non è nel cluster CL2. Poiché il messaggio non può essere inviato al gestore code di destinazione, viene inviato al gestore code che ha la definizione alias.

QM1 colloca il messaggio nella coda di trasmissione del cluster su QM1 per il trasferimento a QM2. QM1 instrada il messaggio a QM2 perché la definizione dell'alias del gestore code su QM1 per QM2 definisce QM2 come il gestore code di destinazione reale. La definizione non è circolare, poiché le definizioni alias possono fare riferimento solo a definizioni reali; l'alias non può puntare a se stesso. La definizione reale viene risolta da QM1, perché sia QM1 che QM2 si trovano nello stesso cluster, CL1. QM1 rileva le informazioni di collegamento per QM2 dal contenitore per CL1e instrada il messaggio a QM2. Perché il messaggio venga reinstradato da QM1, l'applicazione server deve aver aperto la coda di risposta con l'opzione DEFBIND impostata su MQBND_BIND_NOT_FIXED. Se l'applicazione server ha aperto la coda di risposta con l'opzione MQBND_BIND_ON_OPEN, il messaggio non viene reinstradato e finisce su una coda di messaggi non recapitabili.

a. Creare una coda di richieste in cluster con un trigger su QM3.

```
*... On QM3
DEFINE QLOCAL(QR) CLUSTER(CL2) TRIGGER INITQ(SYSTEM.DEFAULT.INITIATION.QUEUE)
PROCESS(ECHO) REPLACE
```

b. Creare una definizione alias della coda cluster di QR sul gestore code del gateway, QM1.

```
*... On QM1
DEFINE QALIAS(QRA) CLUSNL(ALL) TARGET(QR) TARGTYPE(QUEUE) DEFBIND(NOTFIXED) REPLACE
```

c. Creare una definizione di processo per avviare il programma echo di esempio **amqsech** su QM3.

```
*... On QM3
DEFINE PROCESS(ECHO) APPLICID(AMQSECH) REPLACE
```

d. Creare una coda modello su QM2 per il programma di esempio **amqsreq** per creare la coda di risposta dinamica temporanea.

```
*... On QM2
DEFINE QMODEL(SYSTEM.SAMPLE.REPLY) REPLACE
```

e. Verificare la definizione alias del gestore code inviando una richiesta da QM2 a QR on QM3 utilizzando la definizione alias della coda QRA.

i) Eseguire il programma di controllo trigger su QM3.

```
runmqtrm -m QM3
```

L'output è

```
C:\IBM\MQ>runmqtrm -m QM3
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
01/02/2012  16:17:15: WebSphere MQ trigger monitor started.


_____________________________________________
01/02/2012  16:17:15: Waiting for a trigger message
```

ii) Eseguire il programma di esempio **amqsreq** on QM2 per inserire una richiesta e attendere una risposta.

```
C:\IBM\MQ>amqsreq QRA QM2
Sample AMQSREQ0 start
server queue is QRA
replies to 4F2961C802290020
A request message from QM2 to QR on QM3

response <A request message from QM2 to QR on QM3>
no more replies
Sample AMQSREQ0 end
```

Concetti correlati

“Controllo accessi e code di trasmissione di più cluster” a pagina 163
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.QUEUEo la verifica rispetto ai profili locali per la coda del cluster o il gestore code del cluster.

“Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 288
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

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 201
Seguire queste istruzioni per aggiungere il gestore code al cluster creato. I messaggi per le code cluster e gli argomenti vengono trasferiti utilizzando più code di trasmissione cluster.

“Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221

Seguire le istruzioni nell'attività per creare cluster sovrapposti con un gestore code del gateway. Utilizzare i cluster come punto iniziale per i seguenti esempi di isolamento dei messaggi in un'applicazione da messaggi in altre applicazioni in un cluster.

“Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway” a pagina 203
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una definizione remota della coda cluster e un canale mittente e una coda di trasmissione separati.

“Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi” a pagina 226
È possibile modificare il modo predefinito in cui un gestore code memorizza i messaggi per una coda cluster o un argomento su una coda di trasmissione. La modifica del valore predefinito fornisce un modo per isolare i messaggi cluster su 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” a pagina 206
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una coda di trasmissione cluster aggiuntiva per separare il traffico di messaggi a un singolo gestore code in un cluster.

“Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 209
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza un cluster aggiuntivo per isolare i messaggi in una particolare coda cluster.

“Clustering: pianificazione della configurazione delle code di trasmissione del cluster” a pagina 291
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. La configurazione di più code di trasmissione cluster si applica a piattaforme diverse da z/OS.

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

È possibile modificare il modo predefinito in cui un gestore code memorizza i messaggi per una coda cluster o un argomento su una coda di trasmissione. La modifica del valore predefinito fornisce un modo per isolare i messaggi cluster su un gestore code del gateway.

Prima di iniziare

1. Il gestore code del gateway deve essere su Version 7.5o versione successiva e su una piattaforma diversa da z/OS.
2. Creare i cluster sovrapposti mostrati in Figura 37 a pagina 221 in “Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221 seguendo i passi in tale attività.

Informazioni su questa attività

Per implementare l'architettura con più code di cluster, il tuo gestore code del gateway deve essere su Version 7.5o successivo. Per utilizzare più code di trasmissione del cluster, è necessario modificare il tipo di coda di trasmissione del cluster predefinito sul gestore code del gateway. Modificare il valore dell'attributo del gestore code **DEFCLXQ** su `QM1` da `SCTQ` a `CHANNEL`; consultare Figura 39 a pagina 227. Il diagramma mostra un flusso di messaggi. Per i flussi verso altri gestori code o verso altri cluster, il gestore code crea ulteriori code di trasmissione del cluster dinamico permanenti. Ogni canale mittente del cluster trasferisce i messaggi da una coda di trasmissione cluster differente.

La modifica non ha effetto immediato, a meno che non si stia connettendo il gestore code del gateway ai cluster per la prima volta. L'attività include i passi per il caso tipico di gestione di una modifica a una configurazione esistente. Per impostare un gestore code in modo che utilizzi code di trasmissione cluster separate quando si unisce per la prima volta a un cluster; consultare “Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 201.

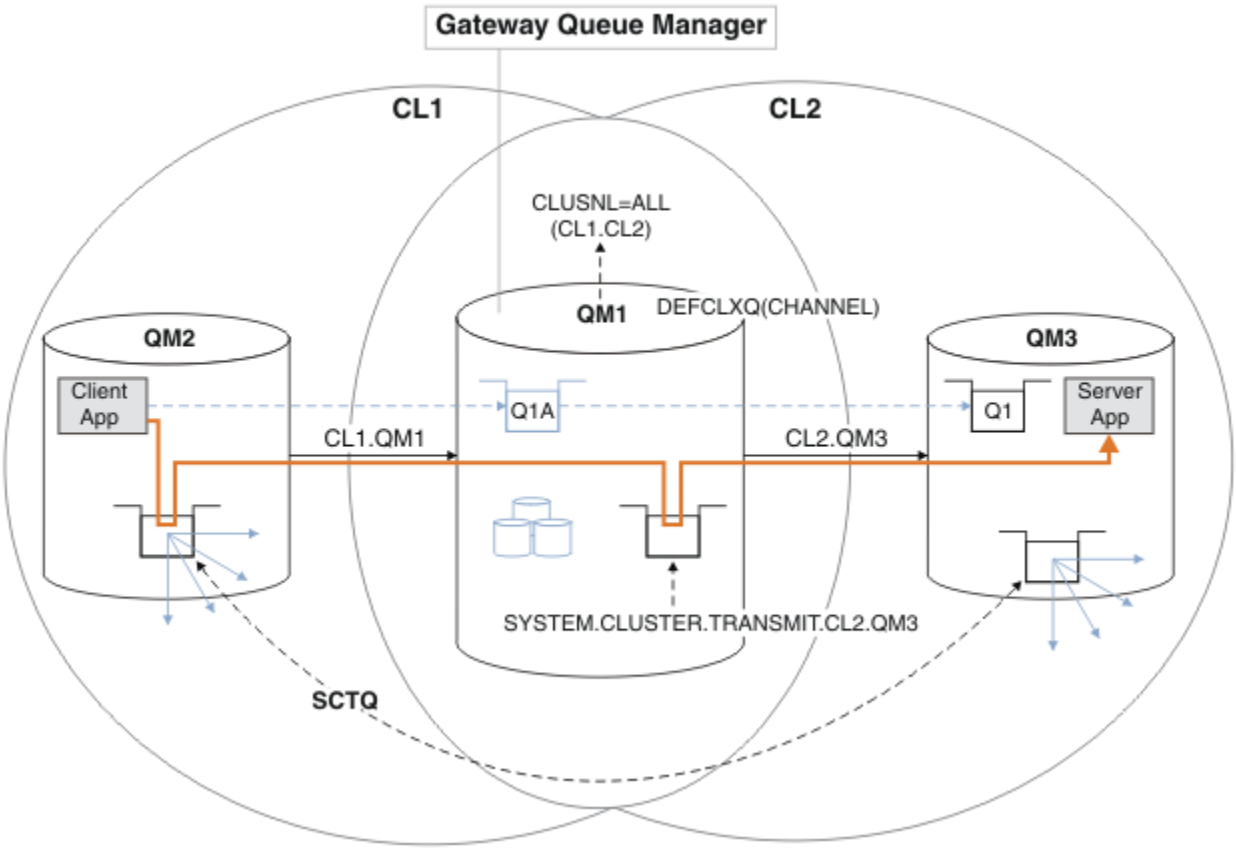


Figura 39. Applicazione client-server distribuita all'architettura hub e spoke con code di trasmissione cluster separate sul gestore code del gateway.

Procedura

1. Modificare il gestore code del gateway in modo da utilizzare code di trasmissione cluster separate.

   ```
   *... On QM1
   ALTER QMGR DEFCLXQ(CHANNEL)
   ```

2. Passare alle code di trasmissione cluster separate.

   Qualsiasi canale mittente del cluster che non è in esecuzione passa all'utilizzo di code di trasmissione del cluster separate al successivo avvio.

   Per commutare i canali in esecuzione, riavviare il gestore code oppure attenersi alla seguente procedura:

   a) Elencare i canali mittente del cluster in esecuzione con `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

   ```
   *... On QM1
   DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
   ```

   La risposta è un elenco di report di stato del canale:

   ```
   AMQ8417: Display Channel Status details.
      CHANNEL(CL1.QM2)            CHLTYPE(CLUSSDR)
      CONNAME(127.0.0.1(1412))    CURRENT
   ```

```
   RQMNAME(QM2)                STATUS(RUNNING)
   SUBSTATE(MQGET)             XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM3)            CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1413))    CURRENT
   RQMNAME(QM3)                STATUS(RUNNING)
   SUBSTATE(MQGET)             XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM5)            CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1415))    CURRENT
   RQMNAME(QM5)                STATUS(RUNNING)
   SUBSTATE(MQGET)             XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
   CHANNEL(CL1.QM4)            CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1414))    CURRENT
   RQMNAME(QM4)                STATUS(RUNNING)
   SUBSTATE(MQGET)             XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

b) Arresta i canali in esecuzione

Per ogni canale nell'elenco, eseguire il comando:

```
*... On QM1
STOP CHANNEL(ChannelName)
```

Dove *ChannelName* è ognuno di `CL1.QM2, CL1.QM4, CL1.QM3, CL1.QM5`.

La risposta è che il comando è accettato:

```
AMQ8019: Stop WebSphere MQ channel accepted.
```

c) Monitorare quali canali sono arrestati

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
```

La risposta è un elenco di canali ancora in esecuzione e di canali arrestati:

```
AMQ8417: Display Channel Status details.
   CHANNEL(CL1.QM2)            CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1412))    CURRENT
   RQMNAME(QM2)                STATUS(STOPPED)
   SUBSTATE( )                 XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM3)            CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1413))    CURRENT
   RQMNAME(QM3)                STATUS(STOPPED)
   SUBSTATE( )                 XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM5)            CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1415))    CURRENT
   RQMNAME(QM5)                STATUS(STOPPED)
   SUBSTATE( )                 XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
   CHANNEL(CL1.QM4)            CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1414))    CURRENT
   RQMNAME(QM4)                STATUS(STOPPED)
   SUBSTATE( )                 XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

d) Avviare ogni canale arrestato.

Eseguire questa operazione per tutti i canali in esecuzione. Se un canale non si arresta, è possibile eseguire nuovamente il comando **STOP CHANNEL** con l'opzione FORCE . Un esempio

di impostazione dell'opzione FORCE è se il canale non si arresta e non è possibile riavviare l'altro gestore code per sincronizzare il canale.

```
*... On QM1
START CHANNEL(CL2.QM5)
```

La risposta è che il comando è accettato:

```
AMQ8018: Start WebSphere MQ channel accepted.
```

e) Monitorare le code di trasmissione che vengono commutate.

Monitorare il file di registrazione errori del gestore code del gateway per il messaggio "AMQ7341 La coda di trasmissione per il canale CL2.QM3 è SYSTEM.CLUSTER.TRANSMIT.*QUEUE | CL2.QM3*".

f) Verificare che SYSTEM.CLUSTER.TRANSMIT.QUEUE non sia più utilizzato

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
DISPLAY QUEUE(SYSTEM.CLUSTER.TRANSMIT.QUEUE) CURDEPTH
```

La risposta è un elenco di report di stato del canale e la profondità di SYSTEM.CLUSTER.TRANSMIT.QUEUE:

```
AMQ8420: Channel Status not found.
AMQ8409: Display Queue details.
   QUEUE(SYSTEM.CLUSTER.TRANSMIT.QUEUE)    TYPE(QLOCAL)
   CURDEPTH(0)
```

g) Monitorare quali canali sono avviati

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
```

La risposta è un elenco dei canali, in questo caso già in esecuzione con le nuove code di trasmissione del cluster predefinite:

```
AMQ8417: Display Channel Status details.
   CHANNEL(CL1.QM2)                        CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1412))                CURRENT
   RQMNAME(QM2)                            STATUS(RUNNING)
   SUBSTATE(MQGET)
   XMITQ(SYSTEM.CLUSTER.TRANSMIT.CL1.QM2)
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM3)                        CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1413))                CURRENT
   RQMNAME(QM3)                            STATUS(RUNNING)
   SUBSTATE(MQGET)
   XMITQ(SYSTEM.CLUSTER.TRANSMIT.CL2.QM3)
AMQ8417: Display Channel Status details.
   CHANNEL(CL2.QM5)                        CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1415))                CURRENT
   RQMNAME(QM5)                            STATUS(RUNNING)
   SUBSTATE(MQGET)
   XMITQ(SYSTEM.CLUSTER.TRANSMIT.CL2.QM5)
AMQ8417: Display Channel Status details.
   CHANNEL(CL1.QM4)                        CHLTYPE(CLUSSDR)
   CONNAME(127.0.0.1(1414))                CURRENT
   RQMNAME(QM4)                            STATUS(RUNNING)
   SUBSTATE(MQGET)
   XMITQ(SYSTEM.CLUSTER.TRANSMIT.CL1.QM4)
```

Operazioni successive

1. Verificare la coda di trasmissione del cluster definita automaticamente inviando un messaggio da QM2 a Q1 on QM3, risolvendo il nome della coda con definizione dell'alias della coda Q1A

   a. Eseguire il programma di esempio **amqsput** su QM2 per inserire un messaggio.

   ```
   C:\IBM\MQ>amqsput Q1A QM2
   Sample AMQSPUT0 start
   target queue is Q1A
   Sample request message from QM2 to Q1 using Q1A

   Sample AMQSPUT0 end
   ```

   b. Eseguire il programma di esempio **amqsget** per richiamare il messaggio da Q1 on QM3

   ```
   C:\IBM\MQ>amqsget Q1 QM3
   Sample AMQSGET0 start
   message <Sample request message from QM2 to Q1 using Q1A>
   no more messages
   Sample AMQSGET0 end
   ```

2. Considerare se riconfigurare la sicurezza, configurando la sicurezza per le code del cluster sui gestori code in cui hanno origine i messaggi per le code del cluster.

Concetti correlati

“Controllo accessi e code di trasmissione di più cluster” a pagina 163
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.QUEUEo la verifica rispetto ai profili locali per la coda del cluster o il gestore code del cluster.

“Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 288
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

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 201
Seguire queste istruzioni per aggiungere il gestore code al cluster creato. I messaggi per le code cluster e gli argomenti vengono trasferiti utilizzando più code di trasmissione cluster.

“Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221
Seguire le istruzioni nell'attività per creare cluster sovrapposti con un gestore code del gateway. Utilizzare i cluster come punto iniziale per i seguenti esempi di isolamento dei messaggi in un'applicazione da messaggi in altre applicazioni in un cluster.

“Aggiunta di una definizione di coda remota per isolare i messaggi inviati da un gestore code del gateway” a pagina 203
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una definizione remota della coda cluster e un canale mittente e una coda di trasmissione separati.

“Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi” a pagina 226
È possibile modificare il modo predefinito in cui un gestore code memorizza i messaggi per una coda cluster o un argomento su una coda di trasmissione. La modifica del valore predefinito fornisce un modo per isolare i messaggi cluster su 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” a pagina 206

Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una coda di trasmissione cluster aggiuntiva per separare il traffico di messaggi a un singolo gestore code in un cluster.

"Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway" a pagina 209
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza un cluster aggiuntivo per isolare i messaggi in una particolare coda cluster.

"Clustering: pianificazione della configurazione delle code di trasmissione del cluster" a pagina 291
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. La configurazione di più code di trasmissione cluster si applica a piattaforme diverse da z/OS.

Rimozione di una coda cluster da un gestore code

Disabilitare la coda INVENTQ a Toronto. Inviare tutti i messaggi di inventario a New York ed eliminare la coda INVENTQ a Toronto quando è vuota.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in "Aggiunta di un gestore code su cui è presente una coda" a pagina 218. Contiene quattro gestori code. LONDON e NEWYORK contengono entrambi repository completi. PARIS e TORONTO contengono repository parziali. L'applicazione di inventario viene eseguita sui sistemi di New York e Toronto ed è guidata dall'arrivo dei messaggi sulla coda INVENTQ .
- A causa della riduzione del carico di lavoro, non si desidera più eseguire l'applicazione di inventario a Toronto. Si desidera disabilitare la coda INVENTQ ospitata dal gestore code TORONTOe disporre di messaggi feed TORONTO nella coda INVENTQ in NEWYORK.
- La connettività di rete esiste tra tutti e quattro i sistemi.
- Il protocollo di rete è TCP.

Informazioni su questa attività

Effettuare le operazioni riportate di seguito per rimuovere una coda cluster.

Procedura

1. Indica che la coda non è più disponibile.

   Per rimuovere una coda da un cluster, rimuovere il nome cluster dalla definizione della coda locale. Modificare il INVENTQ su TORONTO in modo che non sia accessibile dal resto del cluster:

   ```
   ALTER QLOCAL(INVENTQ) CLUSTER(' ')
   ```

2. Verificare che la coda non sia più disponibile.

   Su un gestore code del repository completo, LONDON o NEWYORK, verificare che la coda non sia più ospitata dal gestore code TORONTO emettendo il seguente comando:

   ```
   DIS QCLUSTER (INVENTQ)
   ```

TORONTO non è elencato nei risultati, se il comando ALTER è stato completato correttamente.

3. Disabilitare la coda.

   Disabilitare la coda INVENTQ in TORONTO in modo che non sia possibile scrivere ulteriori messaggi:

   ```
   ALTER QLOCAL(INVENTQ) PUT(DISABLED)
   ```

   Ora i messaggi in transito verso questa coda utilizzando MQOO_BIND_ON_OPEN vanno alla coda di messaggi non instradabili. È necessario impedire a tutte le applicazioni di inserire esplicitamente i messaggi nella coda su questo gestore code.

4. Monitorare la coda finché non è vuota.

   Monitorare la coda utilizzando il comando DISPLAY QUEUE , specificando gli attributi IPPROCS, OPPROCSe CURDEPTHoppure utilizzare il comando **WRKMQMSTS** su IBM i. Quando il numero di processi di input e di output e la profondità corrente delle code sono tutti zero, la coda è vuota.

5. Monitorare il canale per assicurarsi che non vi siano messaggi in dubbio.

   Per essere certi che non vi siano messaggi in dubbio sul canale INVENTORY.TORONTO, monitorare il canale mittente del cluster denominato INVENTORY.TORONTO su ciascuno degli altri gestori code. Immettere il comando DISPLAY CHSTATUS specificando il parametro INDOUBT da ogni gestore code:

   ```
   DISPLAY CHSTATUS(INVENTORY.TORONTO) INDOUBT
   ```

   Se sono presenti messaggi in dubbio, è necessario risolverli prima di procedere. Ad esempio, è possibile provare ad emettere il comando di canale RESOLVE o ad arrestare e riavviare il canale.

6. Eliminare la coda locale.

   Quando si è soddisfatti che non ci sono più messaggi da consegnare all'applicazione di inventario in TORONTO, è possibile eliminare la coda:

   ```
   DELETE QLOCAL(INVENTQ)
   ```

7. Ora è possibile rimuovere l'applicazione di inventario dal sistema a Toronto

   La rimozione dell'applicazione evita la duplicazione e consente di risparmiare spazio sul sistema.

Risultati

Il cluster impostato da questa attività è simile a quello impostato dall'attività precedente. La differenza è che la coda INVENTQ non è più disponibile sul gestore code TORONTO.

Quando la coda è stata tolta dal servizio nel passo 1, il gestore code TORONTO ha inviato un messaggio ai due gestori code del repository completo. Ha notificato loro la modifica dello stato. I gestori code del repository completo trasmettono queste informazioni ad altri gestori code del cluster che hanno richiesto aggiornamenti alle informazioni relative a INVENTQ.

Quando un gestore code inserisce un messaggio nella code INVENTQ , il repository parziale aggiornato indica che la coda INVENTQ è disponibile solo sul gestore code NEWYORK . Il messaggio viene inviato al gestore code NEWYORK .

Operazioni successive

In questa attività, c'era solo una coda da rimuovere e solo un cluster da cui rimuoverla.

Si supponga che vi siano molte code che fanno riferimento a un elenco nomi contenente molti nomi cluster. Ad esempio, il gestore code TORONTO potrebbe contenere non solo INVENTQ , ma anche PAYROLLQ, SALESQ e PURCHASESQ. TORONTO rende queste code disponibili in tutti i cluster appropriati,

INVENTORY , PAYROLL, SALESe PURCHASES . Definire un elenco nomi dei nomi cluster sul gestore code TORONTO :

```
DEFINE NAMELIST(TOROLIST)
       DESCR('List of clusters TORONTO is in')
       NAMES(INVENTORY, PAYROLL, SALES, PURCHASES)
```

Aggiungere l'elenco nomi a ciascuna definizione di coda:

```
DEFINE QLOCAL(INVENTQ) CLUSNL(TOROLIST)
DEFINE QLOCAL(PAYROLLQ) CLUSNL(TOROLIST)
DEFINE QLOCAL(SALESQ) CLUSNL(TOROLIST)
DEFINE QLOCAL(PURCHASESQ) CLUSNL(TOROLIST)
```

Ora si supponga di voler rimuovere tutte le code dal cluster SALES , perché l'operazione SALES deve essere presa in consegna dall'operazione PURCHASES . Tutto ciò che devi fare è modificare l'elenco nomi TOROLIST per rimuovere il nome del cluster SALES da esso.

Se si desidera rimuovere una singola coda da uno dei cluster nell'elenco nomi, creare un elenco nomi contenente il rimanente elenco di nomi cluster. Quindi, modificare la definizione della coda per utilizzare il nuovo elenco nomi. Per rimuovere PAYROLLQ dal cluster INVENTORY :

1. Creare un elenco nomi:

   ```
   DEFINE NAMELIST(TOROSHORTLIST)
          DESCR('List of clusters TORONTO is in other than INVENTORY')
          NAMES(PAYROLL, SALES, PURCHASES)
   ```

2. Modificare la definizione della coda PAYROLLQ :

   ```
   ALTER QLOCAL(PAYROLLQ) CLUSNL(TOROSHORTLIST)
   ```

Spostamento di un repository completo in un altro gestore code

Spostare un repository completo da un gestore code a un altro, creando il nuovo repository dalle informazioni contenute nel secondo repository.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in “Aggiunta di un gestore code a un cluster” a pagina 199.
- Per motivi aziendali, si desidera ora rimuovere il repository completo dal gestore code LONDONe sostituirlo con un repository completo sul gestore code PARIS. Il gestore code NEWYORK deve continuare a mantenere un repository completo.

Informazioni su questa attività

Attenersi alla seguente procedura per spostare un repository completo in un altro gestore code.

Procedura

1. Modificare PARIS per renderlo un gestore code del repository completo.

   Su PARIS, immettere il seguente comando:

   ```
   ALTER QMGR REPOS(INVENTORY)
   ```

2. Aggiungere un canale CLUSSDR su PARIS

   PARIS attualmente ha un canale mittente del cluster che punta a LONDON. LONDON non deve più contenere un repository completo per il cluster. PARIS deve avere un nuovo canale mittente del cluster che punti a NEWYORK, dove ora è conservato l'altro repository completo.

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from PARIS to repository at NEWYORK')
   ```

3. Definire un canale CLUSSDR su NEWYORK che punti a PARIS

   Attualmente NEWYORK ha un canale mittente del cluster che punta a LONDON. Ora che l'altro repository completo è stato spostato in PARIS, devi aggiungere un nuovo canale mittente del cluster in NEWYORK che punti a PARIS.

   ```
   DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(PARIS.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from NEWYORK to repository at PARIS')
   ```

   Quando aggiungi il canale mittente del cluster a PARIS, PARIS impara a conoscere il cluster da NEWYORK. Crea il proprio repository completo utilizzando le informazioni da NEWYORK.

4. Verificare che il gestore code PARIS disponga ora di un repository completo

   Verificare che il gestore code PARIS abbia creato il proprio repository completo dal repository completo sul gestore code NEWYORK. Immettere i seguenti comandi:

   ```
   DIS QCLUSTER(*) CLUSTER (INVENTORY)
   DIS CLUSQMGR(*) CLUSTER (INVENTORY)
   ```

   Verificare che questi comandi mostrino i dettagli delle stesse risorse in questo cluster come su NEWYORK.

   Nota: Se il gestore code NEWYORK non è disponibile, non è possibile completare questa creazione di informazioni. Non passare al passo successivo fino a quando l'attività non è completa.

5. Modificare la definizione del gestore code su LONDON

   Infine, modificare il gestore code in LONDON in modo che non contenga più un repository completo per il cluster. Su LONDON, immettere il comando:

   ```
   ALTER QMGR REPOS(' ')
   ```

   Il gestore code non riceve più le informazioni sul cluster. Dopo 30 giorni le informazioni memorizzate nel relativo repository completo scadono. Il gestore code LONDON ora crea il proprio repository parziale.

6. Eliminare o modificare le definizioni in sospeso.

   Quando si è certi che la nuova disposizione del cluster funziona come previsto, rimuovere o modificare manualmente le definizioni CLUSSDR definite che non sono più corrette.

   - Sul gestore code PARIS , è necessario arrestare ed eliminare il canale mittente del cluster su LONDON, quindi immettere il comando di avvio del canale in modo che il cluster possa utilizzare nuovamente i canali automatici:

     ```
     STOP CHANNEL(INVENTORY.LONDON)
     DELETE CHANNEL(INVENTORY.LONDON)
     START CHANNEL(INVENTORY.LONDON)
     ```

- Sul gestore code NEWYORK , è necessario arrestare ed eliminare il canale mittente del cluster su LONDON, quindi immettere il comando di avvio del canale in modo che il cluster possa utilizzare nuovamente i canali automatici:

```
STOP CHANNEL(INVENTORY.LONDON)
DELETE CHANNEL(INVENTORY.LONDON)
START CHANNEL(INVENTORY.LONDON)
```

- Sostituire tutti gli altri canali mittenti del cluster nel cluster che puntano a LONDON con canali che puntano a NEWYORK o PARIS. In questo piccolo esempio, non ce ne sono altri. Per verificare la presenza di altri elementi dimenticati, immettere il comando DISPLAY CHANNEL da ogni gestore code, specificando TYPE(CLUSSDR). Ad esempio:

```
DISPLAY CHANNEL(*) TYPE(CLUSSDR)
```

È importante eseguire questa attività il più presto possibile dopo aver spostato il repository completo da LONDON a PARIS. Prima di eseguire questa attività, i gestori code che hanno definito manualmente i canali CLUSSDR denominati INVENTORY.LONDON potrebbero inviare richieste di informazioni utilizzando questo canale.

Dopo che LONDON ha cessato di essere un repository completo, se riceve tali richieste scriverà messaggi di errore nel log degli errori del gestore code. I seguenti esempi mostrano quali messaggi di errore potrebbero essere visualizzati su LONDON:

- AMQ9428: Unexpected publication of a cluster queue object received
- AMQ9432: Query received by a non-repository queue manager

Il gestore code LONDON non risponde alle richieste di informazioni perché non è più un repository completo. I gestori code che richiedono le informazioni da LONDON devono basarsi su NEWYORK per le informazioni sul cluster fino a quando le loro definizioni CLUSSDR definite manualmente non vengono corrette per puntare a PARIS. Questa situazione non deve essere tollerata come una configurazione valida a lungo termine.

Risultati

Figura 40 a pagina 236 mostra il cluster impostato da questa attività.

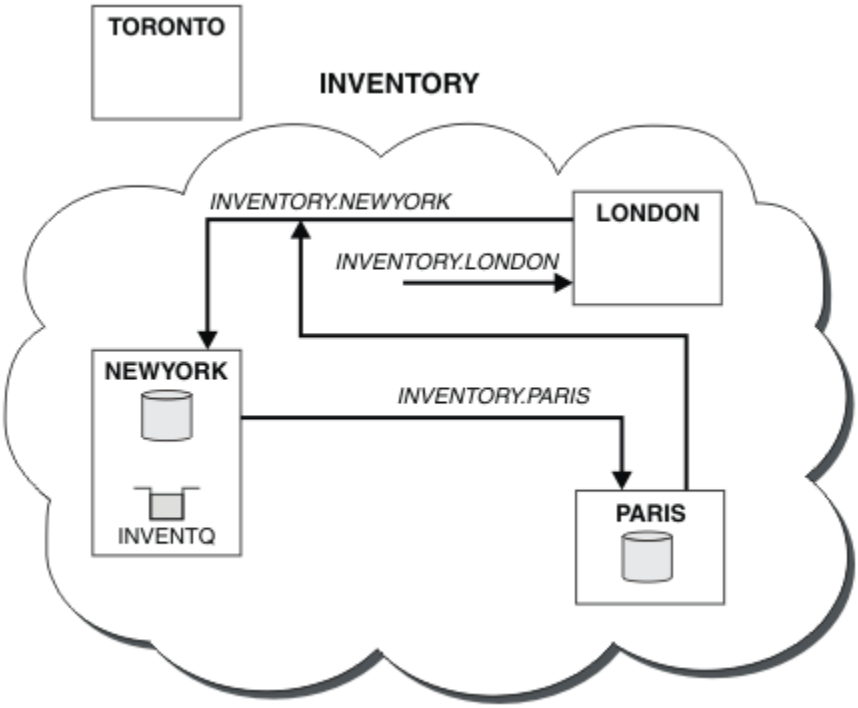


Figura 40. Il cluster INVENTORY con il repository completo è stato spostato in PARIS

Conversione di una rete esistente in un cluster

Convertire una rete di accodamento distribuita esistente in un cluster e aggiungere un ulteriore gestore code per incrementare la capacità.

Prima di iniziare

In “Configurazione di un nuovo cluster” a pagina 188 tramite “Spostamento di un repository completo in un altro gestore code” a pagina 233 hai creato ed esteso un nuovo cluster. Le due attività successive esplorano un approccio diverso: quello di convertire una rete esistente di gestori code in un cluster.

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Una rete IBM WebSphere MQ è già attiva, collegando le filiali nazionali di una catena di negozi. Ha una struttura hub e spoke: tutti i gestori code sono connessi a un unico gestore code centrale. Il gestore code centrale si trova sul sistema su cui viene eseguita l'applicazione di inventario. L'applicazione è guidata dall'arrivo dei messaggi sulla coda INVENTQ , per cui ciascun gestore code ha una definizione di coda remota.

  Questa rete è illustrata in Figura 41 a pagina 237.

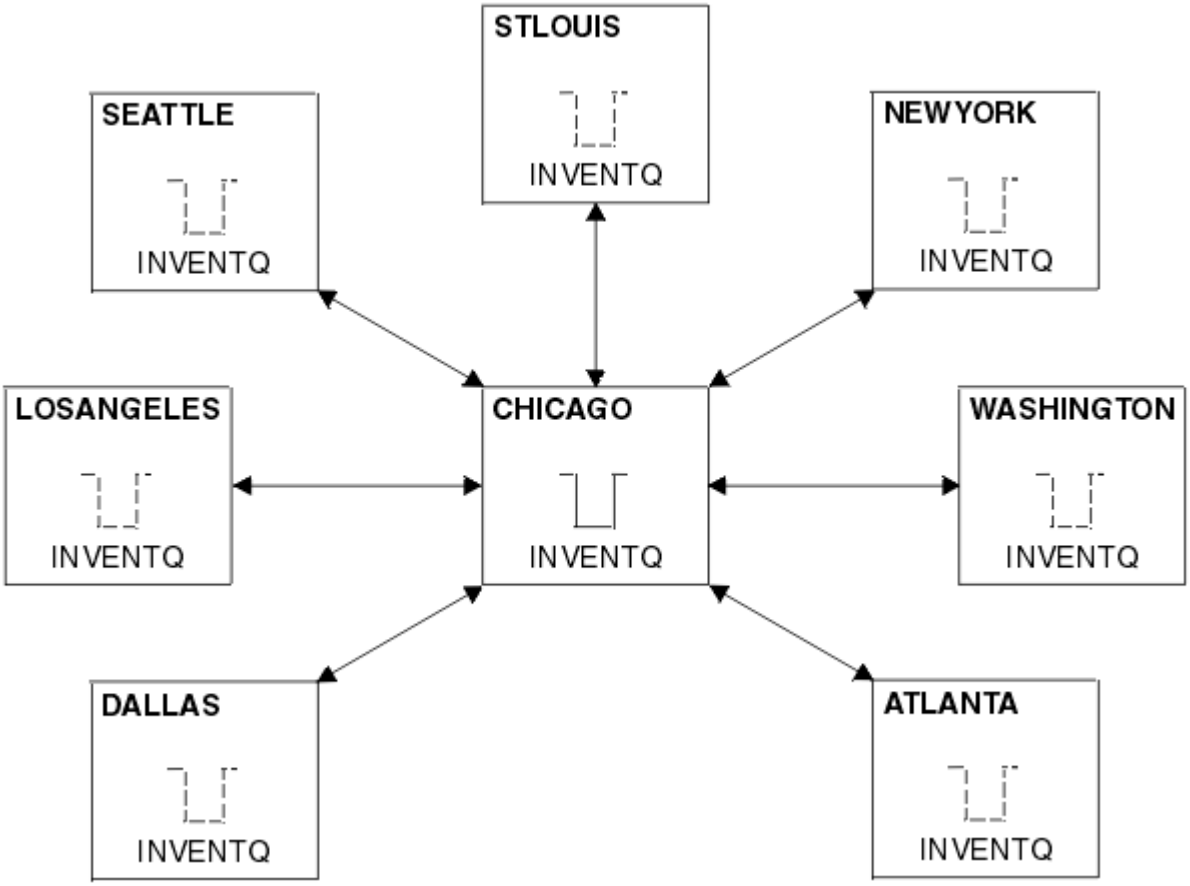


Figura 41. Una rete hub e spoke

- Per facilitare la gestione, si sta per convertire questa rete in un cluster e creare un altro gestore code sul sito centrale per condividere il carico di lavoro.

  Il nome cluster è `CHNSTORE`.

  Nota: Il nome cluster `CHNSTORE` è stato selezionato per consentire la creazione dei nomi dei canali riceventi del cluster utilizzando i nomi nel formato *`cluster-name.queue-manager`* che non superano la lunghezza massima di 20 caratteri, ad esempio `CHNSTORE.WASHINGTON`.
- Entrambi i gestori code centrali devono ospitare repository completi e devono essere accessibili all'applicazione di inventario.
- L'applicazione di inventario deve essere guidata dall'arrivo di messaggi sulla coda `INVENTQ` ospitata da uno dei gestori code centrali.
- L'applicazione di inventario deve essere l'unica applicazione in esecuzione in parallelo e accessibile da più di un gestore code. Tutte le altre applicazioni continuano ad essere eseguite come prima.
- Tutte le filiali hanno la connettività di rete ai due gestori code centrali.
- Il protocollo di rete è TCP.

Informazioni su questa attività

Seguire questa procedura per convertire una rete esistente in un cluster.

Procedura

1. Esaminare l'applicazione inventario per le affinità dei messaggi.

   Prima di procedere, verificare che l'applicazione possa gestire le affinità dei messaggi. Le affinità di messaggi sono le relazioni tra i messaggi di conversazione scambiati tra due applicazioni, dove i messaggi devono essere elaborati da un particolare gestore code o in una particolare sequenza. Per

ulteriori informazioni sulle affinità dei messaggi, consultare: “Gestione delle affinità dei messaggi” a pagina 280

2. Modificare i due gestori code centrali per renderli gestori code con repository completo.

   I due gestori code CHICAGO e CHICAGO2 si trovano nell'hub di questa rete. Si è deciso di concentrare tutte le attività associate al cluster di negozi della catena su questi due gestori code. Oltre all'applicazione di inventario e le definizioni per la coda INVENTQ , si desidera che questi gestori code ospitino i due repository completi per il cluster. Su ciascuno dei due gestori code, immettere il seguente comando:

   ```
   ALTER QMGR REPOS(CHNSTORE)
   ```

3. Definire un canale CLUSRCVR su ciascun gestore code.

   In ogni gestore code del cluster, definire un canale ricevente del cluster e un canale mittente del cluster. Non importa quale canale si definisce per primo.

   Creare una definizione CLUSRCVR per pubblicizzare ogni gestore code, il relativo indirizzo di rete e altre informazioni sul cluster. Ad esempio, sul gestore code ATLANTA:

   ```
   DEFINE CHANNEL(CHNSTORE.ATLANTA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(ATLANTA.CHSTORE.COM) CLUSTER(CHNSTORE)
   DESCR('Cluster-receiver channel')
   ```

4. Definire un canale CLUSSDR su ciascun gestore code

   Creare una definizione CLUSSDR su ogni gestore code per collegare tale gestore code a uno o più gestori code del repository completo. Ad esempio, è possibile collegare ATLANTA a CHICAGO2:

   ```
   DEFINE CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(CHICAGO2.CHSTORE.COM) CLUSTER(CHNSTORE)
   DESCR('Cluster-sender channel to repository queue manager')
   ```

5. Installare l'applicazione di inventario su CHICAGO2.

   Si dispone già dell'applicazione di inventario sul gestore code CHICAGO. Ora è necessario eseguire una copia di questa applicazione sul gestore code CHICAGO2.

6. Definire la coda INVENTQ sui gestori code centrali.

   Su CHICAGO, modificare la definizione della coda locale per la coda INVENTQ per renderla disponibile per il cluster. Immettere il seguente comando:

   ```
   ALTER QLOCAL(INVENTQ) CLUSTER(CHNSTORE)
   ```

   In CHICAGO2, creare una definizione per la stessa coda:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(CHNSTORE)
   ```

   Su z/OS, è possibile utilizzare l'opzione MAKEDEF della funzione COMMAND di **CSQUTIL** per eseguire una copia esatta su CHICAGO2 di INVENTQ su CHICAGO.

   Quando si effettuano queste definizioni, viene inviato un messaggio ai repository completi in CHICAGO e CHICAGO2 e le informazioni in essi contenute vengono aggiornate. Il gestore code rileva dai repository completi quando inserisce un messaggio in INVENTQ, che esiste una scelta di destinazioni per i messaggi.

7. Verificare che le modifiche al cluster siano state propagate.

   Verificare che le definizioni create nel passo precedente siano state propagate attraverso il cluster. Immettere il seguente comando su un gestore code del repository completo:

   ```
   DIS QCLUSTER(INVENTQ)
   ```

Aggiunta di un nuovo cluster interconnesso

Aggiungere un nuovo cluster che condivide alcuni gestori code con un cluster esistente.

Prima di iniziare

Nota:

1. Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.
2. Prima di avviare questa attività, verificare la presenza di conflitti di nomi coda e comprendere le conseguenze. Potrebbe essere necessario ridenominare una coda o impostare gli alias della coda prima di continuare.

Scenario:

- Un cluster WebSphere MQ è stato configurato come descritto in “Conversione di una rete esistente in un cluster” a pagina 236 .
- Deve essere implementato un nuovo cluster denominato MAILORDER . Questo cluster comprende quattro dei gestori code presenti nel cluster CHNSTORE ; CHICAGO, CHICAGO2 , SEATTLEe ATLANTAe due ulteriori gestori code; HARTFORD e OMAHA . L'applicazione MAILORDER viene eseguita sul sistema in Omaha, connesso al gestore code OMAHA. Viene gestito dagli altri gestori code nel cluster che inserendo i messaggi sulla coda MORDERQ .
- I repository completi per il cluster MAILORDER sono conservati sui due gestori code CHICAGO e CHICAGO2.
- Il protocollo di rete è TCP.

Informazioni su questa attività

Seguire questi passi per aggiungere un nuovo cluster interconnesso.

Procedura

1. Creare un elenco nomi dei nomi cluster.

   I gestori code del repository completo in CHICAGO e in CHICAGO2 ora conterranno i repository completi per entrambi i cluster CHNSTORE e MAILORDER . Innanzitutto, creare un elenco nomi contenente i nomi dei cluster. Definire l'elenco nomi su CHICAGO e CHICAGO2 , come segue:

   ```
   DEFINE NAMELIST(CHAINMAIL)
          DESCR('List of cluster names')
          NAMES(CHNSTORE, MAILORDER)
   ```

2. Modificare le definizioni di due gestori code.

   Modificare ora le due definizioni del gestore code in CHICAGO e CHICAGO2. Attualmente queste definizioni mostrano che i gestori code contengono repository completi per il cluster CHNSTORE. Modificare tale definizione per mostrare che i gestori code contengono repository completi per tutti i cluster elencati nell'elenco nomi CHAINMAIL . Modificare le definizioni dei gestori code CHICAGO e CHICAGO2 :

   ```
   ALTER QMGR REPOS(' ') REPOSNL(CHAINMAIL)
   ```

3. Modificare i canali CLUSRCVR su CHICAGO e CHICAGO2.

   Le definizioni di canale CLUSRCVR in CHICAGO e CHICAGO2 mostrano che i canali sono disponibili nel cluster CHNSTORE. È necessario modificare la definizione del ricevente del cluster per mostrare che i canali sono disponibili per tutti i cluster elencati nell'elenco nomi CHAINMAIL . Modificare la definizione del ricevente cluster in CHICAGO:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSRCVR)
         CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

In CHICAGO2, immettere il comando:

```
ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSRCVR)
      CLUSTER(' ') CLUSNL(CHAINMAIL)
```

4. Modificare i canali CLUSSDR su CHICAGO e CHICAGO2.

   Modificare le definizioni di canale CLUSSDR per aggiungere l'elenco nomi. In CHICAGO, immettere il comando:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR)
         CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

   In CHICAGO2, immettere il comando:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSSDR)
         CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

5. Creare un elenco nomi su SEATTLE e ATLANTA.

   Poiché SEATTLE e ATLANTA saranno membri di più di un cluster, è necessario creare un elenco nomi contenente i nomi dei cluster. Definire l'elenco nomi su SEATTLE e ATLANTA , come segue:

   ```
   DEFINE NAMELIST(CHAINMAIL)
          DESCR('List of cluster names')
          NAMES(CHNSTORE, MAILORDER)
   ```

6. Modificare i canali CLUSRCVR su SEATTLE e ATLANTA.

   Le definizioni di canale CLUSRCVR in SEATTLE e ATLANTA mostrano che i canali sono disponibili nel cluster CHNSTORE. Modificare le definizioni di canali di ricezione cluster per mostrare che i canali sono disponibili per tutti i cluster elencati nell'elenco nomi CHAINMAIL . In SEATTLE, immettere il comando:

   ```
   ALTER CHANNEL(CHNSTORE.SEATTLE) CHLTYPE(CLUSRCVR)
         CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

   In ATLANTA, immettere il comando:

   ```
   ALTER CHANNEL(CHNSTORE.ATLANTA) CHLTYPE(CLUSRCVR)
         CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

7. Modificare i canali CLUSSDR su SEATTLE e ATLANTA.

   Modificare le definizioni di canale CLUSSDR per aggiungere l'elenco nomi. In SEATTLE, immettere il comando:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSSDR)
         CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

   In ATLANTA, immettere il comando:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR)
         CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

8. Definire i canali CLUSRCVR e CLUSSDR su HARTFORD e OMAHA .

   Nei due nuovi gestori code HARTFORD e OMAHA, definire i canali ricevente e mittente del cluster. Non importa in quale sequenza si fanno le definizioni. In HARTFORD, immettere:

   ```
   DEFINE CHANNEL(MAILORDER.HARTFORD) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(HARTFORD.CHSTORE.COM) CLUSTER(MAILORDER)
   DESCR('Cluster-receiver channel for HARTFORD')

   DEFINE CHANNEL(MAILORDER.CHICAGO) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(CHICAGO.CHSTORE.COM) CLUSTER(MAILORDER)
   DESCR('Cluster-sender channel from HARTFORD to repository at CHICAGO')
   ```

In OMAHA, immettere:

```
DEFINE CHANNEL(MAILORDER.OMAHA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(OMAHA.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-receiver channel for OMAHA')

DEFINE CHANNEL(MAILORDER.CHICAGO) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(CHICAGO.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-sender channel from OMAHA to repository at CHICAGO')
```

9. Definire la coda MORDERQ su OMAHA .

   Il passo finale per completare questa attività consiste nel definire la coda MORDERQ sul gestore code OMAHA . In OMAHA, immettere:

   ```
   DEFINE QLOCAL(MORDERQ) CLUSTER(MAILORDER)
   ```

10. Verificare che le modifiche al cluster siano state propagate.

    Verificare che le definizioni create con le operazioni precedenti siano state propagate attraverso il cluster. Immettere i comandi riportati di seguito su un gestore code del repository completo:

    ```
    DIS QCLUSTER (MORDERQ)
    DIS CLUSQMGR
    ```

11.

Risultati

Il cluster configurato da questa attività viene mostrato in Figura 42 a pagina 242.

Ora abbiamo due cluster che si sovrappongono. I repository completi per entrambi i cluster si trovano in CHICAGO e CHICAGO2. L'applicazione dell'ordine di posta in esecuzione su OMAHA è indipendente dall'applicazione dell'inventario in esecuzione su CHICAGO. Tuttavia, alcuni dei gestori code che si trovano nel cluster CHNSTORE si trovano anche nel cluster MAILORDER e possono quindi inviare messaggi a entrambe le applicazioni. Prima di eseguire questa attività per sovrapporre due cluster, tenere presente la possibilità di conflitti tra nomi di coda.

Si supponga che su NEWYORK nel cluster CHNSTORE e su OMAHA in cluster MAILORDER, vi sia una coda denominata ACCOUNTQ . Se si sovrappongono i cluster e quindi un'applicazione su SEATTLE inserisce un messaggio nella coda ACCOUNTQ , il messaggio può andare a una delle istanze di ACCOUNTQ .

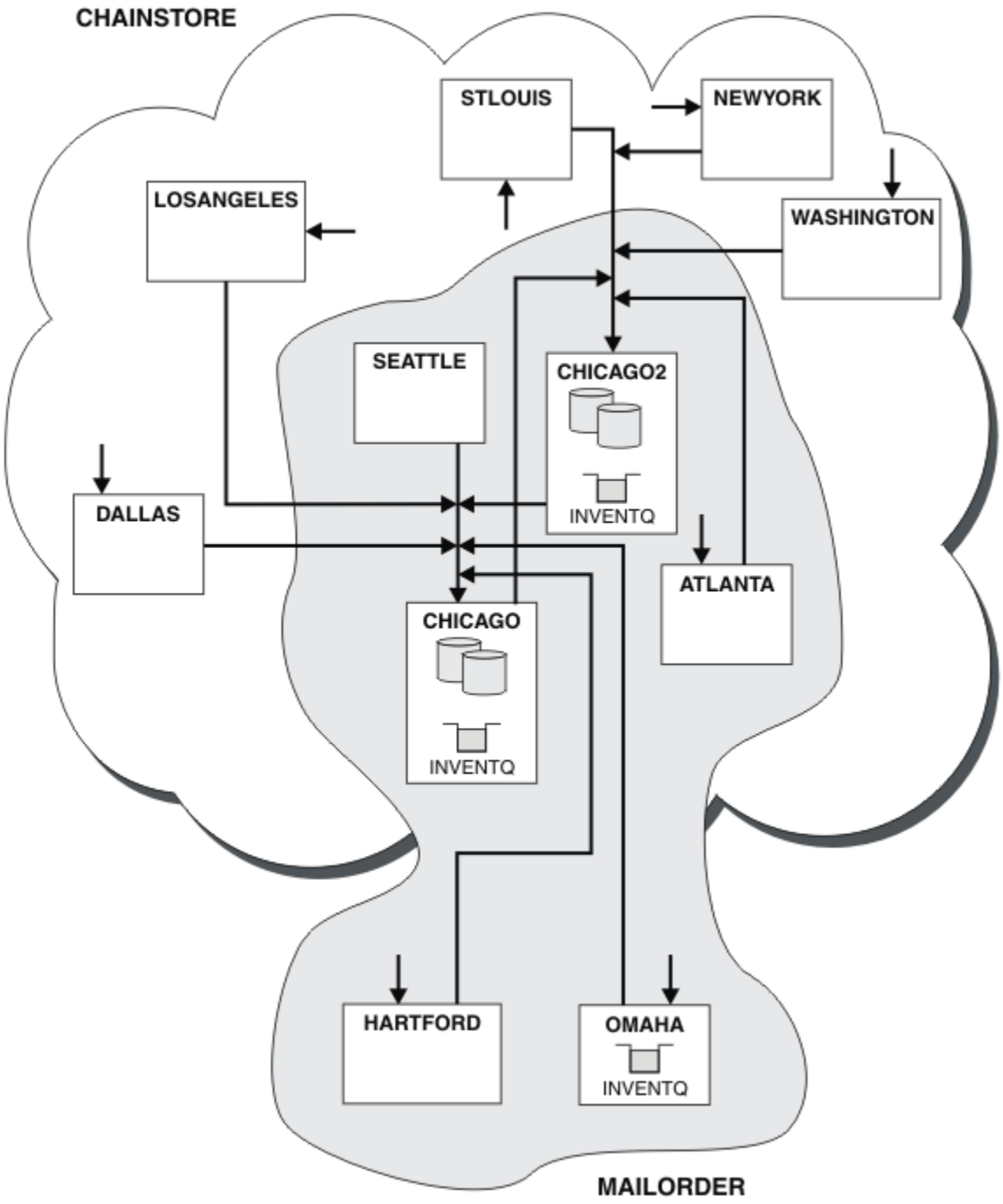


Figura 42. Cluster interconnessi

Operazioni successive

Si supponga di decidere di unire il cluster MAILORDER con quello CHNSTORE per formare un cluster di grandi dimensioni denominato CHNSTORE.

Per unire il cluster MAILORDER con il cluster CHNSTORE , in modo che CHICAGO e CHICAGO2 conservino i repository completi:

- Modificare le definizioni del gestore code per CHICAGO e CHICAGO2, rimuovendo l'attributo REPOSNL, che specifica l'elenco nomi (CHAINMAIL) e sostituendolo con un attributo REPOS che specifica il nome cluster (CHNSTORE). Ad esempio:

```
ALTER QMGR(CHICAGO) REPOSNL(' ') REPOS(CHNSTORE)
```

- Su ciascun gestore code nel cluster MAILORDER , modificare tutte le definizioni di canale e di coda per modificare il valore dell'attributo CLUSTER da MAILORDER a CHNSTORE. Ad esempio, in HARTFORD , immettere:

```
ALTER CHANNEL(MAILORDER.HARTFORD) CLUSTER(CHNSTORE)
```

  In OMAHA immettere:

```
ALTER QLOCAL(MORDERQ) CLUSTER(CHNSTORE)
```

- Modificare tutte le definizioni che specificano l'elenco nomi cluster CHAINMAIL, ossia le definizioni del canale CLUSRCVR e CLUSSDR in CHICAGO, CHICAGO2, SEATTLEe ATLANTA , per indicare invece il cluster CHNSTORE.

Da questo esempio, è possibile vedere il vantaggio di utilizzare gli elenchi nomi. Invece di modificare le definizioni del gestore code per CHICAGO e CHICAGO2 , è possibile modificare il valore dell'elenco nomi CHAINMAIL. Allo stesso modo, invece di modificare le definizioni di canale CLUSRCVR e CLUSSDR all'indirizzo CHICAGO, CHICAGO2 , SEATTLEe ATLANTA, è possibile ottenere il risultato richiesto modificando l'elenco nomi.

Rimozione di una rete cluster

Rimuovere un cluster da una rete e ripristinare la configurazione dell'accodamento distribuito.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Un cluster IBM WebSphere MQ è stato impostato come descritto in “Conversione di una rete esistente in un cluster” a pagina 236.
- Questo cluster deve essere rimosso dal sistema. La rete di gestori code deve continuare a funzionare come prima dell'implementazione del cluster.

Informazioni su questa attività

Seguire questa procedura per rimuovere una rete cluster.

Procedura

1. Rimuovere le code cluster dal cluster CHNSTORE .

   Su CHICAGO e CHICAGO2, modificare la definizione della coda locale per la coda INVENTQ per eliminare la coda dal cluster. Immettere il seguente comando:

```
ALTER QLOCAL(INVENTQ) CLUSTER(' ')
```

   Quando si modifica la coda, le informazioni nei repository completi vengono aggiornate e propagate in tutto il cluster. Le applicazioni attive che utilizzano MQOO_BIND_NOT_FIXEDe le applicazioni che utilizzano MQOO_BIND_AS_Q_DEF in cui la coda è stata definita con DEFBIND(NOTFIXED), non riescono alla successiva chiamata MQPUT o MQPUT1 tentata. Viene restituito il codice di errore MQRC_UNKNOWN_OBJECT_NAME .

Non è necessario eseguire prima il passo 1, ma in caso contrario, eseguirlo dopo il passo 4.

2. Arrestare tutte le applicazioni che hanno accesso alla coda cluster.

   Arrestare tutte le applicazioni che hanno accesso alle code cluster. In caso contrario, alcune informazioni sul cluster potrebbero rimanere sul gestore code locale quando si aggiorna il cluster nel passo 5. Queste informazioni vengono rimosse quando tutte le applicazioni sono state arrestate e i canali cluster sono stati disconnessi.

3. Rimuovere l'attributo repository dai gestori code del repository completo.

   Su CHICAGO e CHICAGO2, modificare le definizioni del gestore code in modo da rimuovere l'attributo del repository. Per eseguire questa operazione, immettere il comando:

   ```
   ALTER QMGR REPOS(' ')
   ```

   I gestori code informano gli altri gestori code nel cluster che non detengono più i repository completi. Quando gli altri gestori code ricevono queste informazioni, viene visualizzato un messaggio che indica che il repository completo è terminato. Vengono inoltre visualizzati uno o più messaggi che indicano che non sono più disponibili repository per il cluster CHNSTORE .

4. Rimuovere i canali cluster.

   Su CHICAGO , eliminare i canali cluster:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR) CLUSTER(' ')
   ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSRCVR) CLUSTER(' ')
   ```

   Nota: È importante immettere prima il comando CLUSSDR , quindi il comando CLUSRCVR . Non immettere prima il comando CLUSRCVR , quindi il comando CLUSSDR . In questo modo, vengono creati canali in dubbio con stato ARRESTATO . È quindi necessario emettere un comando START CHANNEL per ripristinare i canali arrestati; ad esempio, START CHANNEL(CHNSTORE.CHICAGO).

   Vengono visualizzati messaggi che indicano che non vi sono repository per il cluster CHNSTORE.

   Se non sono state rimosse le code del cluster come descritto nel passo 1, procedere ora.

5. Arrestare i canali cluster.

   Su CHICAGO arrestare i canali cluster con i seguenti comandi:

   ```
   STOP CHANNEL(CHNSTORE.CHICAGO2)
   STOP CHANNEL(CHNSTORE.CHICAGO)
   ```

6. Ripetere i passi 4 e 5 per ogni gestore code del cluster.
7. Arrestare i canali cluster, quindi rimuovere tutte le definizioni per i canali cluster e le code cluster da ogni gestore code.
8. Opzionale: Cancellare le informazioni sul cluster memorizzato nella cache contenute nel gestore code.

   Anche se i gestori code non sono più membri del cluster, ciascuno di essi conserva una copia memorizzata nella cache delle informazioni sul cluster. Se si desidera rimuovere questi dati, consultare l'attività “Ripristino di un gestore code allo stato pre - cluster” a pagina 248.

9. Sostituire le definizioni della coda remota per INVENTQ

   In modo che la rete possa continuare a funzionare, sostituire la definizione della coda remota per INVENTQ in ogni gestore code.

10. Riordinare il cluster.

    Eliminare tutte le definizioni di coda o canale non più necessarie.

Rimozione di un gestore code da un cluster

Rimuovere un gestore code da un cluster, in scenari in cui il gestore code può comunicare normalmente con almeno un repository completo nel cluster.

Prima di iniziare

Questo metodo è la procedura ottimale per gli scenari in cui è disponibile almeno un repository completo e può essere contattato dal gestore code che viene rimosso. Questo metodo implica il minimo intervento manuale e consente al gestore code di negoziare un ritiro controllato dal cluster. Se il gestore code che viene rimosso non può contattare un repository completo, consultare "Rimozione di un gestore code da un cluster: metodo alternativo" a pagina 246.

Prima di rimuovere il gestore code dal cluster, è necessario assicurarsi che il gestore code non ospiti più le risorse richieste dal cluster:

- Se sul gestore code è presente un repository completo, completare i punti da 1 a 4 da "Spostamento di un repository completo in un altro gestore code" a pagina 233.
- Se il gestore code ospita le code cluster, completare i passi da 1 a 7 da "Rimozione di una coda cluster da un gestore code" a pagina 231.
- Se il gestore code ospita argomenti cluster, eliminare gli argomenti (ad esempio, utilizzando il comando DELETE TOPIC) o spostarli su altri host.

  Nota: Se si rimuove un gestore code da un cluster e il gestore code ospita ancora un argomento cluster, il gestore code potrebbe continuare a tentare di consegnare le pubblicazioni ai gestori code rimasti nel cluster fino a quando l'argomento non viene eliminato.

Informazioni su questa attività

Questa attività di esempio rimuove il gestore code LONDON dal cluster INVENTORY . Il cluster INVENTORY è impostato come descritto in "Aggiunta di un gestore code a un cluster" a pagina 199e modificato come descritto in "Rimozione di una coda cluster da un gestore code" a pagina 231.

Il processo di rimozione di un gestore code da un cluster è più complicato del processo di aggiunta di un gestore code.

Quando un gestore code si unisce a un cluster, i membri esistenti del cluster non conoscono il nuovo gestore code e quindi non hanno interazioni con esso. È necessario creare nuovi canali mittente e ricevente sul gestore code di unione in modo che possa connettersi a un repository completo.

Quando un gestore code viene rimosso da un cluster, è probabile che le applicazioni connesse al gestore code utilizzino oggetti come code ospitate altrove nel cluster. Inoltre, le applicazioni connesse ad altri gestori code nel cluster potrebbero utilizzare oggetti ospitati sul gestore code di destinazione. Come risultato di queste applicazioni, il gestore code corrente potrebbe creare ulteriori canali mittente per stabilire la comunicazione con i membri del cluster diversi dal repository completo utilizzato per unirsi al cluster. Ogni gestore code nel cluster dispone di una copia memorizzata nella cache dei dati che descrive altri membri cluster. Ciò potrebbe includere quello che si sta rimuovendo.

Procedura

1. Modificare i canali riceventi del cluster definiti manualmente per rimuoverli dal cluster, sul gestore code LONDON:

   ```
   ALTER CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) CLUSTER(' ')
   ```

2. Modificare i canali mittenti del cluster definiti manualmente per rimuoverli dal cluster sul gestore code LONDON:

   ```
   ALTER CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSSDR) CLUSTER(' ')
   ```

   Gli altri gestori code del cluster apprendono che questo gestore code e le sue risorse cluster non fanno più parte del cluster.
3. Monitorare la coda di trasmissione del cluster, sul gestore code LONDON, fino a quando non sono presenti messaggi in attesa di essere trasmessi a un repository completo nel cluster.

   ```
   DISPLAY CHSTATUS(INVENTORY.LONDON) XQMSGSA
   ```

Se i messaggi rimangono nella coda di trasmissione, determinare il motivo per cui non vengono inviati ai repository completi PARIS e NEWYORK prima di continuare.

Risultati

Il gestore code LONDON non è più parte del cluster. Tuttavia, può ancora funzionare come gestore code indipendente.

Operazioni successive

Il risultato di queste modifiche può essere confermato emettendo il seguente comando sui restanti membri del cluster:

```
DISPLAY CLUSQMGR(LONDON)
```

Il gestore code continua ad essere visualizzato fino a quando i canali mittenti del cluster definiti automaticamente non vengono arrestati. È possibile attendere che ciò si verifichi oppure continuare a monitorare le istanze attive immettendo il seguente comando:

```
DISPLAY CHANNEL(INVENTORY.LONDON)
```

Quando si è certi che nessun altro messaggio viene recapitato a questo gestore code, è possibile arrestare i canali mittenti del cluster in LONDON immettendo il seguente comando sui restanti membri del cluster:

```
STOP CHANNEL(INVENTORY.LONDON) STATUS(INACTIVE)
```

Dopo che le modifiche sono state propagate in tutto il cluster e che non sono stati consegnati ulteriori messaggi a questo gestore code, arrestare ed eliminare il canale CLUSRCVR su LONDON:

```
STOP CHANNEL(INVENTORY.LONDON)
DELETE CHANNEL(INVENTORY.LONDON)
```

Il gestore code rimosso può essere aggiunto nuovamente al cluster in un secondo momento, come descritto in “Aggiunta di un gestore code a un cluster” a pagina 199. Il gestore code rimosso continua a memorizzare nella cache i membri rimanenti del cluster per un periodo massimo di 90 giorni. Se si preferisce non attendere la scadenza di questa cache, è possibile rimuoverla forzatamente come descritto in “Ripristino di un gestore code allo stato pre - cluster” a pagina 248.

Rimozione di un gestore code da un cluster: metodo alternativo

Rimuovere un gestore code da un cluster, in scenari in cui, a causa di un significativo problema di sistema o di configurazione, il gestore code non può comunicare con alcun repository completo nel cluster.

Prima di iniziare

Questo metodo alternativo di rimozione di un gestore code da un cluster arresta ed elimina manualmente tutti i canali cluster che collegano al cluster il gestore code rimosso e rimuove forzatamente il gestore code dal cluster. Questo metodo viene utilizzato in scenari in cui il gestore code che viene rimosso non può comunicare con nessuno dei repository completi. Ciò potrebbe verificarsi (ad esempio) perché il gestore code ha smesso di funzionare o perché si è verificato un errore di comunicazioni prolungato tra il gestore code e il cluster. Altrimenti, utilizzare il metodo più comune: “Rimozione di un gestore code da un cluster” a pagina 244.

Prima di rimuovere il gestore code dal cluster, è necessario assicurarsi che il gestore code non ospiti più le risorse richieste dal cluster:

- Se sul gestore code è presente un repository completo, completare i punti da 1 a 4 da “Spostamento di un repository completo in un altro gestore code” a pagina 233.

- Se il gestore code ospita le code cluster, completare i passi da 1 a 7 da “Rimozione di una coda cluster da un gestore code” a pagina 231.
- Se il gestore code ospita argomenti cluster, eliminare gli argomenti (ad esempio, utilizzando il comando DELETE TOPIC) o spostarli su altri host.

  Nota: Se si rimuove un gestore code da un cluster e il gestore code ospita ancora un argomento cluster, il gestore code potrebbe continuare a tentare di consegnare le pubblicazioni ai gestori code rimasti nel cluster fino a quando l'argomento non viene eliminato.

Informazioni su questa attività

Questa attività di esempio rimuove il gestore code LONDON dal cluster INVENTORY . Il cluster INVENTORY è impostato come descritto in “Aggiunta di un gestore code a un cluster” a pagina 199e modificato come descritto in “Rimozione di una coda cluster da un gestore code” a pagina 231.

Il processo di rimozione di un gestore code da un cluster è più complicato del processo di aggiunta di un gestore code.

Quando un gestore code si unisce a un cluster, i membri esistenti del cluster non conoscono il nuovo gestore code e quindi non hanno interazioni con esso. È necessario creare nuovi canali mittente e ricevente sul gestore code di unione in modo che possa connettersi a un repository completo.

Quando un gestore code viene rimosso da un cluster, è probabile che le applicazioni connesse al gestore code utilizzino oggetti come code ospitate altrove nel cluster. Inoltre, le applicazioni connesse ad altri gestori code nel cluster potrebbero utilizzare oggetti ospitati sul gestore code di destinazione. Come risultato di queste applicazioni, il gestore code corrente potrebbe creare ulteriori canali mittente per stabilire la comunicazione con i membri del cluster diversi dal repository completo utilizzato per unirsi al cluster. Ogni gestore code nel cluster dispone di una copia memorizzata nella cache dei dati che descrive altri membri cluster. Ciò potrebbe includere quello che si sta rimuovendo.

Questa procedura potrebbe essere appropriata in caso di emergenza, quando non è possibile attendere che il gestore code lasci il cluster correttamente.

Procedura

1. Arresta tutti i canali utilizzati per comunicare con altri gestori code nel cluster. Utilizzare MODE(FORCE) per arrestare il canale di CLUSRCVR sul gestore code LONDON. Altrimenti, potrebbe essere necessario attendere che il gestore code mittente arresti il canale:

   ```
   STOP CHANNEL(INVENTORY.LONDON) MODE(FORCE)
   STOP CHANNEL(INVENTORY.TORONTO)
   STOP CHANNEL(INVENTORY.PARIS)
   STOP CHANNEL(INVENTORY.NEWYORK)
   ```

2. Monitorare gli stati del canale, nel gestore code LONDON, fino a quando i canali non vengono arrestati:

   ```
   DISPLAY CHSTATUS(INVENTORY.LONDON)
   DISPLAY CHSTATUS(INVENTORY.TORONTO)
   DISPLAY CHSTATUS(INVENTORY.PARIS)
   DISPLAY CHSTATUS(INVENTORY.NEWYORK)
   ```

   Nessun altro messaggio dell'applicazione viene inviato a o dagli altri gestori code nel cluster dopo l'arresto dei canali.
3. Eliminare i canali cluster definiti manualmente, sul gestore code LONDON:

   ```
   DELETE CHANNEL(INVENTORY.NEWYORK)
   DELETE CHANNEL(INVENTORY.TORONTO)
   ```

4. I restanti gestori code nel cluster conservano ancora la conoscenza del gestore code rimosso e potrebbero continuare a inviargli messaggi. Per eliminare la conoscenza dai rimanenti gestori code, reimpostare il gestore code rimosso dal cluster su uno dei repository completi:

   ```
   RESET CLUSTER(INVENTORY) ACTION(FORCEREMOVE) QMNAME(LONDON) QUEUES(YES)
   ```

Se nel cluster potrebbe essere presente un altro gestore code con lo stesso nome del gestore code rimosso, specificare il **QMID** del gestore code rimosso.

Risultati

Il gestore code LONDON non è più parte del cluster. Tuttavia, può ancora funzionare come gestore code indipendente.

Operazioni successive

Il risultato di queste modifiche può essere confermato emettendo il seguente comando sui restanti membri del cluster:

```
DISPLAY CLUSQMGR(LONDON)
```

Il gestore code continua ad essere visualizzato fino a quando i canali mittenti del cluster definiti automaticamente non vengono arrestati. È possibile attendere che ciò si verifichi oppure continuare a monitorare le istanze attive immettendo il seguente comando:

```
DISPLAY CHANNEL(INVENTORY.LONDON)
```

Dopo che le modifiche sono state propagate in tutto il cluster e che non sono stati recapitati ulteriori messaggi a questo gestore code, eliminare il canale CLUSRCVR su LONDON:

```
DELETE CHANNEL(INVENTORY.LONDON)
```

Il gestore code rimosso può essere aggiunto nuovamente al cluster in un secondo momento, come descritto in “Aggiunta di un gestore code a un cluster” a pagina 199. Il gestore code rimosso continua a memorizzare nella cache i membri rimanenti del cluster per un periodo massimo di 90 giorni. Se si preferisce non attendere la scadenza di questa cache, è possibile rimuoverla forzatamente come descritto in “Ripristino di un gestore code allo stato pre - cluster” a pagina 248.

Ripristino di un gestore code allo stato pre - cluster

Quando un gestore code viene rimosso da un cluster, conserva la conoscenza dei restanti membri del cluster. Questa conoscenza alla fine scade e viene eliminata automaticamente. Tuttavia, se si preferisce eliminarlo immediatamente, è possibile utilizzare i passi riportati in questo argomento.

Prima di iniziare

Si presume che il gestore code sia stato rimosso dal cluster e che non stia più eseguendo alcuna attività nel cluster. Ad esempio, le code non ricevono più messaggi dal cluster e nessuna applicazione è in attesa che i messaggi arrivino in queste code.

Importante: Se si rimuove un gestore code da un cluster e lo si aggiorna utilizzando REPOS (YES), non sarà possibile aggiungerlo nuovamente modificando semplicemente l'attributo CLUSTER di CLUSRCVR. Dopo aver modificato l'attributo CLUSTER di CLUSRCVR in modo che non sia vuoto (ossia, il nome cluster), sarà inoltre necessario emettere il cluster di aggiornamento con REPOS (NO), a questo punto i numeri di sequenza interni su CLUSRCVR verranno aggiornati. Quindi, il gestore code riuscirà a reintrodursi nei repository completi e nel resto dei membri del cluster. (Si noti che la versione REPOS (NO) del comando deve essere eseguita dopo che al canale CLUSRCVR è stato assegnato il nome cluster corretto.)

Questa limitazione si applica solo a IBM WebSphere MQ Version 7.5 .

Informazioni su questa attività

Quando un gestore code viene rimosso da un cluster, conserva la conoscenza dei restanti membri del cluster per un massimo di 90 giorni. Ciò può avere dei vantaggi di sistema, in particolare se il gestore code si unisce rapidamente al cluster. Quando questa conoscenza alla fine scade, viene eliminata automaticamente. Tuttavia, ci sono dei motivi per cui è preferibile eliminare queste informazioni manualmente. Ad esempio:

- È possibile confermare di aver arrestato tutte le applicazioni su questo gestore code che in precedenza utilizzavano le risorse cluster. Fino alla scadenza della conoscenza dei restanti membri del cluster, qualsiasi applicazione continua a scrivere in una coda di trasmissione. Una volta eliminata la conoscenza del cluster, il sistema genera un messaggio di errore quando tale applicazione tenta di utilizzare le risorse del cluster.
- Quando si visualizzano le informazioni sullo stato per il gestore code, è possibile che si preferisca non visualizzare le informazioni in scadenza sui restanti membri del cluster.

Questa attività utilizza il cluster INVENTORY come esempio. Il gestore code LONDON è stato rimosso dal cluster INVENTORY come descritto in "Rimozione di un gestore code da un cluster" a pagina 244. Per eliminare la conoscenza dei restanti membri del cluster, immettere il seguente comando sul gestore code LONDON .

Procedura

1. Rimuovere tutta la memoria degli altri gestori code nel cluster da questo gestore code:

```
REFRESH CLUSTER(INVENTORY) REPOS(YES)
```

2. Monitorare il gestore code fino a quando tutte le risorse cluster non sono più disponibili:

```
DISPLAY CLUSQMGR(*) CLUSTER(INVENTORY)
DISPLAY QCLUSTER(*) CLUSTER(INVENTORY)
DISPLAY TOPIC(*) CLUSTER(INVENTORY)
```

Concetti correlati

Cluster

"Confronto tra cluster e accodamento distribuito" a pagina 164
Confrontare i componenti che devono essere definiti per connettere i gestori code utilizzando l'accodamento distribuito e il cluster.

"Componenti di un cluster" a pagina 166
I cluster sono composti da gestore code, repository di cluster, canali cluster e code cluster.

"Gestione dei cluster IBM WebSphere MQ" a pagina 188
È possibile creare, estendere e gestire cluster IBM WebSphere MQ .

Gestione di un gestore code

Sospendere e riprendere un gestore code da un cluster per eseguire la manutenzione.

Informazioni su questa attività

Di tanto in tanto, potrebbe essere necessario eseguire la manutenzione su un gestore code che fa parte di un cluster. Ad esempio, potrebbe essere necessario eseguire backup dei dati nelle relative code o applicare correzioni al software. Se il gestore code ospita delle code, le sue attività devono essere sospese. Una volta completata la manutenzione, è possibile riprendere le attività.

Procedura

1. Sospendere un gestore code immettendo il comando SUSPEND QMGR **runmqsc** :

```
SUSPEND QMGR CLUSTER(SALES)
```

Il comando SUSPEND **runmqsc** notifica ai gestori code nel cluster SALES che questo gestore code è stato sospeso.

Lo scopo del comando SUSPEND QMGR è solo quello di consigliare agli altri gestori code di evitare l'invio di messaggi a questo gestore code, se possibile. Ciò non significa che il gestore code sia disabilitato. Alcuni messaggi che devono essere gestiti da questo gestore code vengono ancora inviati ad esso, ad esempio quando questo gestore code è l'unico host di una coda cluster.

Mentre il gestore code è sospeso, le routine di gestione del carico di lavoro evitano di inviarle messaggi. I messaggi che devono essere gestiti da tale gestore code includono i messaggi inviati dal gestore code locale.

WebSphere MQ utilizza un algoritmo di bilanciamento del carico di lavoro per determinare quali destinazioni sono adatte, piuttosto che selezionare il gestore code locale quando possibile.

a) Applicare la sospensione di un gestore code utilizzando l'opzione FORCE sul comando SUSPEND QMGR :

```
SUSPEND QMGR CLUSTER(SALES) MODE(FORCE)
```

MODE(FORCE) arresta in modo forzato tutti i canali in entrata da altri gestori code nel cluster. Se non si specifica MODE(FORCE), si applica il valore predefinito MODE(QUIESCE) .

2. Eseguire tutte le attività di manutenzione necessarie.
3. Riprendere il gestore code immettendo il comando RESUME QMGR **runmqsc** :

```
RESUME QMGR CLUSTER(SALES)
```

Risultati

Il comando di RESUME **runmqsc** notifica ai repository completi che il gestore code è nuovamente disponibile. I gestori code del repository completo diffondono queste informazioni ad altri gestori code che hanno richiesto aggiornamenti alle informazioni relative a questo gestore code.

Manutenzione della coda di trasmissione del cluster

Fare ogni sforzo per mantenere disponibili le code di trasmissione del cluster. Sono essenziali per le prestazioni dei cluster.

Prima di iniziare

- Assicurarsi che la coda di trasmissione del cluster non diventi piena.
- Fare attenzione a non immettere un comando ALTER **runmqsc** per impostarlo come disabilitato o disabilitato accidentalmente.
- Assicurarsi che il supporto in cui la coda di trasmissione cluster è memorizzata su non diventi pieno.

Aggiornamento di un gestore code cluster

È possibile rimuovere i canali definiti automaticamente e gli oggetti cluster definiti automaticamente dal repository locale utilizzando il comando REFRESH CLUSTER . Nessun messaggio viene perso.

Prima di iniziare

Potrebbe essere richiesto di utilizzare il comando dal centro di supporto IBM . Non utilizzare il comando senza un'attenta considerazione. Ad esempio, per i cluster di grandi dimensioni, l'utilizzo del comando **REFRESH CLUSTER** può essere disruttivo per 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 “Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER” a pagina 310.

Informazioni su questa attività

Un gestore code può avviare nuovamente un cluster. In circostanze normali, non è necessario utilizzare il comando REFRESH CLUSTER .

Procedura

Immettere il comando REFRESH CLUSTER **MQSC** da un gestore code per rimuovere il gestore code del cluster definito automaticamente e gli oggetti coda dal repository locale.

Il comando rimuove solo gli oggetti che fanno riferimento ad altri gestori code, non rimuove gli oggetti relativi al gestore code locale. Il comando rimuove anche i canali definiti automaticamente. Rimuove i canali che non hanno messaggi nella coda di trasmissione del cluster e che non sono collegati a un gestore code del repository completo.

Risultati

In effetti, il comando REFRESH CLUSTER consente a un gestore code di essere avviato a freddo rispetto al contenuto del repository completo. IBM WebSphere MQ garantisce che non si perda alcun dato dalle code.

Concetti correlati

"Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER" a pagina 310
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.

Ripristino di un gestore code

Aggiornare le informazioni del cluster su un gestore code utilizzando il comando REFRESH CLUSTER **runmqsc** . Seguire questa procedura dopo aver ripristinato un gestore code da un backup con riferimento temporale.

Prima di iniziare

È stato ripristinato un gestore code cluster da un backup point - in - time.

Informazioni su questa attività

Per recuperare un gestore code in un cluster, ripristinare il gestore code e aggiornare le relative informazioni utilizzando il comando REFRESH CLUSTER **runmqsc** .

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 gli aggiornamenti di stato a tutti i gestori code interessati. Consultare Refreshing in a large cluster can affect performance and availability of the cluster.

Procedura

Immettere il comando REFRESH CLUSTER sul gestore code ripristinato per tutti i cluster a cui partecipa il gestore code.

Operazioni successive

Non è necessario immettere il comando REFRESH CLUSTER su un altro gestore code.

Concetti correlati

"Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER" a pagina 310
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.

Configurazione dei canali cluster per disponibilità

Seguire le procedure di configurazione ottimali per mantenere i canali cluster in esecuzione senza problemi in caso di arresti di rete intermittenti.

Prima di iniziare

I cluster ti sollevano dalla necessità di definire i canali, ma devi comunque mantenerli. La stessa tecnologia di canale viene utilizzata per la comunicazione tra i gestori code in un cluster come viene utilizzata nell'accodamento distribuito. Per comprendere i canali cluster, è necessario avere dimestichezza con questioni quali:

- Funzionamento dei canali
- Come trovare il loro stato
- Come utilizzare le uscite canale

Informazioni su questa attività

Si consiglia di prestare particolare attenzione ai seguenti punti:

Procedura

Considerare i seguenti punti quando si configurano i canali cluster

- Scegliere i valori per `HBINT` o `KAINT` sui canali mittenti del cluster e i canali riceventi del cluster che non caricano la rete con molti flussi heartbeat o keep alive. Un intervallo inferiore a circa 10 secondi fornisce falsi errori, se la rete a volte rallenta e introduce ritardi di questa lunghezza.
- Impostare il valore `BATCHHB` per ridurre la finestra per la causa di un messaggio di cui è stato eseguito il marooned poiché è in dubbio su un canale non riuscito. Un batch in dubbio su un canale non riuscito è più probabile che si verifichi se il batch viene fornito più a lungo da riempire. Se il traffico di messaggi lungo il canale è sporadico con lunghi periodi di tempo tra le interruzioni di messaggi, è più probabile che un batch non sia riuscito.
- Si verifica un problema se l'estremità mittente del cluster di un canale ha esito negativo e quindi tenta di riavviare prima che l'heartbeat o il keep alive abbia rilevato l'errore. Il riavvio del mittente del canale viene rifiutato se l'estremità ricevente del cluster del canale è rimasta attiva. Per evitare l'errore, fare in modo che il canale ricevente del cluster venga terminato e riavviato quando un canale mittente del cluster tenta il riavvio.

  Su piattaforme diverse da z/OS
  Controllare il problema dell'estremità ricevente del cluster del canale rimasto attivo utilizzando gli attributi `AdoptNewMCA`, `AdoptNewMCATimeoute AdoptNewMCACheck` nel file `qm.ini` o nel registro Windows NT .

Instradamento dei messaggi verso e dai cluster

Utilizzare gli alias di coda, gli alias di gestore code e le definizioni di code remote per connettere i cluster a gestori code esterni e altri cluster.

Per i dettagli sull'instradamento dei messaggi verso e dai cluster, consultare i topic secondari riportati di seguito:

Concetti correlati
Cluster
Funzionamento dei cluster
“Confronto tra cluster e accodamento distribuito” a pagina 164

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

“Componenti di un cluster” a pagina 166
I cluster sono composti da gestore code, repository di cluster, canali cluster e code cluster.

“Gestione dei cluster IBM WebSphere MQ” a pagina 188
È possibile creare, estendere e gestire cluster IBM WebSphere MQ .

“Cluster e alias del gestore code” a pagina 263
Utilizzare gli alias del gestore code per nascondere il nome dei gestori code quando si inviano messaggi all'interno o all'esterno di un cluster e per bilanciare il carico di lavoro dei messaggi inviati a un cluster.

“Alias coda e cluster” a pagina 265
Utilizzare gli alias della coda per nascondere il nome di una coda cluster, per raggruppare una coda, per adottare attributi differenti o per adottare controlli accessi differenti.

“Cluster e alias della coda di risposta” a pagina 265
Una definizione alias coda di risposta viene utilizzata per specificare nomi alternativi per le informazioni di risposta. Le definizioni di alias della coda di risposta possono essere utilizzate con i cluster esattamente come in un ambiente di accodamento distribuito.

Attività correlate

“Configurazione di un cluster di gestore code” a pagina 161
Utilizzare i link in questo argomento per scoprire come funzionano i cluster, come progettare una configurazione cluster e per ottenere un esempio di come impostare un cluster semplice.

“Configurazione di un nuovo cluster” a pagina 188
Seguire queste istruzioni per configurare il cluster di esempio. Istruzioni separate descrivono l'impostazione del cluster su TCP/IP, LU 6.2e con una o più code di trasmissione. Verificare il funzionamento del cluster inviando un messaggio da un gestore code all'altro.

Configurazione della richiesta/risposta a un cluster

Configurare un percorso del messaggio di richiesta / risposta da un gestore code esterno a un cluster. Nascondere i dettagli interni del cluster utilizzando un gestore code del gateway come percorso di comunicazione verso e dal cluster.

Prima di iniziare

La Figura 43 a pagina 254 mostra un gestore code denominato QM3 esterno al cluster denominato DEMO. QM3 potrebbe essere un gestore code su un prodotto WebSphere MQ che non supporta i cluster. QM3 ospita una coda denominata Q3, definita come segue:

```
DEFINE QLOCAL(Q3)
```

All'interno del cluster sono presenti due gestori code denominati QM1 e QM2. QM2 ospita una coda cluster denominata Q2, definita come segue:

```
DEFINE QLOCAL(Q2) CLUSTER(DEMO)
```

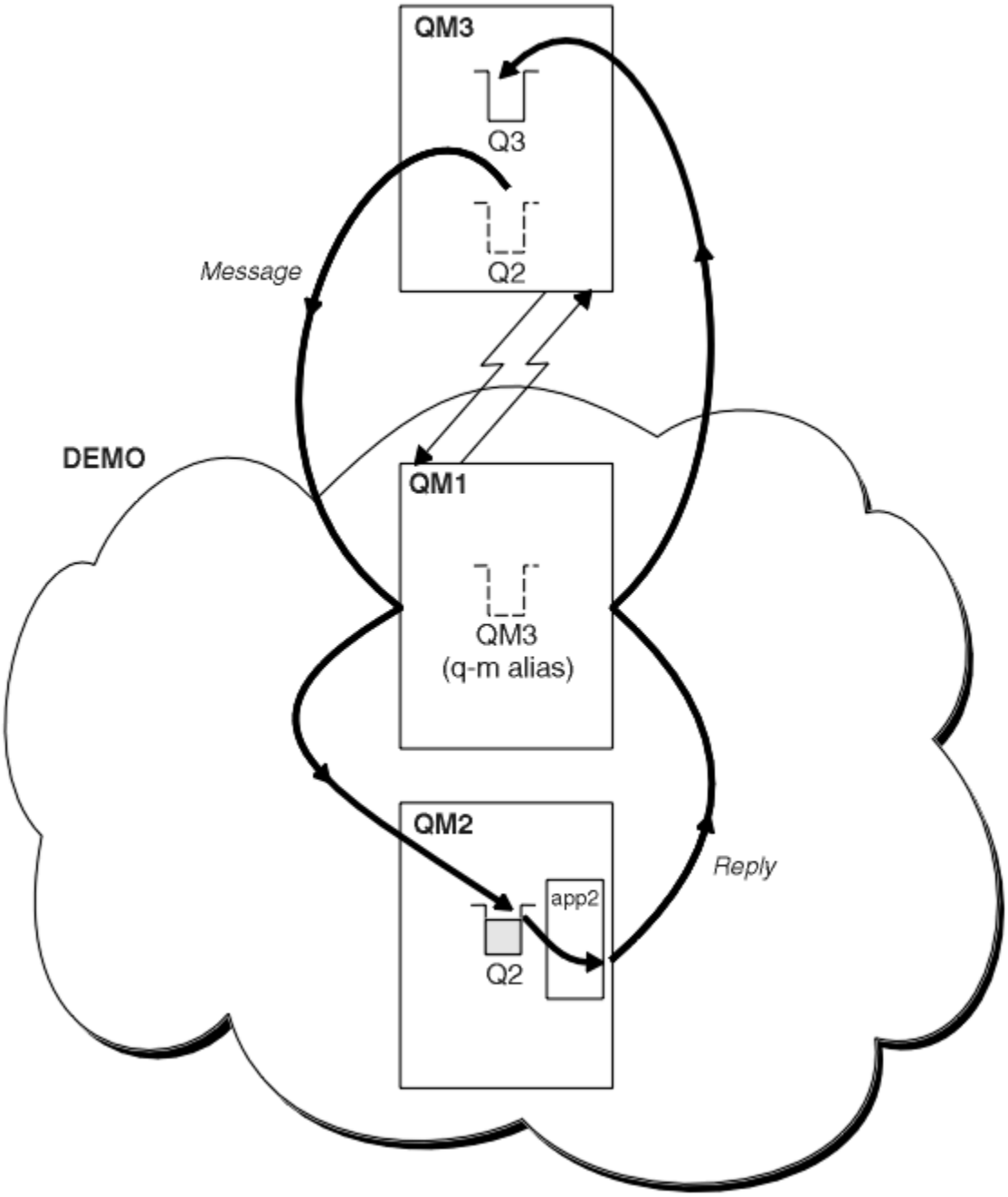


Figura 43. Inserimento da un gestore code esterno al cluster

Informazioni su questa attività

Seguire il consiglio nella procedura per impostare il percorso per i messaggi di richiesta e risposta.

Procedura

1. Inviare il messaggio di richiesta al cluster.

   Considerare come il gestore code esterno al cluster inserisce un messaggio nella coda Q2 in QM2, all'interno del cluster. Un gestore code esterno al cluster deve avere una definizione QREMOTE per ogni coda nel cluster in cui inserisce i messaggi.

   a) Definire una coda remota per Q2 su QM3.

   ```
   DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(QM2) XMITQ(QM1)
   ```

Poiché QM3 non fa parte di un cluster, deve comunicare utilizzando tecniche di accodamento distribuite. Pertanto, deve avere anche un canale mittente e una coda di trasmissione a QM1. QM1 necessita di un canale ricevente corrispondente. I canali e le code di trasmissione non vengono visualizzati esplicitamente in Figura 43 a pagina 254.

Nell'esempio, un'applicazione in QM3 emette una chiamata MQPUT per inserire un messaggio in Q2. La definizione QREMOTE fa in modo che il messaggio venga instradato a Q2 in QM2 utilizzando il canale mittente che sta ricevendo i messaggi dalla coda di trasmissione QM1 .

2. Ricevere il messaggio di risposta dal cluster.

   Utilizzare un alias del gestore code per creare un percorso di ritorno per le risposte a un gestore code esterno al cluster. Il gateway, QM1, annuncia un alias del gestore code per il gestore code esterno al cluster, QM3. Annuncia QM3 ai gestori code all'interno del cluster aggiungendo l'attributo cluster a una definizione di alias del gestore code per QM3. Una definizione alias del gestore code è come una definizione di coda remota, ma con un RNAMEvuoto.

   a) Definire un alias del gestore code per QM3 su QM1.

   ```
   DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO)
   ```

   È necessario considerare la scelta del nome della coda di trasmissione utilizzata per inoltrare le risposte da QM1 a QM3. Implicito nella definizione QREMOTE , per omissione dell'attributo XMITQ , il nome della coda di trasmissione è QM3. Ma QM3 è lo stesso nome che ci aspettiamo di pubblicizzare al resto del cluster utilizzando l'alias del gestore code. WebSphere MQ non consente di assegnare lo stesso nome alla coda di trasmissione e all'alias del gestore code. Una soluzione è quella di creare una coda di trasmissione per inoltrare i messaggi a QM3 con un nome diverso all'alias del gestore code.

   b) Fornire il nome della coda di trasmissione nella definizione QREMOTE .

   ```
   DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO) XMITQ(QM3.XMIT)
   ```

   Il nuovo alias del gestore code accoppia la nuova coda di trasmissione denominata QM3.XMIT con l'alias del gestore code QM3 . Si tratta di una soluzione semplice e corretta, ma non del tutto soddisfacente. È stata interrotta la convenzione di denominazione per le code di trasmissione per cui viene assegnato loro lo stesso nome del gestore code di destinazione. Esistono soluzioni alternative che preservano la convenzione di denominazione della coda di trasmissione?

   Il problema si verifica perché il richiedente utilizza il valore predefinito QM3 come nome del gestore code di risposta nel messaggio di richiesta inviato da QM3. Il server su QM2 utilizza il QM3 nome del gestore code reply - to QM3 nelle sue risposte. La soluzione richiedeva QM1 per pubblicizzare QM3 come alias del gestore code a cui restituire i messaggi di risposta e impediva a QM1 di utilizzare QM3 come nome della coda di trasmissione.

   Invece di fornire per impostazione predefinita QM3 come nome del gestore code di risposta, le applicazioni su QM3 devono passare un alias del gestore code di risposta a QM1 per i messaggi di risposta. Il gestore code del gateway QM1 pubblicizza l'alias del gestore code per le risposte a QM3 piuttosto che QM3 , evitando il conflitto con il nome della coda di trasmissione.

   c) Definire un alias del gestore code per QM3 su QM1.

   ```
   DEFINE QREMOTE(QM3.ALIAS) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO)
   ```

   Sono richieste due modifiche ai comandi di configurazione.

   i) QREMOTE at QM1 ora annuncia il nostro alias del gestore code QM3.ALIAS al resto del cluster, accoppiandolo al nome del gestore code reale QM3. QM3 è nuovamente il nome della coda di trasmissione a cui inviare le code di risposte QM3

   ii) L'applicazione client deve fornire QM3.ALIAS come nome del gestore code di risposta quando crea il messaggio di richiesta. È possibile fornire QM3.ALIAS all'applicazione client in uno dei seguenti due modi.

- Codice QM3.ALIAS nel campo del nome del gestore code di risposta creato da MQPUT in MQMD. È necessario farlo in questo modo se si utilizza una coda dinamica per le risposte.
- Utilizzare un alias della coda di risposta, Q3.ALIAS, piuttosto che una coda di risposta quando si fornisce il nome della coda di risposta.

```
DEFINE QREMOTE(Q3.ALIAS) RNAME(Q3) RQMNAME(QM3.ALIAS)
```

Operazioni successive

Nota: Non è possibile dimostrare l'utilizzo di alias della coda di risposta con **AMQSREQ0**. Apre la coda di risposta utilizzando il nome della coda fornito nel parametro 3 o la coda modello SYSTEM.SAMPLE.REPLY predefinita. È necessario modificare l'esempio fornendo un altro parametro contenente l'alias della coda di risposta per denominare l'alias del gestore code di risposta per MQPUT.

Attività correlate

“Nascondere il nome di un gestore code di destinazione cluster” a pagina 256
Instradare un messaggio a una coda cluster definita su qualsiasi gestore code in un cluster senza denominare il gestore code.

Nascondere il nome di un gestore code di destinazione cluster

Instradare un messaggio a una coda cluster definita su qualsiasi gestore code in un cluster senza denominare il gestore code.

Prima di iniziare

- Evitare di rivelare i nomi dei gestori code interni al cluster ai gestori code esterni al cluster.
  - La risoluzione dei riferimenti al gestore code che ospita una coda all'interno del cluster rimuove la flessibilità per eseguire il bilanciamento del carico di lavoro.
  - Inoltre, rende difficile modificare un gestore code che ospita una coda nel cluster.
  - L'alternativa consiste nel sostituire RQMNAME con un alias del gestore code fornito dall'amministratore del cluster.
  - “Nascondere il nome di un gestore code di destinazione cluster” a pagina 256 descrive l'utilizzo di un alias del gestore code per separare un gestore code esterno a un cluster dalla gestione dei gestori code all'interno di un cluster.
- Tuttavia, il modo consigliato per denominare le code di trasmissione consiste nel fornire loro il nome del gestore code di destinazione. Il nome della coda di trasmissione rivela il nome di un gestore code nel cluster. Devi scegliere quale regola seguire. È possibile scegliere di denominare la coda di trasmissione utilizzando il nome del gestore code o il nome del cluster:

  Denominare la coda di trasmissione utilizzando il nome del gestore code del gateway
  La divulgazione del nome del gestore code del gateway ai gestori code all'esterno di un cluster è un'eccezione ragionevole alla regola di nascondere i nomi dei gestori code del cluster.

  Denominare la coda di trasmissione utilizzando il nome del cluster
  Se non si sta seguendo la convenzione di denominazione delle code di trasmissione con il nome del gestore code di destinazione, utilizzare il nome cluster.

Informazioni su questa attività

Modificare l'attività “Configurazione della richiesta/risposta a un cluster” a pagina 253, per nascondere il nome del gestore code di destinazione all'interno del cluster.

Procedura

Nell'esempio, consultare Figura 44 a pagina 257 , definire un alias del gestore code sul gestore code del gateway QM1 denominato DEMO:

```
DEFINE QREMOTE(DEMO) RNAME(' ') RQMNAME(' ')
```

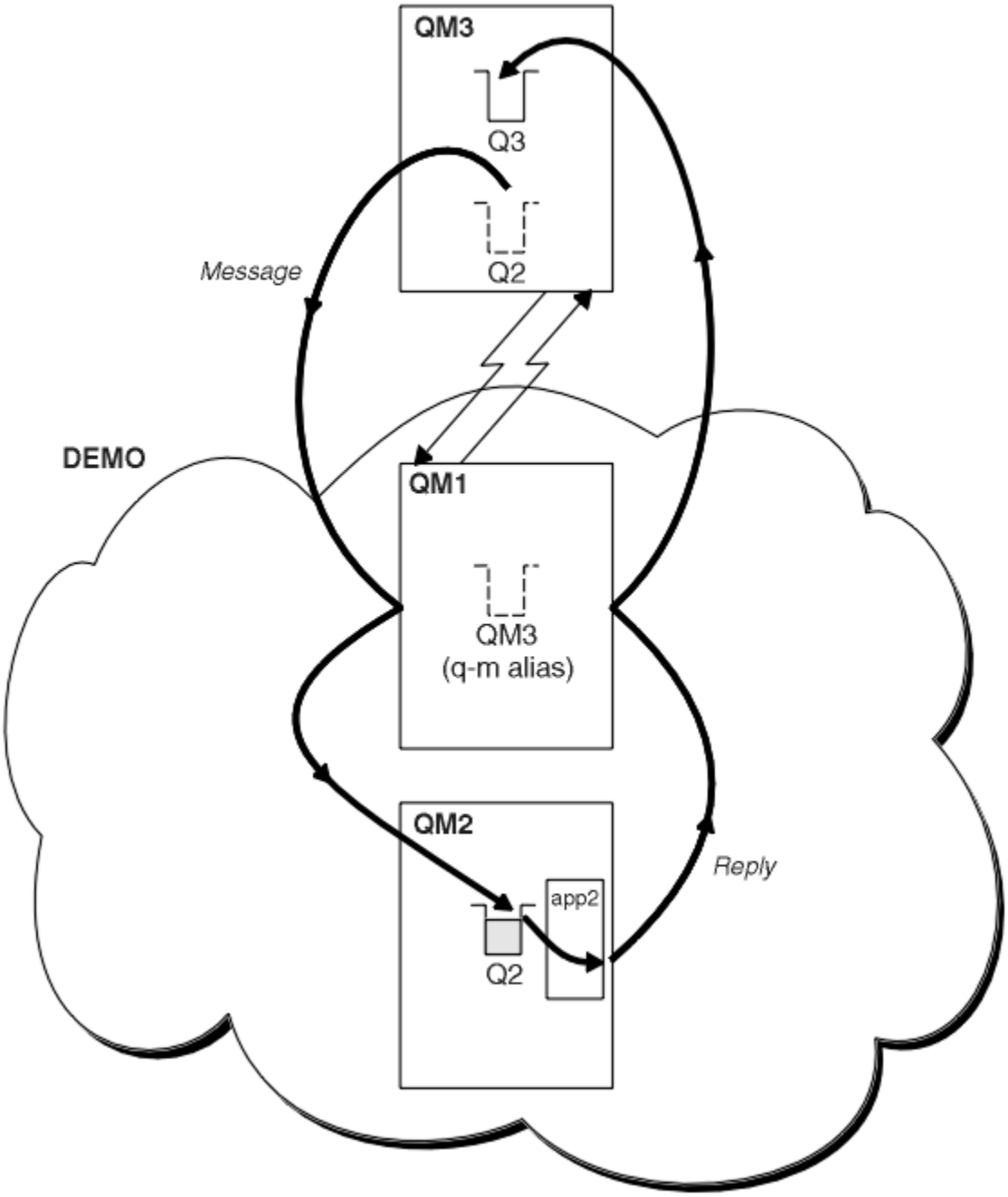


Figura 44. Inserimento da un gestore code esterno al cluster

La definizione QREMOTE su QM1 rende l'alias del gestore code DEMO noto al gestore code gateway. QM3, il gestore code esterno al cluster, può utilizzare l'alias del gestore code DEMO per inviare messaggi alle code del cluster su DEMO, invece di dover utilizzare un nome gestore code effettivo.

Se si adotta la convenzione di utilizzare il nome del cluster per denominare la coda di trasmissione che si connette a un cluster, la definizione della coda remota per Q2 diventa:

```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(DEMO)
```

Risultati

I messaggi destinati a Q2 su DEMO vengono inseriti nella coda di trasmissione DEMO . Dalla coda di trasmissione vengono trasferiti dal canale mittente al gestore code del gateway, QM1. Il gestore code del gateway instrada i messaggi a qualsiasi gestore code nel cluster che ospita la coda del cluster Q2.

Configurazione della richiesta/risposta da un cluster

Configurare un percorso del messaggio di richiesta / risposta da un cluster a un gestore code esterno al cluster. Nascondere i dettagli su come un gestore code all'interno del cluster comunica all'esterno del cluster utilizzando un gestore code gateway.

Prima di iniziare

Figura 45 a pagina 259 mostra un gestore code, QM2, all'interno del cluster DEMO. Invia una richiesta a una coda, Q3, che si trova sul gestore code esterno al cluster. Le risposte vengono restituite a Q2 in QM2 all'interno del cluster.

Per comunicare con il gestore code esterno al cluster, uno o più gestori code all'interno del cluster fungono da gateway. Un gestore code gateway dispone di un percorso di comunicazione per i gestori code esterni al cluster. Nell'esempio, QM1 è il gateway.

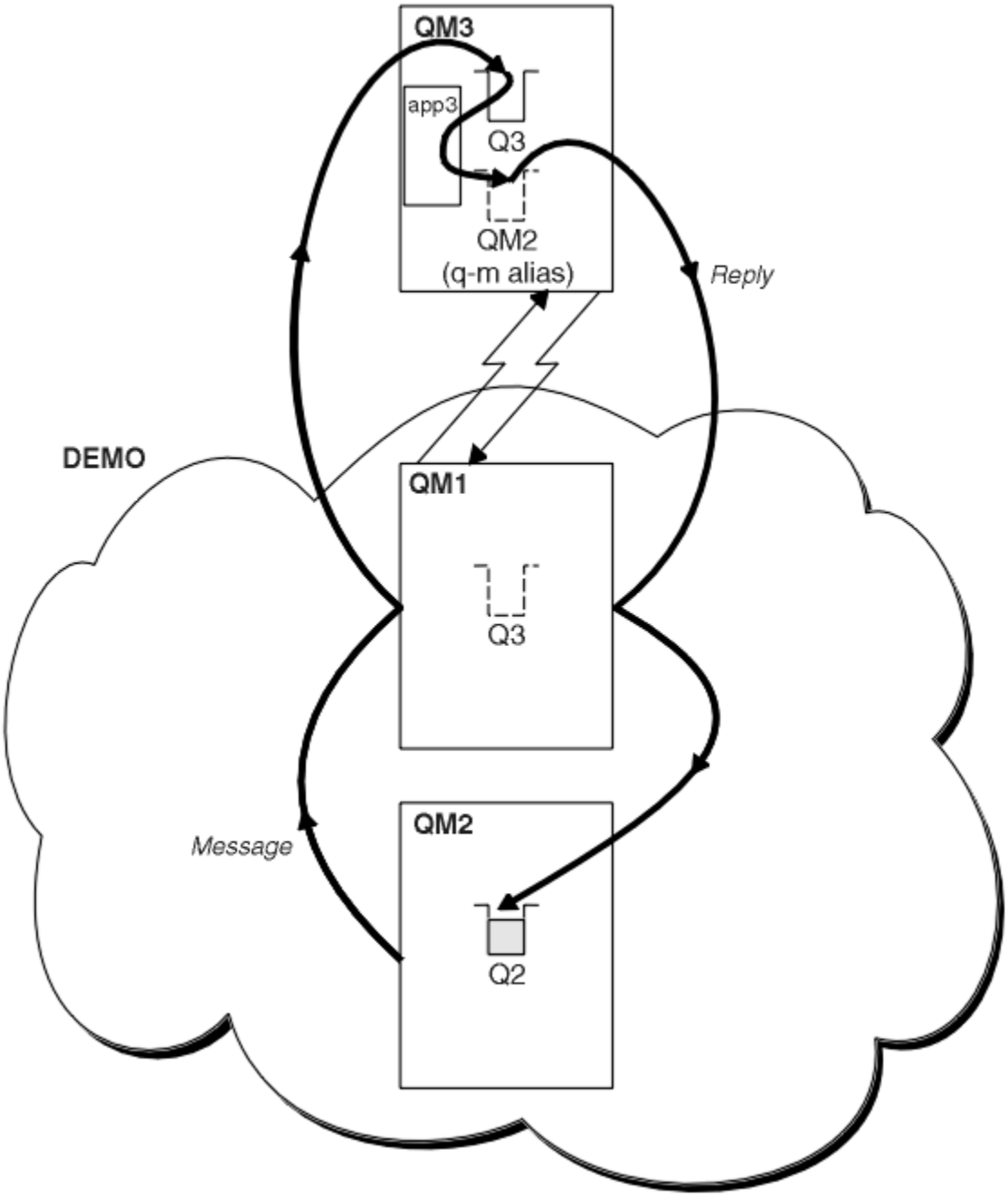


Figura 45. Inserimento in un gestore code all'esterno del cluster

Informazioni su questa attività

Seguire le istruzioni per impostare il percorso per i messaggi di richiesta e risposta

Procedura

1. Invia il messaggio di richiesta dal cluster.

   Considerare il modo in cui il gestore code, QM2, che si trova nel cluster inserisce un messaggio nella coda Q3 in QM3, che si trova all'esterno del cluster.

   a) Creare una definizione QREMOTE su QM1 che annunci la coda remota Q3 al cluster

   ```
   DEFINE QREMOTE(Q3) RNAME(Q3) RQMNAME(QM3) CLUSTER(DEMO)
   ```

Dispone inoltre di un canale mittente e di una coda di trasmissione al gestore code esterno al cluster. QM3 ha un canale ricevente corrispondente. I canali non vengono visualizzati in Figura 45 a pagina 259.

Un'applicazione su QM2 emette una chiamata MQPUT che specifica la coda di destinazione e la coda a cui devono essere inviate le risposte. La coda di destinazione è Q3 e la coda di risposta è Q2.

Il messaggio viene inviato a QM1, che utilizza la definizione della coda remota per risolvere il nome della coda in Q3 at QM3.

2. Ricevere il messaggio di risposta dal gestore code esterno al cluster.

   Un gestore code all'esterno del cluster deve avere un alias del gestore code per ogni gestore code nel cluster a cui invia un messaggio. L'alias del gestore code deve specificare anche il nome della coda di trasmissione al gestore code del gateway. In questo esempio, QM3 ha bisogno di una definizione alias del gestore code per QM2:

   a) Creare un alias del gestore code QM2 su QM3

   ```
   DEFINE QREMOTE(QM2) RNAME(' ') RQMNAME(QM2) XMITQ(QM1)
   ```

   QM3 ha anche bisogno di un canale mittente e di una coda di trasmissione per QM1 e QM1 ha bisogno di un canale ricevente corrispondente.

   L'applicazione, **app3**, su QM3 può quindi inviare risposte a QM2, emettendo una chiamata MQPUT e specificando il nome della coda, Q2 e il nome del gestore code, QM2.

Operazioni successive

È possibile definire più di un instradamento da un cluster.

Configurazione del bilanciamento del workload dall'esterno di un cluster

Configurare un percorso del messaggio da un gestore code esterno a un cluster a qualsiasi copia di una coda cluster. Il risultato è di bilanciare il carico di lavoro delle richieste dall'esterno del cluster a ciascuna istanza di una coda cluster.

Prima di iniziare

Configurare l'esempio, come mostrato in Figura 43 a pagina 254 in “Configurazione della richiesta/risposta a un cluster” a pagina 253.

Informazioni su questa attività

In questo scenario, il gestore code esterno al cluster, QM3 in Figura 46 a pagina 261, invia le richieste alla coda Q2. Q2 è ospitato su due gestori code all'interno del cluster DEMO per utilizzare il bilanciamento del workload. Una coda denominata Q2 è definita sul gestore code QM2 e QM4 ma non sul gestore code del gateway QM1. Le richieste provenienti da QM3, il gestore code esterno al cluster, vengono inviate all'istanza di Q2.

QM3 non fa parte di un cluster e comunica utilizzando tecniche di accodamento distribuite. Deve avere un canale mittente e una coda di trasmissione per QM1. QM1 necessita di un canale ricevente corrispondente. I canali e le code di trasmissione non vengono visualizzati esplicitamente in Figura 46 a pagina 261.

La procedura estende l'esempio in Figura 43 a pagina 254 in “Configurazione della richiesta/risposta a un cluster” a pagina 253.

Procedura

1. Definire una coda locale denominata Q2 su ciascuno di QM2 e QM4.

   ```
   DEFINE QLOCAL(Q2) CLUSTER(DEMO) DEFBIND(NOTFIXED)
   ```

2. Creare una definizione QREMOTE per Q2 su QM3.

```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(Q3) XMITQ(QM1)
```

Creare una definizione QREMOTE per ogni coda nel cluster in cui QM3 inserisce i messaggi.

3. Creare un alias del gestore code Q3 su QM3.

```
DEFINE QREMOTE(Q3) RNAME(' ') RQMNAME(' ') CLUSTER(DEMO) DEFBIND(NOTFIXED)
```

Q3 non è un nome gestore code reale. È il nome di una definizione alias del gestore code nel cluster che equipara il nome alias del gestore code Q3 con vuoto, ' '

4. QM1, il gestore code del gateway, non ha definizioni speciali.

Risultati

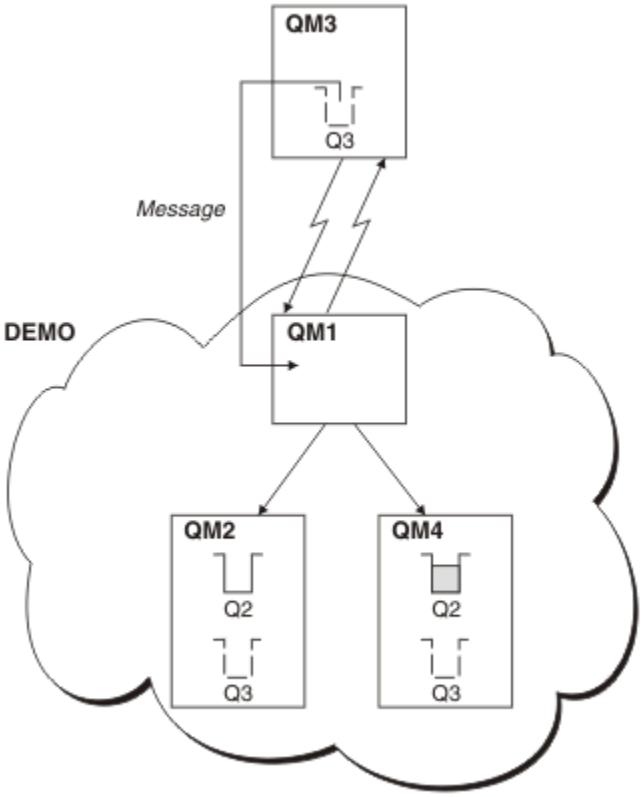


Figura 46. Inserimento da un gestore code esterno al cluster

Quando un'applicazione su QM3 emette una chiamata MQPUT per inserire un messaggio in Q2, la definizione QREMOTE fa in modo che il messaggio venga instradato attraverso il gestore code gateway QM1. QM1 utilizza il bilanciamento del carico di lavoro per distribuire i messaggi destinati a Q2 tra le code denominate Q2 sui due gestori code, QM2 e QM4, che hanno alias del gestore code del cluster per Q3.

Configurazione dei percorsi dei messaggi tra cluster

Connettere i cluster utilizzando un gestore code gateway. Rendere le code o i gestori code visibili a tutti i cluster definendo gli alias della coda del cluster o del gestore code del cluster sul gestore code del gateway.

Informazioni su questa attività

Invece di raggruppare tutti i tuoi gestori code in un unico cluster di grandi dimensioni, puoi avere molti cluster più piccoli. Ogni cluster ha uno o più gestori code che fungono da bridge. Il vantaggio è che è possibile limitare la visibilità dei nomi di code e gestori code nei cluster. Consultare “Cluster sovrapposti”

a pagina 183. Utilizzare gli alias per modificare i nomi delle code e dei gestori code per evitare conflitti di nomi o per rispettare le convenzioni di denominazione locali.

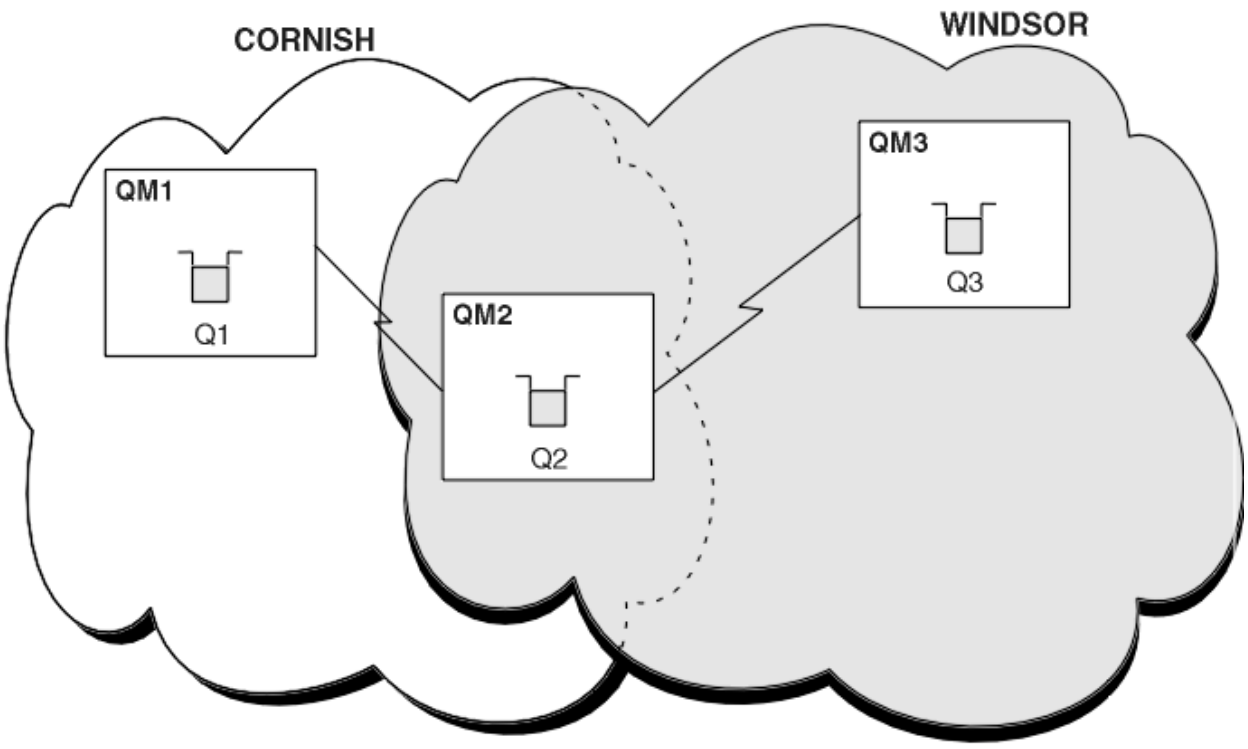


Figura 47. Collegamento tra cluster

Figura 47 a pagina 262 mostra due cluster con un bridge tra loro. Ci potrebbe essere più di un ponte.

Configurare i cluster utilizzando la seguente procedura:

Procedura

1. Definire una coda cluster, Q1 su QM1.

```
DEFINE QLOCAL(Q1) CLUSTER(CORNISH)
```

2. Definire una coda cluster, Q3 su QM3.

```
DEFINE QLOCAL(Q3) CLUSTER(WINDSOR)
```

3. Creare un elenco nomi denominato CORNISHWINDSOR su QM2, contenente i nomi di entrambi i cluster.

```
DEFINE NAMELIST(CORNISHWINDSOR) DESCR('CornishWindsor namelist')
       NAMES(CORNISH, WINDSOR)
```

4. Definire una coda cluster, Q2 su QM2

```
DEFINE QLOCAL(Q2) CLUSNL(CORNISHWINDSOR)
```

Operazioni successive

QM2 è un membro di entrambi i cluster ed è il ponte tra loro. Per ogni coda che si desidera rendere visibile attraverso il bridge, è necessaria una definizione QALIAS sul bridge. Ad esempio, in Figura 47 a pagina 262, su QM2, è necessario:

```
DEFINE QALIAS(MYQ3) TARGET(Q3) CLUSTER(CORNISH) DEFBIND(NOTFIXED)
```

Utilizzando l'alias della coda, un'applicazione connessa a un gestore code in CORNISH, ad esempio QM1, può inserire un messaggio in Q3. Si riferisce a Q3 come MYQ3. Il messaggio viene instradato a Q3 in QM3.

Quando si apre una coda, è necessario impostare DEFBIND su NOTFIXED o QDEF. Se DEFBIND viene lasciato come valore predefinito, OPEN, il gestore code risolve la definizione dell'alias nel gestore code del bridge che lo ospita. Il bridge non inoltra il messaggio.

Per ogni gestore code che si desidera rendere visibile, è necessaria una definizione di alias del gestore code. Ad esempio, su QM2 è necessario:

```
DEFINE QREMOTE(QM1) RNAME(' ') RQMNAME(QM1) CLUSTER(WINDSOR)
```

Un'applicazione connessa a qualsiasi gestore code in WINDSOR, ad esempio QM3, può inserire un messaggio in qualsiasi coda su QM1, denominando esplicitamente QM1 nella chiamata MQOPEN .

Cluster e alias del gestore code

Utilizzare gli alias del gestore code per nascondere il nome dei gestori code quando si inviano messaggi all'interno o all'esterno di un cluster e per bilanciare il carico di lavoro dei messaggi inviati a un cluster.

Gli alias del gestore code, creati utilizzando una definizione di coda remota con un RNAMEvuoto, hanno cinque utilizzi:

Riassociazione del nome del gestore code durante l'invio di messaggi

Un alias del gestore code può essere utilizzato per riassociare il nome del gestore code specificato in una chiamata MQOPEN ad un altro gestore code. Può essere un gestore code cluster. Ad esempio, un gestore code potrebbe avere la definizione di alias del gestore code:

```
DEFINE QREMOTE(YORK) RNAME(' ') RQMNAME(CLUSQM)
```

YORK può essere utilizzato come un alias per il gestore code denominato CLUSQM. Quando un'applicazione sul gestore code che ha creato questa definizione inserisce un messaggio nel gestore code YORK, il gestore code locale risolve il nome in CLUSQM. Se il gestore code locale non è denominato CLUSQM, inserisce il messaggio nella coda di trasmissione del cluster da spostare in CLUSQM. Inoltre, modifica l'intestazione di trasmissione per dire CLUSQM invece che YORK.

Nota: La definizione viene applicata solo al gestore code che la crea. Per indicare l'alias all'intero cluster, è necessario aggiungere l'attributo CLUSTER alla definizione della coda remota. Quindi, i messaggi provenienti da altri gestori code destinati a YORK vengono inviati a CLUSQM .

Modifica o specifica della coda di trasmissione durante l'invio di messaggi

L'aliasing può essere utilizzato per unire un cluster a un sistema non cluster. Ad esempio, i gestori code nel cluster ITALY potrebbero comunicare con il gestore code denominato PALERMO , esterno al cluster. Per comunicare, uno dei gestori code nel cluster deve agire come gateway. Dal gestore code del gateway, immettere il comando:

```
DEFINE QREMOTE(ROME) RNAME(' ') RQMNAME(PALERMO) XMITQ(X) CLUSTER(ITALY)
```

Il comando è una definizione di alias del gestore code. Definisce e pubblicizza ROME come un gestore code su cui i messaggi provenienti da qualsiasi gestore code nel cluster ITALY possono multi - hop per raggiungere la loro destinazione in PALERMO. I messaggi inseriti in una coda aperta con il nome gestore code impostato su ROME vengono inviati al gestore code del gateway con la definizione di alias del gestore code. Una volta lì, i messaggi vengono inseriti sulla coda di trasmissione X e spostati dai canali non cluster al gestore code PALERMO .

La scelta del nome ROME in questo esempio non è significativa. I valori per QREMOTE e RQMNAME potrebbero coincidere.

Determinazione della destinazione durante la ricezione dei messaggi

Quando un gestore code riceve un messaggio, estrae il nome della coda di destinazione e il gestore code dall'intestazione di trasmissione. Ricerca una definizione alias del gestore code con lo stesso

nome del gestore code nell'intestazione di trasmissione. se ne trova uno, sostituisce il RQMNAME dalla definizione alias del gestore code per il nome del gestore code nell'intestazione di trasmissione.

Esistono due ragioni per utilizzare un alias del gestore code in questo modo:

- Per indirizzare i messaggi ad un altro gestore code
- Per modificare il nome del gestore code in modo che sia uguale al gestore code locale

Utilizzo degli alias del gestore code in un gestore code gateway per instradare i messaggi tra i gestori code in cluster differenti.

Un'applicazione può inviare un messaggio a una coda in un cluster differente utilizzando un alias del gestore code. La coda non deve essere una coda cluster. La coda è definita in un cluster. L'applicazione è connessa a un gestore code in un cluster differente. Un gestore code del gateway connette i due cluster. Se la coda non è definita come in cluster, per eseguire l'instradamento corretto, l'applicazione deve aprire la coda utilizzando il nome della coda e un nome alias del gestore code in cluster. Per un esempio di configurazione, vedere “Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221, da cui viene preso il flusso di messaggi di replica illustrato nella figura 1.

Il diagramma mostra il percorso utilizzato dal messaggio di risposta per tornare a una coda dinamica temporanea, denominata RQ. L'applicazione server, connessa a QM3, apre la coda di risposta utilizzando il nome del gestore code QM2. Il nome del gestore code QM2 è definito come alias del gestore code in cluster su QM1. QM3 instrada il messaggio di risposta a QM1. QM1 instrada il messaggio a QM2.

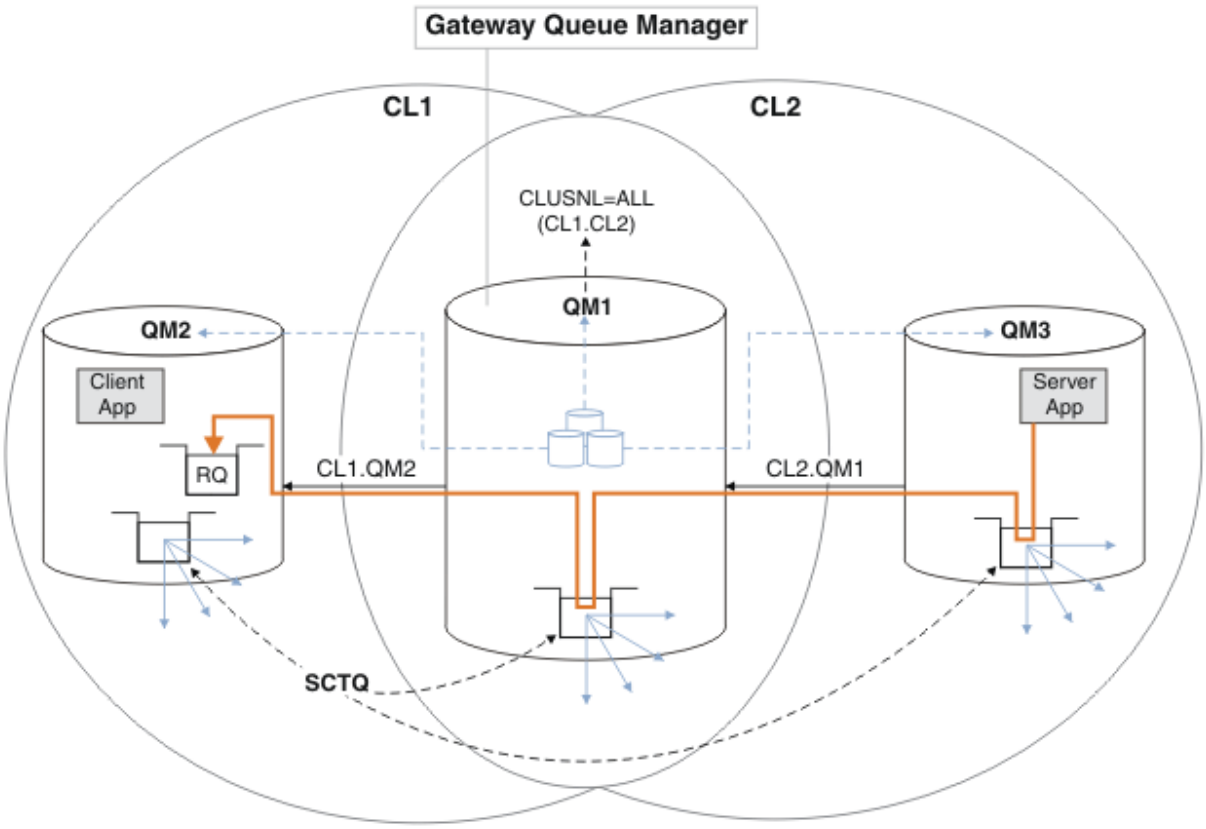


Figura 48. Utilizzo di un alias del gestore code per restituire il messaggio di risposta a un cluster differente

Il modo in cui funziona l'instradamento è il seguente. Ogni gestore code in ogni cluster ha una definizione di alias del gestore code su QM1. Gli alias sono raggruppati in tutti i cluster. Le frecce tratteggiate grigie da ciascuno degli alias a un gestore code mostrano che ogni alias del gestore code viene risolto in un gestore code reale in almeno uno di questi cluster. In questo caso, l'alias QM2 è raggruppato in cluster CL1 e CL2e viene risolto nel gestore code reale QM2 in CL1. L'applicazione

server crea il messaggio di risposta utilizzando il nome della coda di risposta RQe il nome del gestore code di risposta QM2. Il messaggio viene instradato a QM1 perché la definizione alias del gestore code QM2 è definita su QM1 nel cluster CL2 e il gestore code QM2 non è nel cluster CL2. Poiché il messaggio non può essere inviato al gestore code di destinazione, viene inviato al gestore code che ha la definizione alias.

QM1 colloca il messaggio nella coda di trasmissione del cluster su QM1 per il trasferimento a QM2. QM1 instrada il messaggio a QM2 perché la definizione dell'alias del gestore code su QM1 per QM2 definisce QM2 come il gestore code di destinazione reale. La definizione non è circolare, poiché le definizioni alias possono fare riferimento solo a definizioni reali; l'alias non può puntare a se stesso. La definizione reale viene risolta da QM1, perché sia QM1 che QM2 si trovano nello stesso cluster, CL1. QM1 rileva le informazioni di collegamento per QM2 dal contenitore per CL1e instrada il messaggio a QM2. Perché il messaggio venga reinstradato da QM1, l'applicazione server deve aver aperto la coda di risposta con l'opzione DEFBIND impostata su MQBND_BIND_NOT_FIXED. Se l'applicazione server ha aperto la coda di risposta con l'opzione MQBND_BIND_ON_OPEN, il messaggio non viene reinstradato e finisce su una coda di messaggi non recapitabili.

Utilizzo di un gestore code come gateway nel cluster per bilanciare il carico di lavoro dei messaggi provenienti dall'esterno del cluster.

Definire una coda denominata EDINBURGH su più di un gestore code nel cluster. Si desidera che il meccanismo di cluster bilancii il carico di lavoro per i messaggi che arrivano a tale coda dall'esterno del cluster.

Un gestore code esterno al cluster richiede una coda di trasmissione e un canale mittente per un gestore code nel cluster. Questa coda è denominata gestore code gateway. Per sfruttare il meccanismo di bilanciamento del workload predefinito, è necessario applicare una delle seguenti regole:

- Il gestore code del gateway non deve contenere un'istanza della coda EDINBURGH .
- Il gestore code del gateway specifica CLWLUSEQ(ANY) su ALTER QMGR.

Per un esempio di bilanciamento del carico di lavoro esterno a un cluster, consultare “Configurazione del bilanciamento del workload dall'esterno di un cluster” a pagina 260

Cluster e alias della coda di risposta

Una definizione alias coda di risposta viene utilizzata per specificare nomi alternativi per le informazioni di risposta. Le definizioni di alias della coda di risposta possono essere utilizzate con i cluster esattamente come in un ambiente di accodamento distribuito.

Ad esempio:

- Un'applicazione al gestore code VENICE invia un messaggio al gestore code PISA utilizzando la chiamata MQPUT . L'applicazione fornisce le seguenti informazioni sulla coda di risposta nel descrittore del messaggio:

```
ReplyToQ='QUEUE'
ReplyToQMgr=''
```

- Affinché le risposte inviate a QUEUE possano essere ricevute su OTHERQ alle PISA, creare una definizione di coda remota su VENICE utilizzata come alias della coda di risposta. L'alias è valido solo sul sistema su cui è stato creato.

```
DEFINE QREMOTE(QUEUE) RNAME(OTHERQ) RQMNAME(PISA)
```

RQMNAME e QREMOTE possono specificare gli stessi nomi, anche se RQMNAME è un gestore code del cluster.

Alias coda e cluster

Utilizzare gli alias della coda per nascondere il nome di una coda cluster, per raggruppare una coda, per adottare attributi differenti o per adottare controlli accessi differenti.

Una definizione QALIAS viene utilizzata per creare un alias mediante il quale una coda deve essere riconosciuta. È possibile creare un alias per una serie di ragioni:

- Si desidera iniziare a utilizzare una coda diversa ma non si desidera modificare le applicazioni.
- Non si desidera che le applicazioni conoscano il nome reale della coda in cui stanno inserendo i messaggi.
- È possibile che si disponga di una convenzione di denominazione diversa da quella in cui è definita la coda.
- Le applicazioni potrebbero non essere autorizzate ad accedere alla coda in base al suo nome reale, ma solo in base all'alias.

Creare una definizione QALIAS su un gestore code utilizzando il comando DEFINE QALIAS . Ad esempio, eseguire il comando:

```
DEFINE QALIAS(PUBLIC) TARGET(LOCAL) CLUSTER(C)
```

Il comando annuncia una coda denominata PUBLIC ai gestori code nel cluster C. PUBLIC è un alias che si risolve nella coda denominata LOCAL. I messaggi inviati a PUBLIC vengono instradati alla coda denominata LOCAL.

È anche possibile utilizzare una definizione alias della coda per risolvere un nome coda in una coda cluster. Ad esempio, eseguire il comando:

```
DEFINE QALIAS(PRIVATE) TARGET(PUBLIC)
```

Il comando consente a un gestore code di utilizzare il nome PRIVATE per accedere a una coda pubblicizzata altrove nel cluster dal nome PUBLIC. Poiché questa definizione non include l'attributo CLUSTER , viene applicata solo al gestore code che la crea.

Utilizzo dei cluster per la gestione del carico di lavoro

Definendo più istanze di una coda su gestori code differenti in un cluster, è possibile distribuire il lavoro di gestione della coda su più server. Esistono diversi fattori che possono impedire la riaccodamento dei messaggi a un gestore code differente in caso di errore.

Oltre a configurare i cluster per ridurre l'amministrazione del sistema, è possibile creare cluster in cui più di un gestore code ospita un'istanza della stessa coda.

È possibile organizzare il cluster in modo che i gestori code al suo interno siano cloni l'uno dell'altro. Ogni gestore code è in grado di eseguire le stesse applicazioni e dispone di definizioni locali delle stesse code. È possibile distribuire il carico di lavoro tra i gestori code disponendo di diverse istanze di un'applicazione. Ogni istanza dell'applicazione riceve messaggi e viene eseguita indipendentemente l'una dall'altra.

I vantaggi di utilizzare i cluster in questo modo sono:

- Maggiore disponibilità di code e applicazioni
- Maggiore velocità di trasmissione dei messaggi
- Distribuzione più uniforme del carico di lavoro nella rete

Qualsiasi gestore code che ospita un'istanza di una particolare coda può gestire i messaggi destinati a tale coda. Le applicazioni non denominano un gestore code quando inviano messaggi. Un algoritmo di gestione del carico di lavoro determina quale gestore code gestisce il messaggio.

Consultare i seguenti argomenti secondari per ulteriori informazioni sulle configurazioni cluster per la gestione del carico di lavoro:

Concetti correlati

Cluster

Funzionamento dei cluster

“Confronto tra cluster e accodamento distribuito” a pagina 164

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

“Componenti di un cluster” a pagina 166
I cluster sono composti da gestore code, repository di cluster, canali cluster e code cluster.

“Gestione dei cluster IBM WebSphere MQ” a pagina 188
È possibile creare, estendere e gestire cluster IBM WebSphere MQ .

“Instradamento dei messaggi verso e dai cluster” a pagina 252
Utilizzare gli alias di coda, gli alias di gestore code e le definizioni di code remote per connettere i cluster a gestori code esterni e altri cluster.

Attività correlate

“Configurazione di un cluster di gestore code” a pagina 161
Utilizzare i link in questo argomento per scoprire come funzionano i cluster, come progettare una configurazione cluster e per ottenere un esempio di come impostare un cluster semplice.

“Configurazione di un nuovo cluster” a pagina 188
Seguire queste istruzioni per configurare il cluster di esempio. Istruzioni separate descrivono l'impostazione del cluster su TCP/IP, LU 6.2e con una o più code di trasmissione. Verificare il funzionamento del cluster inviando un messaggio da un gestore code all'altro.

Scrittura e compilazione delle uscite del carico di lavoro del cluster

Esempio di un cluster con più di un'istanza di una coda

In questo esempio di cluster con più di un'istanza di una coda, i messaggi vengono instradati a istanze differenti della coda. È possibile forzare un messaggio a una specifica istanza della coda ed è possibile scegliere di inviare una sequenza di messaggi a uno dei gestori code.

Figura 49 a pagina 268 mostra un cluster in cui è presente più di una definizione per la coda Q3.
Se un'applicazione in QM1 inserisce un messaggio in Q3, non necessariamente sa quale istanza di Q3 elaborerà il suo messaggio. Se un'applicazione è in esecuzione su QM2 o QM4, in cui sono presenti istanze locali di Q3, l'istanza locale di Q3 viene aperta per impostazione predefinita. Impostando l'attributo della coda CLWLUSEQ , l'istanza locale della coda può essere trattata come un'istanza remota della coda.

L'opzione MQOPEN DefBind controlla se il gestore code di destinazione viene scelto quando viene emessa la chiamata MQOPEN o quando il messaggio viene trasferito dalla coda di trasmissione.

Se si imposta DefBind su MQBND_BIND_NOT_FIXED , il messaggio può essere inviato a un'istanza della coda disponibile quando il messaggio viene trasmesso. Ciò evita i seguenti problemi:

- La coda di destinazione non è disponibile quando il messaggio arriva al gestore code di destinazione.
- Lo stato della coda è cambiato.
- Il messaggio è stato inserito utilizzando un alias della coda cluster e non esiste alcuna istanza della coda di destinazione sul gestore code in cui è definita l'istanza dell'alias della coda cluster.

Se questi problemi vengono rilevati al momento della trasmissione, viene ricercata un'altra istanza disponibile della coda di destinazione e il messaggio viene reinstradato. Se non sono disponibili istanze della coda, il messaggio viene inserito nella coda di messaggi non recapitabili.

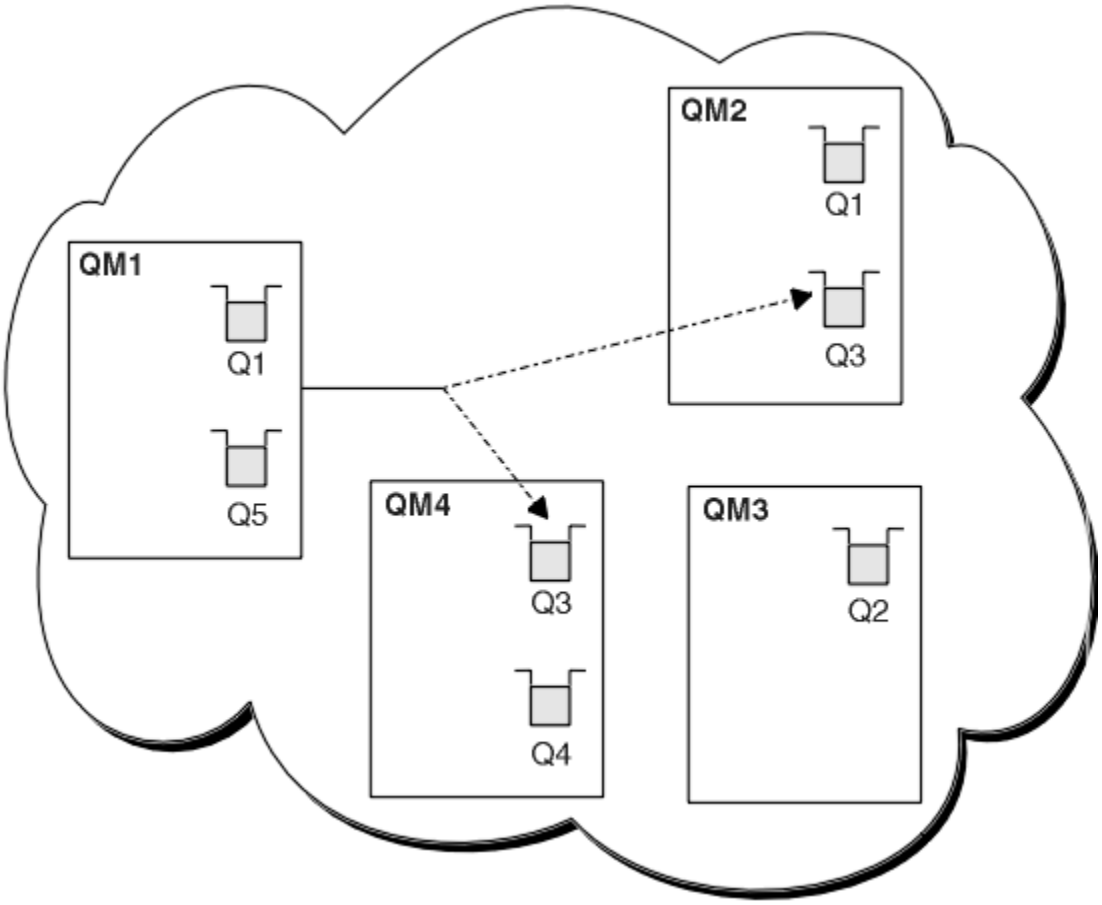


Figura 49. Un cluster con più istanze della stessa coda

Un fattore che può impedire il reinstradamento dei messaggi è se i messaggi sono stati assegnati a un canale o a un gestore code fisso con MQBND_BIND_ON_OPEN. I messaggi collegati su MQOPEN non vengono mai riassegnati ad un altro canale. Si noti inoltre che la riallocazione del messaggio avviene solo quando un canale cluster è in errore. La riassegnazione non si verifica se il canale ha già avuto esito negativo.

Il sistema tenta di reinstradare un messaggio se il gestore code di destinazione non è più in servizio. In questo modo, non influisce sull'integrità del messaggio, correndo il rischio di perderlo o creando un duplicato. Se un gestore code ha esito negativo e lascia un messaggio in dubbio, tale messaggio non viene reinstradato.

Aggiunta di un gestore code che ospita una coda localmente

Seguire queste istruzioni per aggiungere un'istanza di INVENTQ per fornire ulteriore capacità per eseguire il sistema dell'applicazione di inventario a Parigi e New York.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in Aggiunta di un nuovo gestore code a un cluster. Contiene tre gestori code; LONDON e NEWYORK contengono entrambi repository completi, PARIS contiene un repository parziale. L'applicazione di inventario viene eseguita sul sistema a New

York, connesso al gestore code NEWYORK . L'applicazione è guidata dall'arrivo di messaggi sulla coda INVENTQ .

- Si desidera aggiungere un'istanza di INVENTQ per fornire ulteriore capacità per eseguire il sistema dell'applicazione di inventario a Parigi e New York.

Informazioni su questa attività

Seguire questa procedura per aggiungere un gestore code che ospita localmente una coda.

Procedura

1. Modificare il gestore code PARIS .

   Affinché l'applicazione a Parigi utilizzi INVENTQ a Parigi e quella a New York, è necessario informare il gestore code. Su PARIS immettere il seguente comando:

   ```
   ALTER QMGR CLWLUSEQ(ANY)
   ```

2. Esaminare l'applicazione inventario per le affinità dei messaggi.

   Prima di procedere, assicurarsi che l'applicazione di inventario non abbia alcuna dipendenza dalla sequenza di elaborazione dei messaggi. Per ulteriori informazioni, consultare “Gestione delle affinità dei messaggi” a pagina 280.

3. Installare l'applicazione inventario sul sistema a Parigi.
4. Definire la coda del cluster INVENTQ.

   La coda INVENTQ già ospitata dal gestore code NEWYORK deve essere ospitata anche da PARIS. Definirlo sul gestore code PARIS nel modo seguente:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

   Ora che sono state completate tutte le definizioni, se non è stato ancora fatto, avviare l'iniziatore di canali su WebSphere MQ per z/OS. Su tutte le piattaforme, avviare un programma listener sul Gestore code PARIS. Il listener ascolta le richieste di rete in entrata e avvia il canale ricevente del cluster quando è necessario.

Risultati

Figura 50 a pagina 270 mostra il cluster impostato da questa attività.

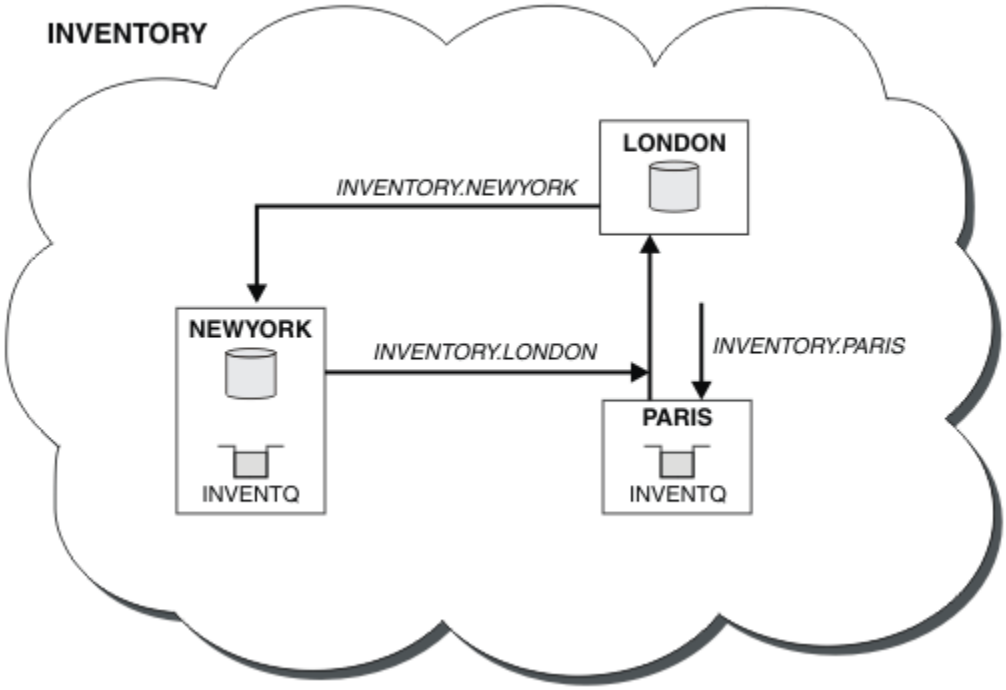


Figura 50. Il cluster INVENTORY , con tre gestori code

La modifica a questo cluster è stata effettuata senza modificare i gestori code NEWYORK o LONDON. I repository completi in questi gestori code vengono aggiornati automaticamente con le informazioni necessarie per inviare messaggi a INVENTQ all'indirizzo PARIS.

Operazioni successive

La coda INVENTQ e l'applicazione di inventario si trovano ora su due gestori code nel cluster. Ciò aumenta la loro disponibilità, velocizza la velocità di trasmissione dei messaggi e consente la distribuzione del carico di lavoro tra i due gestori code. I messaggi immessi in INVENTQ da uno qualsiasi dei gestori code LONDON, NEWYORK, PARIS vengono instradati alternativamente a PARIS o NEWYORK, in modo che il carico di lavoro sia bilanciato.

Utilizzo di due reti in un cluster

Seguire queste istruzioni per aggiungere un nuovo negozio in TOKYO in cui sono presenti due reti differenti. Entrambi devono essere disponibili per comunicare con il gestore code di Tokyo.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in "Aggiunta di un gestore code a un cluster". Contiene tre gestori code; LONDON e NEWYORK contengono entrambi repository completi, PARIS contiene un repository parziale. L'applicazione di inventario viene eseguita sul sistema a New York, connesso al gestore code NEWYORK . L'applicazione è guidata dall'arrivo di messaggi sulla coda INVENTQ .
- È stato aggiunto un nuovo negozio in TOKYO dove sono presenti due reti differenti. Entrambi devono essere disponibili per comunicare con il gestore code di Tokyo.

Informazioni su questa attività

Seguire questa procedura per utilizzare due reti in un cluster.

Procedura

1. Decidere quale repository completo TOKYO fa riferimento per primo.

   Ogni gestore code in un cluster deve fare riferimento a uno o più repository completi per raccogliere informazioni sul cluster. Crea il proprio repository parziale. Non è di particolare importanza quale repository si sceglie. In questo esempio, viene selezionato NEWYORK . Una volta che il nuovo gestore code si è unito al cluster, comunica con entrambi i repository.

2. Definire i canali CLUSRCVR .

   Ogni gestore code in un cluster deve definire un ricevente del cluster su cui può ricevere messaggi. Questo gestore code deve essere in grado di comunicare su ciascuna rete.

   ```
   DEFINE CHANNEL(INVENTORY.TOKYO.NETB) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME('TOKYO.NETB.CMSTORE.COM') CLUSTER(INVENTORY) DESCR('Cluster-receiver
   channel using network B for TOKYO')
   ```

   ```
   DEFINE CHANNEL(INVENTORY.TOKYO.NETA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME('TOKYO.NETA.CMSTORE.COM') CLUSTER(INVENTORY) DESCR('Cluster-receiver
   channel using network A for TOKYO')
   ```

3. Definire un canale CLUSSDR nel gestore code TOKYO.

   Ogni gestore code di un cluster deve definire un canale mittente del cluster su cui può inviare messaggi al primo repository completo. In questo caso è stato scelto NEWYORK, quindi TOKYO ha bisogno della definizione seguente:

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) DESCR('Cluster-sender
   channel from TOKYO to repository at NEWYORK')
   ```

   Ora che sono state completate tutte le definizioni, se non è ancora stato fatto, avviare l'iniziatore di canali su WebSphere MQ per z/OS. Su tutte le piattaforme, avviare un programma listener sul Gestore code PARIS. Il programma listener ascolta le richieste di rete in entrata e avvia il canale ricevente del cluster quando è necessario.

Risultati

Figura 51 a pagina 272 mostra il cluster impostato da questa attività.

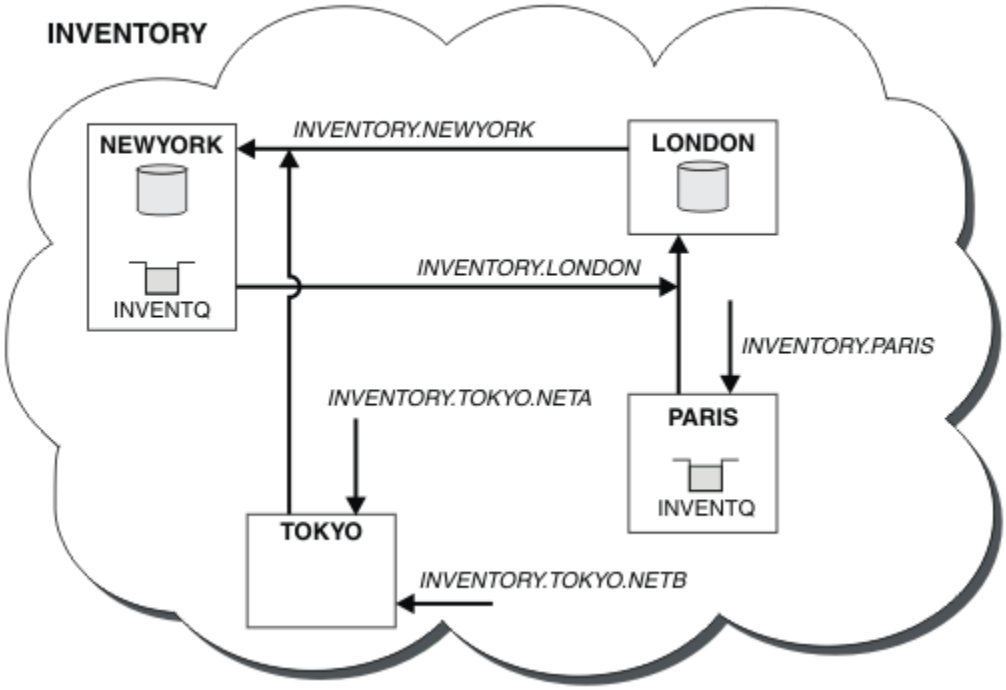


Figura 51. Il cluster INVENTORY , con quattro gestori code

Facendo solo tre definizioni, abbiamo aggiunto il gestore code TOKYO al cluster con due diversi instradamenti di rete disponibili.

Attività correlate

"Aggiunta di un gestore code a un cluster" a pagina 199
Seguire queste istruzioni per aggiungere il gestore code al cluster creato. I messaggi per le code e gli argomenti del cluster vengono trasferiti utilizzando la singola coda di trasmissione del cluster SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Utilizzo di una rete primaria e di una secondaria in un cluster

Seguire queste istruzioni per rendere una rete la rete principale e un'altra la rete di backup. Utilizzare la rete di backup se si verifica un problema con la rete principale.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in "Utilizzo di due reti in un cluster" a pagina 270. Contiene quattro gestori code; LONDON e NEWYORK contengono entrambi repository completi; PARIS e TOKYO conservano repository parziali. L'applicazione di inventario viene eseguita sul sistema a New York, connesso al gestore code NEWYORK. Il gestore code TOKYO ha due reti differenti su cui può comunicare.
- Si desidera rendere una delle reti la rete primaria e un'altra delle reti la rete di backup. Si prevede di utilizzare la rete di backup se si verifica un problema con la rete principale.

Informazioni su questa attività

Utilizzare l'attributo NETPRTY per configurare una rete primaria e una secondaria in un cluster.

Procedura

Modificare i canali CLUSRCVR esistenti su TOKYO.

Per indicare che il canale di rete A è il canale primario e il canale di rete B è il canale secondario, utilizzare i seguenti comandi:

a) `ALTER CHANNEL(INVENTORY.TOKYO.NETA) CHLTYPE(CLUSRCVR) NETPRTY(2) DESCR('Main cluster-receiver channel for TOKYO')`

b) `ALTER CHANNEL(INVENTORY.TOKYO.NETB) CHLTYPE(CLUSRCVR) NETPRTY(1) DESCR('Backup cluster-receiver channel for TOKYO')`

Operazioni successive

Configurando il canale con priorità di rete differenti, hai ora definito per il cluster che hai una rete primaria e una rete secondaria. I gestori code nel cluster che utilizzano questi canali utilizzano automaticamente la rete primaria quando è disponibile. I gestori code eseguono il failover per utilizzare la rete secondaria quando la rete primaria non è disponibile.

Aggiunta di una coda da utilizzare come backup

Seguire queste istruzioni per fornire un backup a Chicago per il sistema di inventario che ora viene eseguito a New York. Il sistema di Chicago è usato solo quando c'è un problema con il sistema di New York.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in “Aggiunta di un gestore code a un cluster” a pagina 199. Contiene tre gestori code; LONDON e NEWYORK contengono entrambi repository completi, PARIS contiene un repository parziale. L'applicazione di inventario viene eseguita sul sistema a New York, connesso al gestore code NEWYORK . L'applicazione è guidata dall'arrivo di messaggi sulla coda INVENTQ .
- Un nuovo negozio è stato creato a Chicago per fornire un backup per il sistema di inventario che ora viene eseguito a New York. Il sistema di Chicago è usato solo quando c'è un problema con il sistema di New York.

Informazioni su questa attività

Effettuare le operazioni riportate di seguito per aggiungere una coda da utilizzare come backup.

Procedura

1. Decidere quale repository completo CHICAGO fa riferimento per primo.

   Ogni gestore code in un cluster deve fare riferimento a uno o più repository completi per raccogliere informazioni sul cluster. Crea il proprio repository parziale. Non è di particolare importanza quale repository si sceglie per un particolare gestore code. In questo esempio, viene selezionato NEWYORK . Una volta che il nuovo gestore code si è unito al cluster, comunica con entrambi i repository.
2. Definire il canale CLUSRCVR .

   Ogni gestore code in un cluster deve definire un ricevente del cluster su cui può ricevere messaggi. Su CHICAGO, definire:

```
DEFINE CHANNEL(INVENTORY.CHICAGO) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(CHICAGO.CMSTORE.COM) CLUSTER(INVENTORY) DESCR('Cluster-receiver
channel for CHICAGO')
```

3. Definire un canale CLUSSDR nel gestore code CHICAGO.

   Ogni gestore code di un cluster deve definire un canale mittente del cluster su cui può inviare messaggi al primo repository completo. In questo caso è stato scelto NEWYORK, quindi CHICAGO ha bisogno della definizione seguente:

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) DESCR('Cluster-sender
   channel from CHICAGO to repository at NEWYORK')
   ```

4. Modificare la coda cluster esistente INVENTQ.

   INVENTQ che è già ospitato dal gestore code NEWYORK è l'istanza principale della coda.

   ```
   ALTER QLOCAL(INVENTQ) CLWLPRTY(2)
   ```

5. Esaminare l'applicazione inventario per le affinità dei messaggi.

   Prima di procedere, assicurarsi che l'applicazione di inventario non abbia alcuna dipendenza dalla sequenza di elaborazione dei messaggi.

6. Installare l'applicazione di inventario sul sistema in CHICAGO.
7. Definire la coda del cluster di backup INVENTQ

   Il INVENTQ che è già ospitato dal gestore code NEWYORK , deve essere ospitato anche come backup da CHICAGO. Definirlo sul gestore code CHICAGO nel modo seguente:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY) CLWLPRTY(1)
   ```

   Ora che sono state completate tutte le definizioni, se non è ancora stato fatto, avviare l'iniziatore di canali su WebSphere MQ per z/OS. Su tutte le piattaforme, avviare un programma listener sul Gestore code CHICAGO. Il programma listener ascolta le richieste di rete in entrata e avvia il canale ricevente del cluster quando è necessario.

Risultati

Figura 52 a pagina 275 mostra il cluster impostato da questa attività.

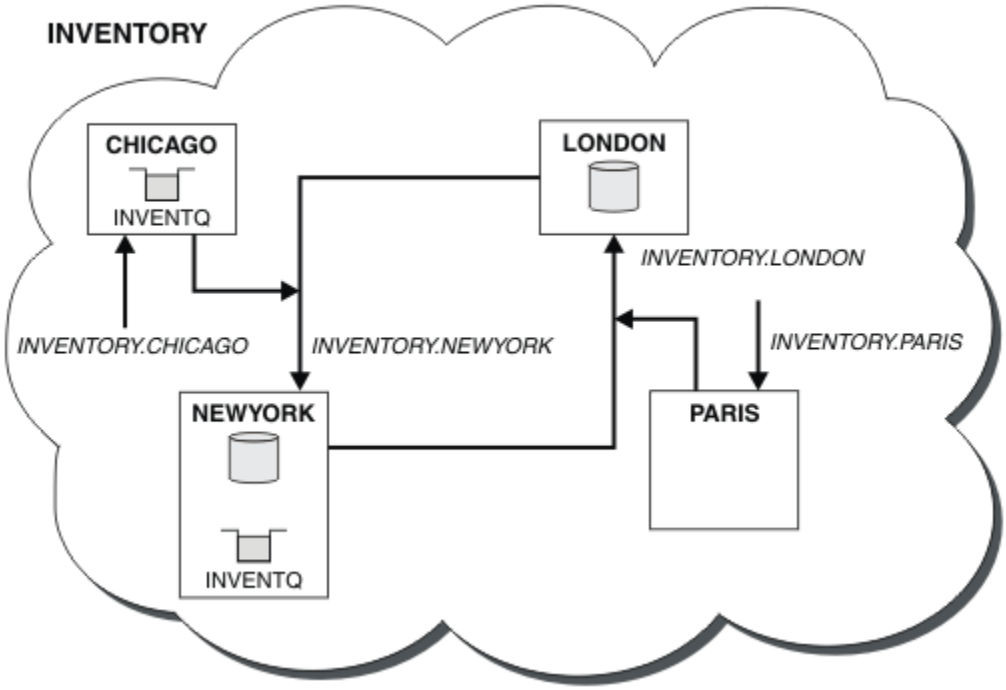


Figura 52. Il cluster INVENTORY, con quattro gestori code

La coda INVENTQ e l'applicazione di inventario si trovano ora su due gestori code nel cluster. Il gestore code CHICAGO è un backup. I messaggi immessi in INVENTQ vengono instradati a NEWYORK a meno che non siano non disponibili quando vengono inviati a CHICAGO.

Nota:

La disponibilità di un gestore code remoto si basa sullo stato del canale per tale gestore code. Quando i canali vengono avviati, il loro stato cambia diverse volte, con alcuni stati meno preferenziali rispetto all'algoritmo di gestione del carico di lavoro del cluster. In pratica, ciò significa che è possibile scegliere destinazioni con priorità più bassa (backup) mentre i canali verso destinazioni con priorità più alta (primaria) sono in fase di avvio.

Se è necessario accertarsi che nessun messaggio venga inviato a una destinazione di backup, non utilizzare CLWLPRTY. Prendere in considerazione l'utilizzo di code separate o di CLWLRANK con un passaggio manuale dal primario al backup.

Limitazione del numero di canali utilizzati

Seguire queste istruzioni per limitare il numero di canali attivi che ciascun server esegue quando un'applicazione di controllo prezzi è installata su vari gestori code.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Un'applicazione di controllo prezzi deve essere installata su vari gestori code. Per mantenere basso il numero di canali utilizzati, il numero di canali attivi eseguiti da ciascun server è limitato. L'applicazione è guidata dall'arrivo di messaggi sulla coda PRICEQ .

- Quattro gestori code del server ospitano l'applicazione di controllo prezzi. Due gestori code di query inviano messaggi a PRICEQ per interrogare un prezzo. Altri due gestori code sono configurati come repository completi.

Informazioni su questa attività

Effettuare le operazioni riportate di seguito per limitare il numero di canali utilizzati.

Procedura

1. Scegliere due repository completi.

   Scegliere due gestori code come repository completi per il cluster di controllo prezzi. Sono denominati REPOS1 e REPOS2.

   Emetti il seguente comando:

   ```
   ALTER QMGR REPOS(PRICECHECK)
   ```
2. Definire un canale CLUSRCVR su ciascun gestore code.

   In ogni gestore code del cluster, definire un canale ricevente del cluster e un canale mittente del cluster. Non importa quale sia definito per primo.

   ```
   DEFINE CHANNEL(PRICECHECK.SERVE1) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(SERVER1.COM) CLUSTER(PRICECHECK) DESCR('Cluster-receiver channel')
   ```
3. Definire un canale CLUSSDR su ciascun gestore code.

   Creare una definizione CLUSSDR su ogni gestore code per collegare tale gestore code a uno o più gestori code del repository completo.

   ```
   DEFINE CHANNEL(PRICECHECK.REPOS1) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(REPOS1.COM) CLUSTER(PRICECHECK) DESCR('Cluster-sender channel to
   repository queue manager')
   ```
4. Installare l'applicazione di controllo prezzi.
5. Definire la coda PRICEQ su tutti i gestori code server.

   Immettere il seguente comando per ciascuno di essi:

   ```
   DEFINE QLOCAL(PRICEQ) CLUSTER(PRICECHECK)
   ```
6. Limitare il numero di canali utilizzati dalle query

   Sui gestori code delle query viene limitato il numero di canali attivi utilizzati, immettendo i seguenti comandi su ciascuno di essi:

   ```
   ALTER QMGR CLWLMRUC(2)
   ```
7. Se non è stato ancora fatto, avviare l'iniziatore di canali su WebSphere MQ per z/OS. Su tutte le piattaforme, avviare un programma listener.

   Il programma listener ascolta le richieste di rete in entrata e avvia il canale ricevente del cluster quando è necessario.

Risultati

Figura 53 a pagina 277 mostra il cluster impostato da questa attività.

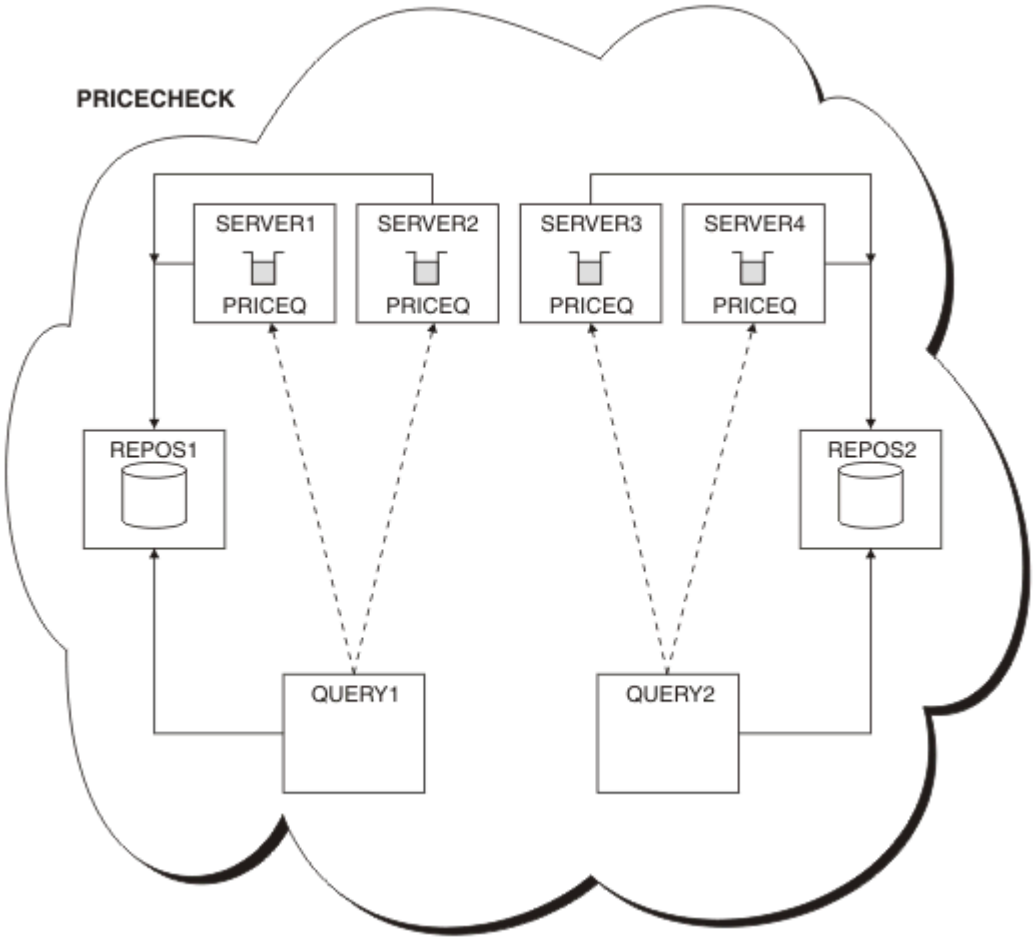


Figura 53. Il cluster PRICECHECK , con quattro gestori code del server, due repository e due gestori code di query

Anche se ci sono quattro istanze della coda PRICEQ disponibili nel cluster PRICECHECK , ogni gestore code che esegue la query utilizza solo due di esse. Ad esempio, il gestore code QUERY1 dispone solo di canali attivi per i gestori code SERVER1 e SERVER2 . Se SERVER1 diventasse non disponibile, il gestore code QUERY1 inizierebbe a utilizzare un altro gestore code, ad esempio SERVER3.

Operazioni successive

Anche se ci sono quattro istanze della coda PRICEQ disponibili nel cluster PRICECHECK , ogni gestore code che esegue la query utilizza solo due di esse. Ad esempio, il gestore code QUERY1 dispone solo di canali attivi per i gestori code SERVER1 e SERVER2 . Se SERVER1 diventasse non disponibile, il gestore code QUERY1 inizierebbe a utilizzare un altro gestore code, ad esempio SERVER3.

Aggiunta di un gestore code più potente che ospita una coda

Seguire queste istruzioni per fornire ulteriore capacità eseguendo il sistema di inventario a Los Angeles e New York, dove Los Angeles può gestire il doppio del numero di messaggi rispetto a New York.

Prima di iniziare

Nota: Affinché le modifiche ad un cluster vengano propagate in tutto il cluster, deve essere sempre disponibile almeno un repository completo. Assicurarsi che i repository siano disponibili prima di avviare questa attività.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in “Aggiunta di un gestore code a un cluster” a pagina 199. Contiene tre gestori code: LONDON e NEWYORK contengono entrambi repository completi, PARIS contiene un repository parziale e inserisce i messaggi da INVENTQ. L'applicazione di inventario viene eseguita sul sistema a New York connesso al gestore code NEWYORK . L'applicazione è guidata dall'arrivo di messaggi sulla coda INVENTQ .
- Si sta allestendo un nuovo negozio a Los Angeles. Per fornire capacità aggiuntiva, si desidera eseguire il sistema di inventario a Los Angeles e New York. Il nuovo gestore code può elaborare il doppio dei messaggi rispetto a New York.

Informazioni su questa attività

Seguire questa procedura per aggiungere un gestore code più potente che ospita una coda.

Procedura

1. Decidere quale repository completo LOSANGELES fa riferimento per primo.
2. Ogni gestore code in un cluster deve fare riferimento a uno o più repository completi per raccogliere informazioni sul cluster. Crea il proprio repository parziale. Non è di particolare importanza quale repository si sceglie. In questo esempio, viene selezionato NEWYORK . Una volta che il nuovo gestore code si è unito al cluster, comunica con entrambi i repository.

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from LOSANGELES to repository at NEWYORK')
   ```

3. Definire il canale CLUSRCVR sul gestore code LOSANGELES.

   Ogni gestore code in un cluster deve definire un canale ricevente del cluster su cui può ricevere i messaggi. Su LOSANGELES, definire:

   ```
   DEFINE CHANNEL(INVENTORY.LOSANGELES) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(LOSANGELES.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for queue manager LOSANGELES')
   CLWLWGHT(2)
   ```

   Il canale ricevente del cluster annuncia la disponibilità del gestore code a ricevere messaggi da altri gestori code nel cluster INVENTORY. L'impostazione di CLWLWGHT su due garantisce che il gestore code di Los Angeles riceva il doppio dei messaggi di inventario rispetto a New York (quando il canale di NEWYORK è impostato su uno).
4. Modificare il canale CLUSRCVR sul gestore code NEWYORK.

   Assicurarsi che il gestore code di Los Angeles riceva il doppio dei messaggi di inventario di New York. Modificare la definizione del canale ricevente del cluster.

   ```
   ALTER CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) CLWLWGHT(1)
   ```

5. Esaminare l'applicazione inventario per le affinità dei messaggi.

   Prima di procedere, assicurarsi che l'applicazione di inventario non abbia alcuna dipendenza dalla sequenza di elaborazione dei messaggi.
6. Installa l'applicazione di inventario sul sistema a Los Angeles
7. Definire la coda del cluster INVENTQ.

   La coda INVENTQ , che è già ospitata dal gestore code NEWYORK , deve essere ospitata anche da LOSANGELES. Definirlo sul gestore code LOSANGELES nel modo seguente:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

   Ora che sono state completate tutte le definizioni, se non è ancora stato fatto, avviare l'iniziatore di canali su WebSphere MQ per z/OS. Su tutte le piattaforme, avviare un programma listener sul Gestore code LOSANGELES. Il programma listener ascolta le richieste di rete in entrata e avvia il canale ricevente del cluster quando è necessario.

Risultati

“Aggiunta di un gestore code più potente che ospita una coda” a pagina 277 mostra il cluster impostato da questa attività.

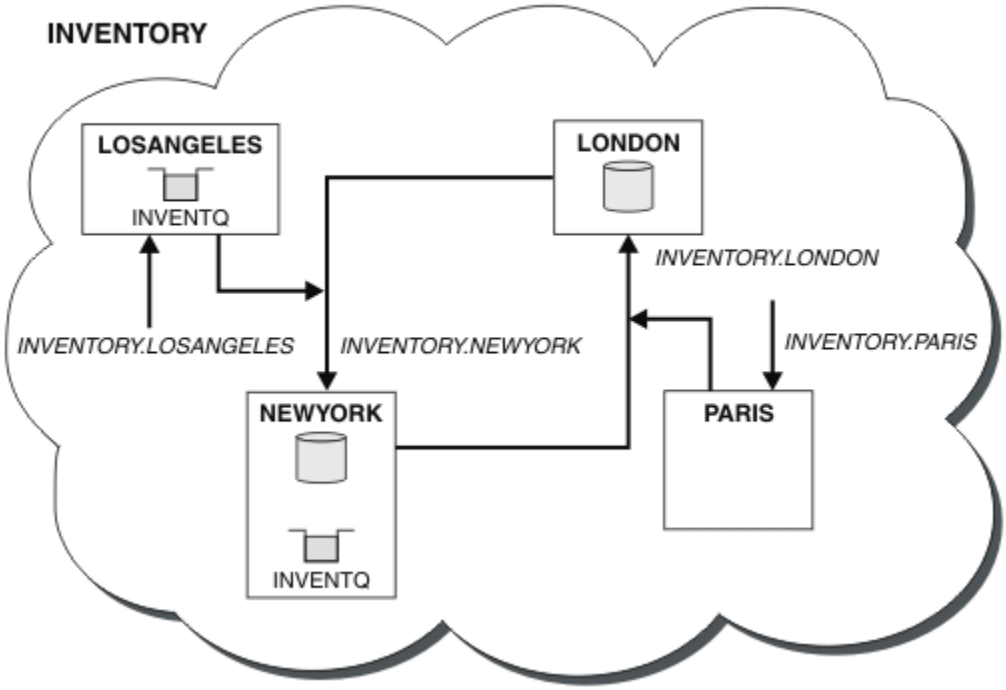


Figura 54. Il cluster INVENTORY con quattro gestori code

Questa modifica al cluster è stata effettuata senza dover modificare i gestori code LONDON e PARIS. I repository in questi gestori code vengono aggiornati automaticamente con le informazioni necessarie per inviare messaggi a INVENTQ all'indirizzo LOSANGELES.

Operazioni successive

La coda INVENTQ e l'applicazione di inventario si trovano su due gestori code nel cluster. La configurazione aumenta la loro disponibilità, velocizza la velocità di trasmissione dei messaggi e consente la distribuzione del carico di lavoro tra i due gestori code. I messaggi inseriti in INVENTQ da LOSANGELES o NEWYORK vengono gestiti dall'istanza sul gestore code locale quando possibile. I messaggi inseriti da LONDON o PARIS vengono instradati a LOSANGELES o NEWYORK, con il doppio dei messaggi inviati a LOSANGELES.

Cluster e programmazione delle applicazioni

Non è necessario apportare alcuna modifica di programmazione per trarre vantaggio da più istanze della stessa coda. Tuttavia, alcuni programmi non funzionano correttamente a meno che non venga inviata una sequenza di messaggi alla stessa istanza di una coda.

Le applicazioni possono aprire una coda utilizzando la chiamata MQOPEN . Le applicazioni utilizzano la chiamata MQPUT per inserire messaggi in una coda aperta. Le applicazioni possono inserire un singolo messaggio in una coda non già aperta, utilizzando la chiamata MQPUT1 .

Se si configurano i cluster che hanno più istanze della stessa coda, non ci sono considerazioni specifiche sulla programmazione dell'applicazione. Tuttavia, per trarre vantaggio dagli aspetti di gestione del carico di lavoro del cluster, potrebbe essere necessario modificare le applicazioni. Se si imposta una rete in cui sono presenti più definizioni della stessa coda, esaminare le applicazioni per le affinità dei messaggi.

Si supponga, ad esempio, di avere due applicazioni che si basano su una serie di messaggi che scorrono tra di loro sotto forma di domande e risposte. Probabilmente si desidera che le risposte ritornino allo stesso gestore code che ha inviato una domanda. È importante che la routine di gestione del carico di lavoro non invii i messaggi ad alcun gestore code che ospita una copia della coda di risposta.

È possibile disporre di applicazioni che richiedono l'elaborazione dei messaggi in sequenza (ad esempio, un'applicazione di replica del database che invia batch di messaggi che devono essere richiamati in sequenza). L'utilizzo di messaggi segmentati può anche causare un problema di affinità.

Apertura di una versione locale o remota della coda di destinazione

Tenere presente il modo in cui il gestore code sceglie di utilizzare una versione locale o remota della coda di destinazione.

1. Il gestore code apre la versione locale della coda di destinazione per leggere i messaggi o per impostare gli attributi della coda.
2. Il gestore code apre qualsiasi istanza della coda di destinazione in cui scrivere i messaggi, se si verifica almeno una delle seguenti condizioni:
   - Una versione locale della coda di destinazione non esiste.
   - Il gestore code specifica `CLWLUSEQ(ANY)` su `ALTER QMGR`.
   - La coda sul gestore code specifica `CLWLUSEQ(ANY)`.

Gestione delle affinità dei messaggi

Le affinità dei messaggi sono raramente parte di un buon progetto di programmazione. È necessario rimuovere le affinità di messaggi per utilizzare completamente il clustering. Se non è possibile rimuovere le affinità dei messaggi, è possibile forzare la consegna dei messaggi correlati utilizzando lo stesso canale e lo stesso gestore code.

Se si dispone di applicazioni con affinità di messaggi, rimuovere le affinità prima di iniziare a utilizzare i cluster.

La rimozione delle affinità dei messaggi migliora la disponibilità delle applicazioni. Un'applicazione invia un batch di messaggi con affinità di messaggi a un gestore code. Il gestore code non riesce dopo aver ricevuto solo una parte del batch. Il gestore code di invio deve attendere il ripristino ed elaborare il batch di messaggi incompleto prima di poter inviare ulteriori messaggi.

La rimozione delle affinità dei messaggi migliora anche la scalabilità delle applicazioni. Un batch di messaggi con affinità può bloccare le risorse sul gestore code di destinazione in attesa di messaggi successivi. Queste risorse potrebbero rimanere bloccate per lunghi periodi di tempo, impedendo ad altre applicazioni di svolgere il proprio lavoro.

Inoltre, le affinità dei messaggi impediscono alle routine di gestione del carico di lavoro del cluster di effettuare la scelta migliore del gestore code.

Per rimuovere le affinità, considerare le seguenti possibilità:

- Trasmissione delle informazioni di stato nei messaggi
- Gestione delle informazioni sullo stato nella memoria non volatile accessibile a qualsiasi gestore code, ad esempio in un database Db2
- Replica dei dati di sola lettura in modo che siano accessibili a più di un gestore code

Se non è appropriato modificare le proprie applicazioni per rimuovere le affinità dei messaggi, esistono diverse soluzioni possibili per il problema.

Denominare una destinazione specifica sulla chiamata `MQOPEN`

Specificare il nome della coda remota e il nome del gestore code in ogni chiamata `MQOPEN` e tutti i messaggi inseriti nella coda utilizzando l'handle dell'oggetto vanno allo stesso gestore code, che potrebbe essere il gestore code locale.

La specifica del nome della coda remota e del gestore code su ogni chiamata MQOPEN presenta degli svantaggi:

- Non viene eseguito alcun bilanciamento del workload. Non si traggono vantaggi dal bilanciamento del carico di lavoro del cluster.
- Se il gestore code di destinazione è remoto e vi è più di un canale, i messaggi potrebbero essere instradati in modo diverso e la sequenza di messaggi non viene ancora conservata.
- Se il gestore code dispone di una definizione per una coda di trasmissione con lo stesso nome del gestore code di destinazione, i messaggi vengono inseriti in tale coda di trasmissione piuttosto che nella coda di trasmissione del cluster.

Restituisce il nome del gestore code nel campo del gestore code di risposta

Consentire al gestore code che riceve il primo messaggio in batch di restituire il suo nome nella risposta. Ciò avviene utilizzando il campo ReplyToQMgr del descrittore del messaggio. Il gestore code all'estremità di invio può quindi estrarre il nome del gestore code di risposta e specificarlo su tutti i messaggi successivi.

L'uso delle informazioni ReplyToGestore code dalla risposta ha degli svantaggi:

- Il gestore code richiedente deve attendere una risposta al primo messaggio
- È necessario scrivere ulteriore codice per trovare e utilizzare le informazioni ReplyToGestore code prima di inviare i messaggi successivi
- Se è presente più di un instradamento al gestore code, la sequenza dei messaggi potrebbe non essere conservata

Impostare l'opzione MQOO_BIND_ON_OPEN sulla chiamata MQOPEN

Forzare tutti i messaggi da inserire nella stessa destinazione utilizzando l'opzione MQOO_BIND_ON_OPEN sulla chiamata MQOPEN . È necessario specificare MQOO_BIND_ON_OPEN o MQOO_BIND_ON_GROUP quando si utilizzano gruppi di messaggi con cluster per garantire che tutti i messaggi nel gruppo vengano elaborati alla stessa destinazione.

Aprendo una coda e specificando MQOO_BIND_ON_OPEN, si forza l'invio di tutti i messaggi inviati a questa coda alla stessa istanza della coda. MQOO_BIND_ON_OPEN esegue il bind di tutti i messaggi allo stesso gestore code e allo stesso instradamento. Ad esempio, se esiste un instradamento IP e un instradamento NetBIOS alla stessa destinazione, uno di questi viene selezionato quando la coda viene aperta e questa selezione viene rispettata per tutti i messaggi inseriti nella stessa coda utilizzando l'handle dell'oggetto ottenuto.

Specificando MQOO_BIND_ON_OPEN si forzano tutti i messaggi ad essere instradati alla stessa destinazione. Pertanto, le applicazioni con affinità di messaggi non vengono interrotte. Se la destinazione non è disponibile, i messaggi rimangono nella coda di trasmissione fino a quando non diventano nuovamente disponibili.

MQOO_BIND_ON_OPEN si applica anche quando il nome gestore code viene specificato nel descrittore oggetto quando si apre una coda. È possibile che vi sia più di un instradamento al gestore code indicato. Ad esempio, potrebbero essere presenti più percorsi di rete oppure un altro gestore code potrebbe aver definito un alias. Se si specifica MQOO_BIND_ON_OPEN, viene selezionato un instradamento quando la coda viene aperta.

Nota: Questa è la tecnica consigliata. Tuttavia, non funziona in una configurazione multi - hop in cui un gestore code annuncia un alias per una coda cluster. Inoltre, non è utile nelle situazioni in cui le applicazioni utilizzano code differenti sullo stesso gestore code per diversi gruppi di messaggi.

Un'alternativa per specificare MQOO_BIND_ON_OPEN sulla chiamata MQOPEN , è quella di modificare le proprie definizioni di coda. Sulle definizioni della coda, specificare DEFBIND(OPEN) e consentire l'opzione DefBind sulla chiamata MQOPEN per impostazione predefinita MQOO_BIND_AS_Q_DEF.

Impostare l'opzione MQOO_BIND_ON_GROUP sulla chiamata MQOPEN

Forzare l'inserimento di tutti i messaggi in un gruppo nella stessa destinazione utilizzando l'opzione MQOO_BIND_ON_GROUP nella chiamata MQOPEN . È necessario specificare MQOO_BIND_ON_OPEN o MQOO_BIND_ON_GROUP quando si utilizzano gruppi di messaggi con cluster per garantire che tutti i messaggi nel gruppo vengano elaborati alla stessa destinazione.

Aprendo una coda e specificando MQOO_BIND_ON_GROUP, si forza l'invio di tutti i messaggi in un gruppo inviati a questa coda alla stessa istanza della coda. MQOO_BIND_ON_GROUP associa tutti i messaggi in un gruppo allo stesso gestore code e anche allo stesso instradamento. Ad esempio, se c'è un instradamento IP e un instradamento NetBIOS alla stessa destinazione, uno di questi viene selezionato quando la coda viene aperta e questa selezione viene rispettata per tutti i messaggi in un gruppo inserito nella stessa coda utilizzando l'handle dell'oggetto ottenuto.

Specificando MQOO_BIND_ON_GROUP si forzano tutti i messaggi in un gruppo ad essere instradati alla stessa destinazione. Pertanto, le applicazioni con affinità di messaggi non vengono interrotte. Se la destinazione non è disponibile, i messaggi rimangono nella coda di trasmissione fino a quando non diventano nuovamente disponibili.

MQOO_BIND_ON_GROUP si applica anche quando il nome gestore code viene specificato nel descrittore oggetto quando si apre una coda. È possibile che vi sia più di un instradamento al gestore code indicato. Ad esempio, potrebbero essere presenti più percorsi di rete oppure un altro gestore code potrebbe aver definito un alias. Se si specifica MQOO_BIND_ON_GROUP, viene selezionato un instradamento quando la coda viene aperta.

Perché MQOO_BIND_ON_GROUP sia effettivo, è necessario includere l'opzione di inserimento MQPMO_LOGICAL_ORDER in MQPUT. È possibile impostare **GroupId** in MQMD del messaggio su MQGI_NONEed è necessario includere i seguenti indicatori di messaggio nel campo MQMD **MsgFlags** dei messaggi:

- Ultimo messaggio nel gruppo: MQMF_LAST_MSG_IN_GROUP
- Tutti gli altri messaggi nel gruppo: MQMF_MSG_IN_GROUP

Se MQOO_BIND_ON_GROUP è specificato ma i messaggi non sono raggruppati, il funzionamento è equivalente a MQOO_BIND_NOT_FIXED.

Nota: Questa è la tecnica consigliata per garantire che i messaggi in un gruppo vengano inviati alla stessa destinazione. Tuttavia, non funziona in una configurazione multi - hop in cui un gestore code annuncia un alias per una coda cluster.

Un'alternativa per specificare MQOO_BIND_ON_GROUP sulla chiamata MQOPEN , è quella di modificare le proprie definizioni di coda. Sulle definizioni della coda, specificare DEFBIND(GROUP) e consentire l'opzione DefBind sulla chiamata MQOPEN per impostazione predefinita MQOO_BIND_AS_Q_DEF.

Scrivere un programma di uscita del carico di lavoro del cluster personalizzato

Invece di modificare le applicazioni, è possibile aggirare il problema di affinità dei messaggi scrivendo un programma di uscita del carico di lavoro cluster. La scrittura di un programma di uscita del carico di lavoro del cluster non è semplice e non è una soluzione consigliata. Il programma dovrebbe essere progettato per riconoscere l'affinità ispezionando il contenuto dei messaggi. Dopo aver riconosciuto l'affinità, il programma dovrà forzare il programma di utilità di gestione del carico di lavoro ad instradare tutti i messaggi correlati allo stesso gestore code.

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 WebSphere MQ , come una buona gestione dell'applicazione e la progettazione della rete. Prima di continuare, accertarsi di conoscere le informazioni riportate negli argomenti correlati elencati di seguito.

Concetti correlati

Clustering

Concetti di intercomunicazione

Funzionamento dei cluster

Clustering: considerazioni speciali per i cluster che si sovrappongono

Questo argomento fornisce una guida per pianificare e gestire i cluster IBM WebSphere 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. Consultare “Cluster sovrapposti” a pagina 183 e “Configurazione dei percorsi dei messaggi tra cluster” a pagina 261 per le informazioni necessarie.

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

- Sebbene i cluster IBM WebSphere 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. Si consiglia di seguire una convenzione di denominazione adatta, le convenzioni possibili sono descritte in “Convenzioni di denominazione cluster” a pagina 182.
- A volte la cooperazione amministrativa e di gestione del sistema è essenziale / inevitabile: ad esempio, la cooperazione tra organizzazioni che possiedono diversi cluster che devono sovrapporsi. Una chiara comprensione di chi possiede cosa e delle regole / 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 283per 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 implementa SSL o 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:

- Il nome indicato in tale cluster è accessibile all'altro cluster.

- Il nome pubblicizzato in un cluster può essere pubblicizzato nell'altro per estrarre i messaggi idonei.
- L'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 teo 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 182
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 WebSphere 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

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 WebSphere MQ sottoscrizioni utilizzate per la messaggistica di pubblicazione / sottoscrizione in IBM WebSphere 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 applicazioniIBM WebSphere 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 cluster” a pagina 166.

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 WebSphere 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 impostazione può causare problemi di amministrazione in un secondo momento; considerare, ad esempio, il caso in cui SSL deve essere applicato a un cluster ma non a un secondo. È quindi preferibile creare definizioni separate e la convenzione di denominazione suggerita in “Convenzioni di denominazione cluster” a pagina 182 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 compreso prima di utilizzare le informazioni qui), consultare “Utilizzo dei cluster per la gestione del carico di lavoro” a pagina 266, il Bilanciamento del carico di lavoro e L'algoritmo di gestione del carico di lavoro 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 WebSphere 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 WebSphere 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 WebSphere 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 55 a pagina 289 è una sezione di una grande distribuzione IBM WebSphere MQ che illustra l'importanza 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.

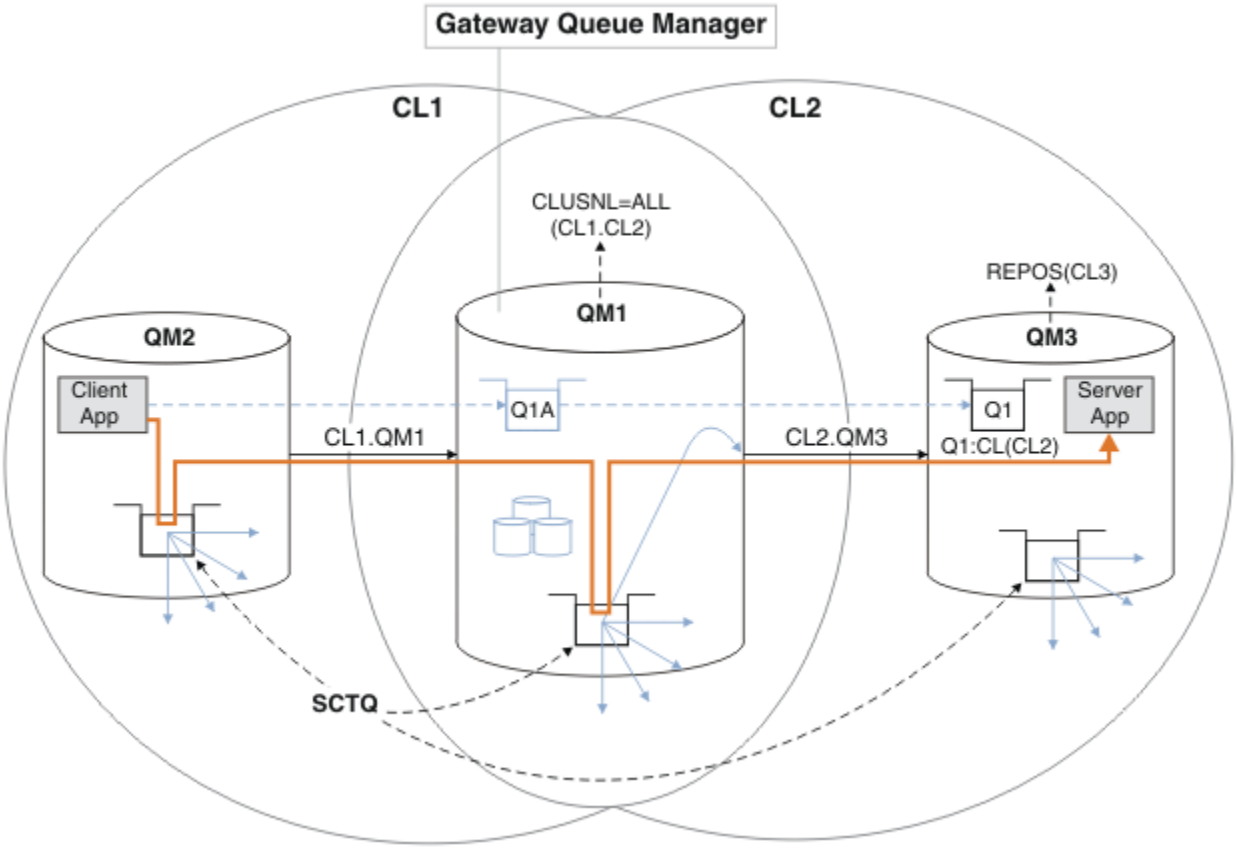
L'architettura hub e spoke richiede tutti i messaggi tra i cluster per passare attraverso il gestore code del gateway. Il risultato è che tutti i messaggi passano attraverso la singola coda di trasmissione del cluster su QM1, SYSTEM.CLUSTER.TRANSMIT.QUEUE.

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 55 a pagina 289 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 55. Applicazione client-server distribuita all'architettura hub e spoke utilizzando i cluster IBM WebSphere MQ

In Figura 55 a pagina 289, 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 55 a pagina 289, 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 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 pagina 203.

A partire da Version 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 mittente del cluster trasferiscono i messaggi da ciascuna coda di trasmissione; consultare “Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 206.
2. Consente al gestore code di creare e gestire automaticamente ulteriori code di trasmissione cluster. Definisce una coda di trasmissione cluster differente per ogni canale mittente del cluster; consultare “Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi” a pagina 226

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 adottato in “Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 206. 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” a pagina 206è 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 nelle singole code utilizzando le definizioni di coda remota 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 cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 209, la limitazione viene eluso aggiungendo un altro cluster e rendendo il gestore code e la coda cluster un membro 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 163
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.

“Clustering: considerazioni speciali per i cluster che si sovrappongono” a pagina 283
Questo argomento fornisce una guida per pianificare e gestire i cluster IBM WebSphere MQ . Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

“Code di trasmissione cluster e canali mittente cluster” a pagina 174
I messaggi tra i gestori code con cluster vengono memorizzati nelle code di trasmissione cluster e inoltrati dai canali mittenti del cluster.

“Cluster sovrapposti” a pagina 183
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” a pagina 203
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una definizione remota della coda cluster e un canale mittente e una coda di trasmissione separati.

“Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 206
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una coda di trasmissione cluster aggiuntiva per separare il traffico di messaggi a un singolo gestore code in un cluster.

“Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 209
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza un cluster aggiuntivo per isolare i messaggi in una particolare coda cluster.

“Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi” a pagina 226
È possibile modificare il modo predefinito in cui un gestore code memorizza i messaggi per una coda cluster o un argomento su una coda di trasmissione. La modifica del valore predefinito fornisce un modo per isolare i messaggi cluster su un gestore code del gateway.

“Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221
Seguire le istruzioni nell'attività per creare cluster sovrapposti con un gestore code del gateway. Utilizzare i cluster come punto iniziale per i seguenti esempi di isolamento dei messaggi in un'applicazione da messaggi in altre applicazioni in un cluster.

“Configurazione dei percorsi dei messaggi tra cluster” a pagina 261
Connettere i cluster utilizzando un gestore code gateway. Rendere le code o i gestori code visibili a tutti i cluster definendo gli alias della coda del cluster o del gestore code del cluster sul gestore code del gateway.

“Clustering: pianificazione della configurazione delle code di trasmissione del cluster” a pagina 291
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. La configurazione di più code di trasmissione cluster si applica a piattaforme diverse da z/OS.

Riferimenti correlati

“Sicurezza” a pagina 435
Utilizzare la stanza `Security` nel file `qm.ini` per specificare opzioni per OAM (Object Authority Manager).

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. La configurazione di più code di trasmissione cluster si applica a piattaforme diverse da z/OS.

Prima di iniziare

Consultare “Come scegliere quale tipo di coda di trasmissione del cluster utilizzare” a pagina 294.

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 56 a pagina 292. 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.

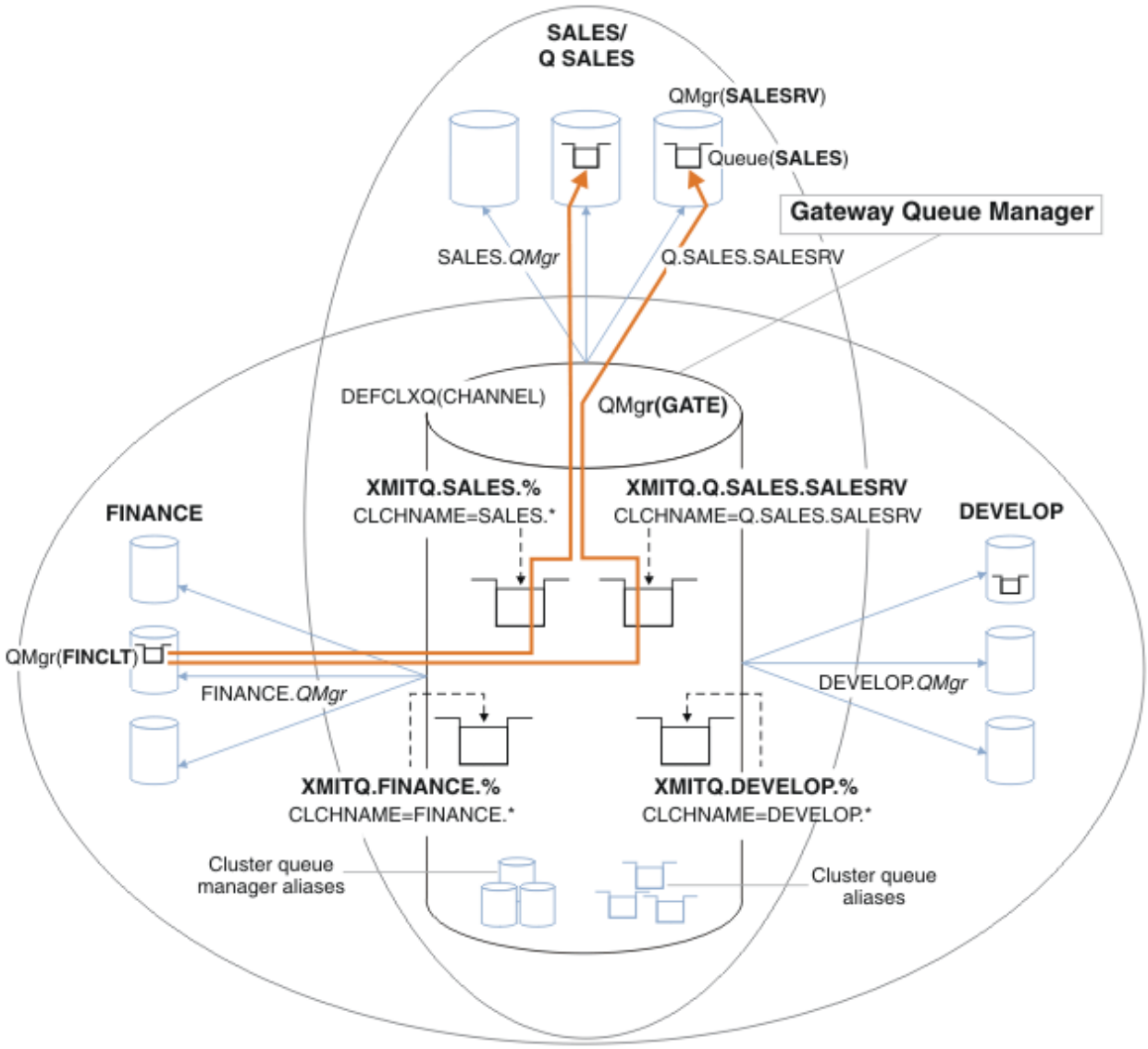


Figura 56. Esempio di code di trasmissione specifiche per cluster IBM WebSphere MQ dipartimentali differenti

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 296. 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 283.

   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 296.
   - 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

“Code di trasmissione cluster e canali mittente cluster” a pagina 174
I messaggi tra i gestori code con cluster vengono memorizzati nelle code di trasmissione cluster e inoltrati dai canali mittenti del cluster.

“Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster” a pagina 288
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.

“Controllo accessi e code di trasmissione di più cluster” a pagina 163
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.

“Clustering: considerazioni speciali per i cluster che si sovrappongono” a pagina 283
Questo argomento fornisce una guida per pianificare e gestire i cluster IBM WebSphere MQ . Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

“Cluster sovrapposti” a pagina 183
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” a pagina 203
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una definizione remota della coda cluster e un canale mittente e una coda di trasmissione separati.

“Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 206
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza una coda di trasmissione cluster aggiuntiva per separare il traffico di messaggi a un singolo gestore code in un cluster.

“Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 209
Modificare la configurazione dei cluster sovrapposti che utilizzano un gestore code gateway. Dopo che i messaggi di modifica sono stati trasferiti a un'applicazione dal gestore code del gateway senza utilizzare la stessa coda di trasmissione o gli stessi canali degli altri messaggi cluster. La soluzione utilizza un cluster aggiuntivo per isolare i messaggi in una particolare coda cluster.

“Modifica del valore predefinito per separare le code di trasmissione del cluster per isolare il traffico dei messaggi” a pagina 226
È possibile modificare il modo predefinito in cui un gestore code memorizza i messaggi per una coda cluster o un argomento su una coda di trasmissione. La modifica del valore predefinito fornisce un modo per isolare i messaggi cluster su un gestore code del gateway.

“Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 221
Seguire le istruzioni nell'attività per creare cluster sovrapposti con un gestore code del gateway. Utilizzare i cluster come punto iniziale per i seguenti esempi di isolamento dei messaggi in un'applicazione da messaggi in altre applicazioni in un cluster.

“Configurazione dei percorsi dei messaggi tra cluster” a pagina 261
Connettere i cluster utilizzando un gestore code gateway. Rendere le code o i gestori code visibili a tutti i cluster definendo gli alias della coda del cluster o del gestore code del cluster sul gestore code del gateway.

Come scegliere quale tipo di coda di trasmissione del cluster utilizzare

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

Da Version 7.5 in poi, è possibile scegliere quale coda di trasmissione cluster è associata ad un canale mittente del cluster.

1. È possibile avere tutti i canali mittente del cluster associati alla singola coda di trasmissione del cluster predefinita, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Questa opzione è l'opzione predefinita ed è l'unica scelta per i gestori code su cui è in esecuzione la versione Version 7.1o precedente.
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.

   Attenzione: Se si sta utilizzando SYSTEM.CLUSTER.TRANSMIT.QUEUES dedicato con un gestore code che è stato aggiornato da una versione precedente del prodotto, assicurarsi che SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE abbia l'opzione SHARE/NOSHARE impostata su **SHARE**.
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 283, 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.

Procedure consigliate

Nella maggior parte dei casi, per le installazioni esistenti di IBM WebSphere 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 WebSphere 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, condividendo 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 inviati da un gestore code gateway” a pagina 209

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 il metodo “Aggiunta di un cluster e di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 209 sistematicamente a tutte le code 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 291 e arrivare alla configurazione mostrata in Figura 57 a pagina 297. 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 299.

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`, `FINANCE`e `DEVELOP` sono già definiti. I messaggi cluster vengono attualmente inoltrati da `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

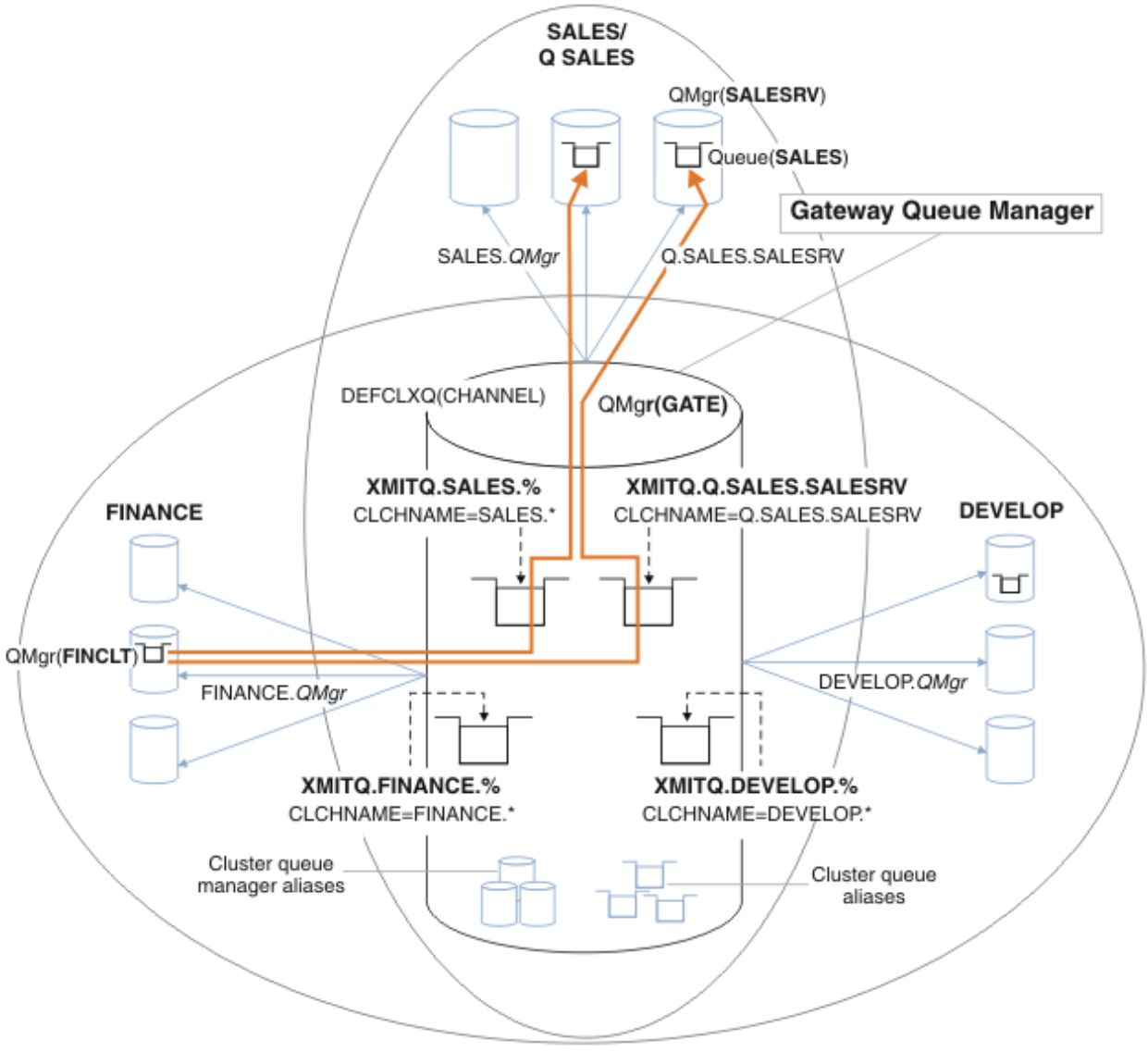


Figura 57. Esempio di code di trasmissione specifiche per cluster IBM WebSphere MQ dipartimentali differenti

La procedura per modificare i cluster è la seguente; consultare Modifiche per isolare le code di vendita in un nuovo cluster e separare le code di trasmissione cluster gateway per le definizioni.

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 58 a pagina 302.

   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) FINANCE(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
```

Quando lo switch è completo, rimuovere la coda SALES dal cluster SALES ; consultare Figura 58 a pagina 302.

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 dei gestori code in Tabella 27 a pagina 300.

Tabella 27. Nomi di gestori code e numeri di porta		
Descrizione	**Nome 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 27 a pagina 300.

   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 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 58 a pagina 302:

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

   Figura 58. 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 301
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 "Come funziona il processo di commutazione del canale mittente del cluster in una coda di trasmissione differente" a pagina 176 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 306.

  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 307.

  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.

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” a pagina 306
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.

“Commutazione di un canale mittente del cluster arrestato ad un'altra coda di trasmissione del cluster” a pagina 307

Informazioni correlate

“Come funziona il processo di commutazione del canale mittente del cluster in una coda di trasmissione differente” a pagina 176

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 “Come funziona il processo di commutazione del canale mittente del cluster in una coda di trasmissione differente” a pagina 176 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: Controllare i messaggi "AMQ7341 La coda di trasmissione per il canale *ChannelName* è passata 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

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 “Come funziona il processo di commutazione del canale mittente del cluster in una coda di trasmissione differente” a pagina 176 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(QUIESCSE) STATUS(STOPPED)
      ```

2. Opzionale: Apportare le modifiche alla configurazione.

Ad esempio, consultare “Clustering: configurazione di esempio di più code di trasmissione cluster” a pagina 296.

3. Passare i canali mittente del cluster alle nuove code di trasmissione del cluster.

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

Il comando **runswchl** trasferisce tutti 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 306 in “Commutazione dei canali mittenti del cluster attivi in un'altra serie di code di trasmissione cluster” a pagina 306. 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: Controllare i messaggi "AMQ7341 La coda di trasmissione per il canale *ChannelName* è passata 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

Risoluzione canale

Arresto canale

Clustering: procedure ottimali di migrazione e modifica

Questo argomento fornisce una guida per la pianificazione e la gestione dei cluster IBM WebSphere MQ . Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

1. “Spostamento di oggetti in un cluster” a pagina 308 (Procedure ottimali per spostare gli oggetti all'interno di un cluster, senza installare fix pack o nuove versioni di IBM WebSphere MQ).
2. “Aggiornamenti e installazioni di manutenzione” a pagina 310 (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 gli aggiornamenti di 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 WebSphere 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 lo "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 gestione a tutti i gestori code, quindi l'avvio di tutto allo stesso tempo): i cluster sono progettati per funzionare ancora con più versioni del gestore code coesistenti, quindi si raccomanda un approccio di manutenzione pianificato e graduale.

Disporre di un piano di backup:

- Su z/OS, sono state applicate le PTF di migrazione all'indietro?
- 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. Ad esempio, nello spostamento in IBM WebSphere MQ Version 7.1 da IBM WebSphere MQ Version 6.0, se un gestore code definisce un argomento cluster, i gestori code IBM WebSphere MQ Version 6.0 non comprenderanno la definizione o non saranno in grado di eseguire la pubblicazione su questo argomento.

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.

Concetti correlati

“Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER” a pagina 310
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: 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 WebSphere 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 nella documentazione di questo prodotto o quando richiesto dal supporto IBM , è possibile utilizzare il comando **REFRESH CLUSTER** per eliminare tutte le informazioni contenute 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 311.

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 eseguire lo scaglionamento dell'attività per diverse ore o per 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 di z/OS , SCHQ deve essere definito manualmente. I messaggi sullo SCHQ scadono dopo tre mesi.

Concetti correlati

Problemi dell'applicazione durante l'esecuzione di REFRESH CLUSTER

REFRESH CLUSTER considerazioni per i cluster di pubblicazione / sottoscrizione

Riferimenti correlati

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 WebSphere MQ . Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

IBM WebSphere 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 WebSphere 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 WebSphere MQ sia il più disponibile possibile in modo che possa essere utilizzata in tale architettura.

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 la migliore offerta integrata per mantenere disponibili i tuoi messaggi esistenti. Consultare “Utilizzo di WebSphere MQ con configurazioni ad alta disponibilità” a pagina 321, “Crea un gestore code a più istanze” a pagina 349e la 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 Version 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 WebSphere 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 WebSphere MQ può aiutare, ma non può farlo automaticamente. L'unica opzione di ripristino di emergenza 'true' in IBM WebSphere 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.
  - Non emettere il certificato SSL attivo per il sistema di ripristino di emergenza fino a quando, o a meno che, non si verifichi un reale scenario di ripristino di emergenza.
- 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 310. Esaminare tutta la documentazione del processo interno e la documentazione di IBM WebSphere 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.

Clustering: monitoraggio

Questo argomento fornisce una guida per pianificare e gestire i cluster IBM WebSphere MQ . Queste informazioni sono una guida basata sul test e sul feedback dei clienti.

Monitoraggio dei messaggi dell'applicazione nel cluster

Generalmente, tutti i messaggi cluster che lasciano il gestore code passano attraverso SYSTEM.CLUSTER.TRANSMIT.QUEUE, indipendentemente dal canale mittente del cluster utilizzato per trasmettere il messaggio. Ogni canale sta svuotando i messaggi destinati a tale canale in parallelo con tutti gli altri canali mittente del cluster. Un crescente accumulo di messaggi su questa coda può indicare un problema con uno o più canali e deve essere analizzato:

- La profondità della coda deve essere monitorata in modo appropriato per la progettazione del cluster.
- Il seguente comando restituisce tutti i canali che hanno più di un messaggio in attesa sulla coda di trasmissione:

  ```
  DIS CHSTATUS(*) WHERE(XQMSGSA GT 1)
  ```

  Con tutti i messaggi cluster su una singola coda, non sempre è facile vedere quale canale ha problemi quando inizia a riempirsi. L'utilizzo di questo comando è un modo semplice per vedere quale canale è responsabile.

È possibile configurare un gestore code cluster in modo che abbia più code di trasmissione. Se si modifica l'attributo del gestore code DEFCLXQ in CHANNEL, ogni canale mittente del cluster viene associato a una coda di trasmissione del cluster differente. In alternativa, è possibile configurare manualmente code di trasmissione separate. Per visualizzare tutte le code di trasmissione del cluster associate ai canali mittenti del cluster, eseguire il comando:

```
DISPLAY CLUSQMGR (qmgrName) XMITQ
```

Definire le code di trasmissione cluster in modo che seguano il modello di avere la radice fissa del nome della coda sulla sinistra. È quindi possibile interrogare la profondità di tutte le code di trasmissione cluster restituite dal comando **DISPLAY CLUSMGR** , utilizzando un nome coda generico:

```
DISPLAY QUEUE (qname*) CURDEPTH
```

Monitoraggio dei messaggi di controllo nel cluster

La coda SYSTEM.CLUSTER.COMMAND.QUEUE viene utilizzata per elaborare tutti i messaggi di controllo cluster per un gestore code, generati dal gestore code locale o inviati a questo gestore code da altri gestori code nel cluster. Quando un gestore code mantiene correttamente il proprio stato cluster,

questa coda tende a zero. Ci sono situazioni in cui la profondità dei messaggi su questa coda può temporaneamente aumentare:

- Avere molti messaggi nella coda indica il tasso di abbandono nello stato del cluster.
- Quando si apportano modifiche significative, consentire alla coda di stabilirsi tra tali modifiche. Ad esempio, quando si spostano i repository, consentire alla coda di raggiungere lo zero prima di spostare il secondo repository.

Mentre un backlog di messaggi è presente su questa coda, gli aggiornamenti allo stato del cluster o i comandi relativi al cluster non vengono elaborati. Se i messaggi non vengono rimossi da questa coda per un lungo periodo di tempo, è necessaria un'ulteriore analisi, inizialmente mediante l'ispezione dei log di errori del gestore code che potrebbe spiegare il processo che sta causando questa situazione.

Il `SYSTEM.CLUSTER.REPOSITORY.QUEUE` contiene le informazioni sulla cache del repository del cluster come un numero di messaggi. È consuetudine che i messaggi siano sempre presenti in questa coda e più per i cluster più grandi. Pertanto, la profondità dei messaggi su questa coda non è un problema.

Log di monitoraggio

I problemi che si verificano nel cluster potrebbero non mostrare sintomi esterni alle applicazioni per molti giorni (e anche mesi) dopo che il problema si verifica originariamente a causa della memorizzazione nella cache delle informazioni e della natura distribuita del clustering. Tuttavia, il problema originale viene spesso riportato nei log degli errori IBM WebSphere MQ. Per questo motivo, è fondamentale monitorare attivamente questi log per tutti i messaggi scritti relativi al clustering. Questi messaggi devono essere letti e compresi, con qualsiasi azione intrapresa ove necessario.

Ad esempio: un'interruzione nelle comunicazioni con un gestore code in un cluster può determinare la conoscenza di alcune risorse cluster che vengono eliminate a causa del modo in cui i cluster riconvalidono regolarmente le risorse cluster ripubblicando le informazioni. Un'avvertenza di tale evento che potrebbe verificarsi viene riportata dal messaggio AMQ9465. Questo messaggio indica che è necessario esaminare il problema.

Considerazioni speciali per il bilanciamento del carico

Quando il cluster esegue il bilanciamento del carico tra due o più istanze di una coda, le applicazioni che utilizzano devono elaborare i messaggi su ciascuna delle istanze. Se una o più di queste applicazioni terminano o arrestano l'elaborazione dei messaggi, è possibile che il clustering continui a inviare messaggi a tali istanze della coda. In questa situazione, i messaggi non vengono elaborati fino a quando le applicazioni non funzionano nuovamente correttamente. Per questo motivo, il controllo delle applicazioni è una parte importante della soluzione e occorre intraprendere azioni per reinstradare i messaggi in tale situazione. Un esempio di meccanismo per automatizzare tale monitoraggio è il seguente: Programma di esempio Monitoraggio coda cluster (AMQSCLM) .

Disponibilità, ripristino e riavvio

Rendere le applicazioni altamente disponibili mantenendo la disponibilità della coda in caso di errore di un gestore code e ripristinare i messaggi dopo un errore del server o della memoria.

Migliorare la disponibilità delle applicazioni client utilizzando la riconnessione client per passare automaticamente un client tra un gruppo di gestori code o alla nuova istanza attiva di un gestore code a più istanze dopo un errore del gestore code. La riconnessione automatica del client non è supportata dalle classi WebSphere MQ per Java.

Su piattaforme Windows, UNIX, Linux e IBM i distribuiscono applicazioni server a un gestore code a più istanze, configurato per essere eseguito come un singolo gestore code su più server; se il server che esegue l'istanza attiva ha esito negativo, l'esecuzione viene automaticamente commutata in un'istanza in standby dello stesso gestore code su un server diverso. Se si configurano le applicazioni del server per l'esecuzione come servizi del gestore code, queste vengono riavviate quando un'istanza in standby diventa l'istanza del gestore code in esecuzione attiva.

È possibile configurare WebSphere MQ come parte di una soluzione di clustering specifica della piattaforma come Microsoft Cluster Server, o PowerHA per AIX (precedentemente HACMP su AIX) e altre soluzioni di clustering UNIX and Linux .

Un altro modo per aumentare la disponibilità delle applicazioni server consiste nel distribuire le applicazioni server su più computer in un cluster di gestori code.

Un sistema di messaggistica garantisce che i messaggi immessi nel sistema vengano consegnati alla loro destinazione. WebSphere MQ può tracciare l'instradamento di un messaggio mentre si sposta da un gestore code all'altro utilizzando il comando **dspmqrte** . Se un sistema ha esito negativo, i messaggi possono essere ripristinati in vari modi a seconda del tipo di errore e del modo in cui un sistema è configurato.

WebSphere MQ garantisce che i messaggi non vengano persi conservando i log di ripristino delle attività dei gestori code che gestiscono la ricezione, trasmissione e consegna dei messaggi.Utilizza questi log per tre tipi di ripristino:

1. *Riavviare il ripristino*, quando si arresta WebSphere MQ in modo pianificato.
2. *Ripristino da errore*, quando un errore arresta WebSphere MQ.
3. *Ripristino dei supporti*, per ripristinare gli oggetti danneggiati.

In tutti i casi, il ripristino ripristina il gestore code allo stato in cui si trovava quando il gestore code è stato arrestato, ad eccezione del fatto che le transazioni in corso vengono sottoposte a rollback, rimuovendo dalle code gli aggiornamenti in corso al momento dell'arresto del gestore code. Il ripristino ripristina tutti i messaggi persistenti; i messaggi non persistenti potrebbero essere persi durante il processo.

Riconnessione automatica del client

È possibile riconnettere automaticamente le proprie applicazioni client, senza scrivere alcun codice aggiuntivo, configurando un certo numero di componenti.

La riconnessione automatica del client è *in linea*. La connessione viene ripristinata automaticamente in qualsiasi punto del programma applicativo client e vengono ripristinati anche tutti gli handle per aprire gli oggetti.

Al contrario, la riconnessione manuale richiede che l'applicazione client crei nuovamente una connessione utilizzando `MQCONN` o `MQCONNX`e riapra gli oggetti. La riconnessione automatica del client è adatta a molte ma non a tutte le applicazioni client.

Tabella 28 a pagina 316 elenca il primo release del supporto client IBM WebSphere MQ che deve essere installato su una workstation client. È necessario aggiornare le stazioni di lavoro client a uno di questi livelli affinché un'applicazione possa utilizzare la riconnessione client automatica. La Tabella 29 a pagina 316 elenca altri requisiti per abilitare la riconnessione automatica del client.

Con l'accesso del programma alle opzioni di riconnessione, un'applicazione client può impostare le opzioni di riconnessione. Ad eccezione dei client JMS e XMS , se un'applicazione client ha accesso alle opzioni di riconnessione, può anche creare un gestore eventi per gestire gli eventi di riconnessione.

Un'applicazione client esistente potrebbe beneficiare del supporto di riconnessione, senza ricompilazione e collegamento:

- Per un client non JMS, impostare la `mqclient.ini` variabile di ambiente `DefRecon` per impostare opzioni di riconnessione. Utilizzare una CCDT per connettersi a un gestore code. Se il client deve connettersi a un gestore code a più istanze, fornire gli indirizzi di rete delle istanze del gestore code attivo e in standby in CCDT.
- Per un cliente JMS, impostare le opzioni di riconnessione nella configurazione della produzione connessioni. Quando si utilizza l'adattatore di risorse WebSphere MQ o un client JMS integrato in un ambiente Java EE , la riconnessione automatica del client potrebbe non essere disponibile. Esistono delle limitazioni in alcuni degli ambienti gestiti, per ulteriori informazioni consultare Utilizzo della riconnessione automatica del client in ambienti Java SE e Java EE.

Nota: La riconnessione automatica del client non è supportata dalle classi WebSphere MQ per Java.

Tabella 28. Client supportati

Interfaccia client	Client	Accesso del programma alle opzioni di riconnessione	Supporto riconnessione
API di messaggistica	C, C + +, COBOL, Unmanaged Visual Basic, XMS (Unmanaged XMS su Windows)	7.0.1	7.0.1
	JMS (contenitore client JSE e Java EE e contenitori gestiti)	7.0.1.3	7.0.1.3
	Classi WebSphere MQ per Java	Non supportato	Non supportato
	XMS gestiti e client .NET gestiti: C#, Visual Basic	7.1	7.1
Altre API	Windows Communication Foundation (non gestito[1])	Non supportato	7.0.1
	Windows Communication Foundation (gestito[1])	Non supportato	Non supportato
	Asse 1	Non supportato	Non supportato
	Asse 2	Non supportato	7.0.1.3
	HTTP (web 2.0)	Non supportato	7.0.1.3

1. Impostare la modalità gestita o non gestita nella configurazione del bind WCF.

La riconnessione automatica ha i seguenti requisiti di configurazione:

Tabella 29. Requisiti di configurazione della riconnessione automatica

Componente	Requisito	Effetto del mancato rispetto dei requisiti
Installazione del client WebSphere MQ MQI	Consultare Tabella 28 a pagina 316	`MQRC_OPTIONS_ERROR`
Installazione del server WebSphere MQ	Livello 7.0.1	`MQRC_OPTIONS_ERROR`
Canale	`SHARECNV > 0`	`MQRC_ENVIRONMENT_ERROR`
ambiente applicativo	Deve essere con thread	`MQRC_ENVIRONMENT_ERROR`
MQI	Uno tra: • `MQCONNX` con `MQCNO Opzioni` impostate su `MQCNO_RECONNECT` o `MQCNO_RECONNECT_Q_MGR`. • `Defrecon=YES|QMGR` in `mqclient.ini` • In JMS impostare la proprietà CLIENTRECONNECTOPTIONS della produzione connessioni.	`MQCC_FAILED` quando una connessione è interrotta o il gestore code termina o non riesce.

La Figura 59 a pagina 317 mostra le interazioni principali tra i componenti coinvolti nella riconnessione client.

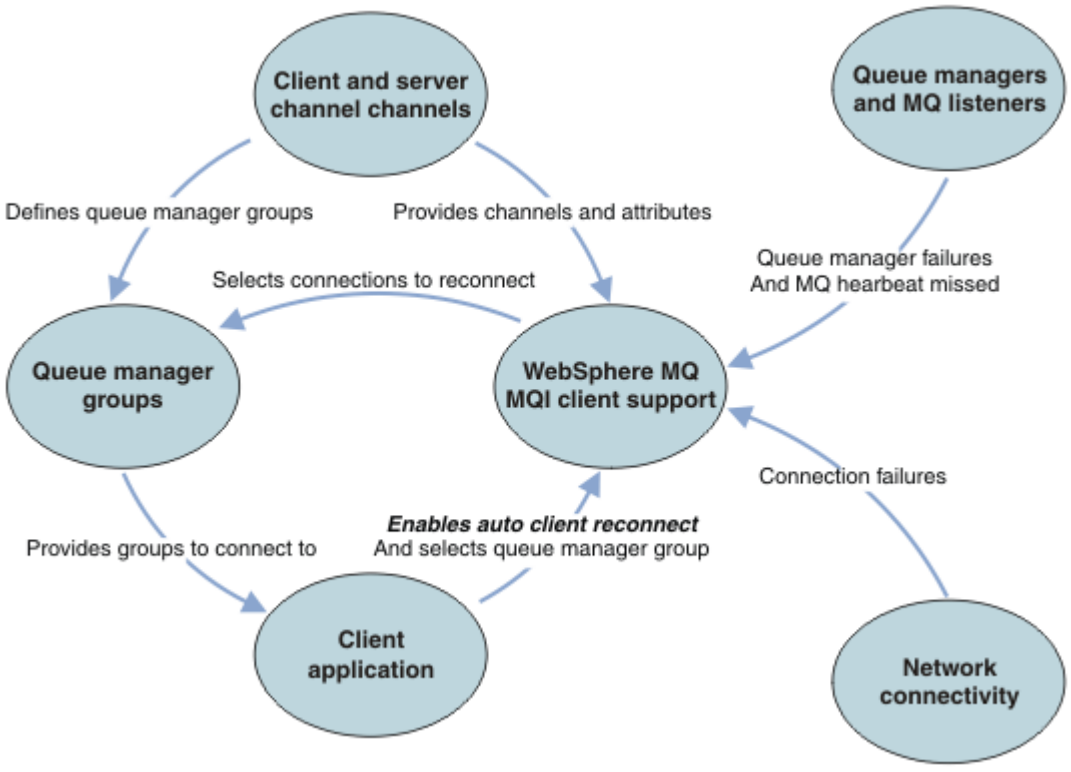


Figura 59. Riconnessione automatica del client

Applicazione client

L'applicazione client è un client IBM WebSphere MQ MQI.

- Per impostazione predefinita, i client non vengono riconnessi automaticamente. Abilitare la riconnessione automatica del client impostando l'opzione `MQCONNX` `MQCNO` `MQCNO_RECONNECT` o `MQCNO_RECONNECT_Q_MGR`.
- Molte applicazioni sono scritte in modo che siano in grado di sfruttare la riconnessione automatica senza alcuna codifica aggiuntiva. Abilitare la riconnessione automatica per programmi esistenti, senza apportare alcuna modifica di codifica, impostando l'attributo `DefRecon` nella stanza dei canali del file di configurazione `mqclient.ini` .
- Utilizzare una delle seguenti tre opzioni:

  1. Modificare il programma in modo che la logica non sia influenzata dalla riconnessione. Ad esempio, potrebbe essere necessario emettere chiamate MQI all'interno del punto di sincronizzazione e inoltrare nuovamente le transazioni di cui è stato eseguito il backout.
  2. Aggiungere un gestore eventi per rilevare la riconnessione e ripristinare lo stato dell'applicazione client quando la connessione viene ristabilita.
  3. Non abilitare la riconnessione automatica: disconnettere il client ed emettere una nuova chiamata MQI `MQCONN` o `MQCONNX` per individuare un'altra istanza del gestore code in esecuzione nello stesso gruppo di gestori code.

  Per ulteriori dettagli su queste tre opzioni, consultare “Ripristino applicazione” a pagina 395.
- La riconnessione a un gestore code con lo stesso nome non garantisce la riconnessione alla stessa istanza di un gestore code.

Utilizzare un'opzione MQ MQCNO_RECONNECT_Q_MGR per riconnettersi a un'istanza dello stesso gestore code.

- Un client può registrare un gestore eventi in modo che possa essere informato dello stato di riconnessione. Il MQHCONN passato nel gestore eventi non può essere utilizzato. Vengono forniti i seguenti codici di errore:

  MQRC_RECONNECTING
  La connessione non è riuscita e il sistema sta tentando di riconnettersi. Si ricevono più eventi MQRC_RECONNECTING se vengono effettuati più tentativi di riconnessione.

  MQRC_RECONNECTED
  La riconnessione è stata effettuata e tutti gli handle sono stati ristabiliti correttamente.

  MQRC_RECONNECT_NON RIUSCITO
  La riconnessione non è riuscita.

  MQRC_RECONNECT_QMID_MISMATCH
  Una connessione ricollegabile ha specificato MQCNO_RECONNECT_Q_MGR e la connessione ha tentato di riconnettersi a un gestore code differente.

  MQRC_RECONNECT_Q_MGR_REQD
  Un'opzione, come MQMO_MATCH_MSG_TOKEN in una chiamata MQGET , è stata specificata nel programma del client che richiede la riconnessione allo stesso gestore code.

- Un client ricollegabile è in grado di riconnettersi automaticamente solo *dopo* la connessione. In altre parole, la chiamata MQCONNX non viene ritentata se ha esito negativo. Ad esempio, se si riceve il codice di ritorno 2543 - MQRC_STANDBY_Q_MGR da MQCONNX, emettere nuovamente la chiamata dopo un breve ritardo.

  MQRC_RECONNECT_INCOMPATIBILE
  Questo codice motivo viene restituito quando l'applicazione tenta di utilizzare MQPMO_LOGICAL_ORDER (con MQPUT e MQPUT1) o MQGMO_LOGICAL_ORDER (con MQGET) quando sono impostate le opzioni di riconnessione. Il motivo per restituire il codice di errore è assicurarsi che le applicazioni non utilizzino mai la riconnessione in tali casi.

  MQRC_CALL_INTERROTTO
  Questo codice motivo viene restituito quando la connessione si interrompe durante l'esecuzione della chiamata Commit e il client si riconnette. Un MQPUT di un messaggio persistente esterno al punto di sincronizzazione determina anche la restituzione dello stesso codice di errore all'applicazione.

Gestori code a più istanze

Semplificare il riavvio delle applicazioni client WebSphere MQ MQI, dopo che un gestore code a più istanze ha attivato la propria istanza in standby, utilizzando la riconnessione client automatica.

L'istanza in standby di un gestore code a più istanze si trova generalmente a un indirizzo di rete diverso rispetto all'istanza attiva. Includere gli indirizzi di rete di entrambe le istanze nella CCDT (client connection definition table). Fornire un elenco di indirizzi di rete per il parametro **CONNAME** oppure definire più righe per il gestore code in CCDT.

Di solito, i client WebSphere MQ MQI si riconnettono a qualsiasi gestore code in un gruppo di gestori code. A volte si desidera che un client WebSphere MQ MQI si riconnette solo allo stesso gestore code. Potrebbe avere un'affinità con un gestore code. È possibile evitare che un client si riconnette a un gestore code differente. Impostare l'opzione MQCNO , MQCNO_RECONNECT_Q_MGR. Il client WebSphere MQ MQI ha esito negativo se si riconnette a un gestore code differente. Se si imposta l'opzione MQCNO , MQCNO_RECONNECT_Q_MGR, non includere gli altri gestori code nello stesso gruppo di gestori code. Il client restituisce un errore se il gestore code a cui si riconnette non è lo stesso gestore code a cui si è connesso.

Gruppi gestore code

È possibile selezionare se l'applicazione client si connette sempre e si riconnette a un gestore code con lo stesso nome, allo stesso gestore code o a uno qualsiasi dei gestori code definiti con lo stesso valore QMNAME nella tabella di connessione client.

- L'attributo *name* del gestore code, QMNAME , nella definizione del canale client è il nome di un gruppo di gestori code.
- Nell'applicazione client, se si imposta il valore del parametro MQCONN o MQCONNX QmgrName su un nome gestore code, il client si connette solo ai gestori code con tale nome. Se si aggiunge un asterisco (*) al nome del gestore code, il client si connette a qualsiasi gestore code nel gruppo di gestori code con lo stesso valore QMNAME . Per una spiegazione completa, consultare Gruppi di gestori code in CCDT.

Gruppi di condivisione code

La riconnessione automatica del client ai gruppi di condivisione code z/OS utilizza gli stessi meccanismi di riconnessione di qualsiasi altro ambiente. Il client si riconnetterà alla stessa selezione di gestori code configurata per la connessione originale. Ad esempio, quando si utilizza la tabella di definizione del canale client, l'amministratore deve verificare che tutte le voci nella tabella si risolvano nello stesso gruppo di condivisione code z/OS .

Definizioni di canali client e server

Le definizioni dei canali client e server definiscono i gruppi di gestori code a cui un'applicazione client può riconnettersi. Le definizioni gestiscono la selezione e la tempistica delle riconnessioni e altri fattori, come la sicurezza; consultare gli argomenti correlati. Gli attributi del canale più rilevanti da considerare per la riconnessione sono elencati in due gruppi:

Attributi di connessione client

Affinità di connessione (AFFINITY)AFFINITY
: Affinità connessione.

Peso del canale client (CLNTWGHT)CLNTWGHT
: Importanza del canale del client.

Nome connessione (CONNAME)CONNAME
: Informazioni di connessione.

Intervallo heartbeat (HBINT)HBINT
: Intervallo heartbeat. Impostare l'intervallo di heartbeat sul canale di connessione server.

Intervallo keepalive (KAINT)KAINT
: Intervallo keepalive. Impostare l'intervallo keepalive sul canale di connessione server.

  Notare che KAINT si applica solo a z/OS .

Nome gestore code (QMNAME)QMNAME
: È il nome del gestore code.

Attributi connessione server

Intervallo heartbeat (HBINT)HBINT
: Intervallo heartbeat. Impostare l'intervallo di heartbeat sul canale di connessione client.

Intervallo keepalive (KAINT)KAINT
: Intervallo keepalive. Impostare l'intervallo keepalive sul canale di connessione client.

  Notare che KAINT si applica solo a z/OS .

KAINT è un heartbeat del livello di rete e HBINT è un heartbeat WebSphere MQ tra il client e il gestore code. L'impostazione di questi heartbeat su un tempo più breve serve a due scopi:

1. Simulando l'attività sulla connessione, il software del livello di rete responsabile della chiusura delle connessioni inattive ha meno probabilità di chiudere la connessione.
2. Se la connessione viene chiusa, il ritardo prima che venga rilevata la connessione interrotta viene abbreviato.

L'intervallo di keepalive TCP/IP predefinito è due ore. Impostare gli attributi KAINT e HBINT su un periodo di tempo più breve. Non presumere che il normale funzionamento di una rete si adatti alle esigenze di riconnessione automatica. Ad esempio, alcuni firewall possono arrestare una connessione TCP/IP inattiva dopo soli 10 minuti.

Connettività di rete

Solo gli errori di rete trasmessi al client WebSphere MQ MQI dalla rete vengono gestiti dalla funzione di riconnessione automatica del client.

- Le riconnessioni eseguite automaticamente dal trasporto sono invisibili a IBM WebSphere MQ.
- L'impostazione HBINT consente di gestire gli errori di rete invisibili a WebSphere MQ.

Gestori code e listener WebSphere MQ

La riconnessione client viene attivata per errore del server, errore del gestore code, errore di connettività di rete e da un amministratore che passa a un'altra istanza del gestore code.

- Se si utilizza un gestore code a più istanze, un'ulteriore causa della riconnessione del client si verifica quando si passa il controllo dall'istanza del gestore code attivo a un'istanza in standby.
- La chiusura di un gestore code utilizzando il comando **endmqm** predefinito non attiva la riconnessione client automatica. Aggiungere l'opzione `-r` sul comando **endmqm** per richiedere la riconnessione automatica del client o l'opzione `-s` per il trasferimento a un'istanza del gestore code in standby dopo la chiusura.

WebSphere MQ Supporto di riconnessione automatica del client MQI

Se si utilizza il supporto per la riconnessione client automatica nel client WebSphere MQ MQI, l'applicazione client si riconnette automaticamente e continua l'elaborazione senza emettere una chiamata MQCONN o MQCONNX MQI per riconnettersi al gestore code.

- La riconnessione automatica del client viene attivata da uno dei seguenti eventi:
  - errore del gestore code
  - terminazione di un gestore code e specifica dell'opzione `-r`, riconnessione, sul comando **endmqm**
- Le opzioni di MQCONNX MQCNO controllano se è stata abilitata la riconnessione automatica del client. Le opzioni sono descritte in Opzioni di riconnessione.
- La riconnessione automatica del client emette chiamate MQI per conto dell'applicazione per ripristinare l'handle di connessione e gli handle per altri oggetti aperti, in modo che il programma possa riprendere la normale elaborazione dopo aver elaborato gli errori MQI risultanti dalla connessione interrotta. Consultare “Ripristino di un client riconnesso automaticamente” a pagina 397.
- Se è stato scritto un programma di uscita del canale per la connessione, l'exit riceve queste chiamate MQI aggiuntive.
- È possibile registrare un gestore eventi di riconnessione, che viene attivato all'inizio e al termine della riconnessione.

Sebbene la riconnessione non richiede più di un minuto, la riconnessione può richiedere più tempo perché un gestore code potrebbe disporre di numerose risorse da gestire. Durante questo periodo, un'applicazione client potrebbe mantenere dei blocchi che non appartengono alle risorse WebSphere MQ . Esiste un valore di timeout che è possibile configurare per limitare il tempo di attesa di un client per la riconnessione. Il valore (in secondi) è impostato nel file `mqclient.ini` .

```
Channels:
    MQReconnectTimeout = 1800
```

Non viene effettuato alcun tentativo di riconnessione dopo la scadenza del timeout. Quando il sistema rileva che il timeout è scaduto, restituisce un errore `MQRC_RECONNECT_FAILED` .

Monitoraggio dei messaggi della console

Ci sono una serie di messaggi informativi emessi dal gestore code o dall'iniziatore di canali che devono essere considerati particolarmente significativi. Questi messaggi non indicano di per sé un problema, ma possono essere utili per la traccia perché indicano un potenziale problema che potenzialmente deve essere risolto.

La presenza di questo messaggio può anche indicare che un'applicazione utente sta inserendo un numero elevato di messaggi nella serie di pagine, che potrebbe essere un sintomo di un problema più grande:

- Un problema con l'applicazione utente che utilizza i messaggi PUT, come un loop non controllato.
- Un'applicazione utente che GET ha i messaggi dalla coda non funziona più.

Utilizzo di WebSphere MQ con configurazioni ad alta disponibilità

Se si desidera utilizzare i gestori code WebSphere MQ in una configurazione HA (High Availability), è possibile impostare i gestori code in modo che funzionino con un gestore HA, come PowerHA per AIX (precedentemente HACMP) o Microsoft Cluster Service (MSCS), o con gestori code a più istanze WebSphere MQ .

È necessario essere consapevoli delle seguenti definizioni di configurazione:

Cluster gestore code
Gruppi di due o più gestori code su uno o più computer, che forniscono l'interconnessione automatica e che consentono la condivisione delle code per il bilanciamento del carico e la ridondanza.

Cluster HA
I cluster HA sono gruppi di due o più computer e risorse come dischi e reti, collegati tra loro e configurati in modo tale che, in caso di errore, un gestore HA (High Availability), come HACMP (UNIX) o MSCS (Windows) esegua un *failover*. Il failover trasferisce i dati di stato delle applicazioni dal computer in errore ad un altro computer nel cluster e ne riavvia l'operazione. Ciò fornisce l'alta disponibilità dei servizi in esecuzione all'interno del cluster HA. La relazione tra cluster IBM WebSphere MQ e cluster HA è descritta in “Relazione tra cluster HA e cluster del gestore code” a pagina 322.

Gestori code a più istanze
Istanze dello stesso gestore code configurate su due o più computer. Avviando più istanze, un'istanza diventa l'istanza attiva e le altre istanze diventano standby. Se l'istanza attiva ha esito negativo, un'istanza in standby in esecuzione su un computer differente prende automaticamente il sopravvento. È possibile utilizzare gestori code a più istanze per configurare i propri sistemi di messaggistica altamente disponibili basati su WebSphere MQ, senza richiedere una tecnologia cluster come HACMP o MSCS. I cluster HA e i gestori code a più istanze sono modi alternativi per rendere i gestori code altamente disponibili. Non combinarli inserendo un gestore code a più istanze in un cluster HA.

Differenze tra gestori code a più istanze e cluster HA

I gestori code a più istanze e i cluster HA sono modi alternativi per ottenere l'elevata disponibilità per i gestori code. Ecco alcuni punti che evidenziano le differenze tra i due approcci.

I gestori code a più istanze includono le seguenti funzioni:

- Supporto failover di base integrato in WebSphere MQ
- Failover più rapido rispetto al cluster HA
- Configurazione e funzionamento semplici
- Integrazione con WebSphere MQ Explorer

Le limitazioni dei gestori code a più istanze includono:

- Storage di rete altamente disponibile e ad alte prestazioni richiesto

- Configurazione di rete più complessa perché il gestore code modifica l'indirizzo IP quando si verifica il failover

I cluster HA includono le seguenti funzioni:

- La capacità di coordinare più risorse, come un server delle applicazioni o un database
- Opzioni di configurazione più flessibili, inclusi i cluster che comprendono più di due nodi
- È possibile eseguire il failover più volte senza l'intervento dell'operatore
- Acquisizione dell'indirizzo IP del gestore code come parte del failover

Le limitazioni dei cluster HA includono:

- Sono richiesti ulteriori acquisti di prodotti e competenze
- I dischi che possono essere commutati tra i nodi del cluster sono obbligatori
- La configurazione dei cluster HA è relativamente complessa
- Il failover è piuttosto lento storicamente, ma i prodotti cluster HA recenti stanno migliorando
- I failover non necessari possono verificarsi se si verificano delle carenze negli script utilizzati per monitorare le risorse, ad esempio i gestori code

Relazione tra cluster HA e cluster del gestore code

I cluster del gestore code riducono l'amministrazione e forniscono il bilanciamento del carico dei messaggi tra le istanze delle code del cluster del gestore code. Inoltre, offrono una disponibilità superiore rispetto a un singolo gestore code poiché, in seguito a un malfunzionamento di un gestore code, le applicazioni di messaggistica possono ancora accedere alle istanze rimanenti di una coda cluster del gestore code. Tuttavia, i cluster del gestore code da soli non forniscono il rilevamento automatico dell'errore del gestore code e l'attivazione automatica del riavvio o del failover del gestore code. I cluster HA forniscono queste funzioni. I due tipi di cluster possono essere utilizzati insieme per un buon effetto.

Utilizzo di WebSphere MQ con cluster ad alta disponibilità su UNIX and Linux

È possibile utilizzare WebSphere MQ con un cluster HA (high availability) su piattaforme UNIX and Linux : ad esempio, PowerHA per AIX (precedentemente HACMP), Veritas Cluster Server, HP Serviceguard o un cluster Red Hat Enterprise Linux con Red Hat Cluster Suite.

Prima di WebSphere MQ Versione 7.0.1, veniva fornito SupportPac MC91 per assistere nella configurazione dei cluster HA. WebSphere MQ Versione 7.0.1 ha fornito un grado di controllo maggiore rispetto alle versioni precedenti su cui i gestori code memorizzano i propri dati. Ciò rende più semplice configurare i gestori code in un cluster HA. La maggior parte degli script forniti con SupportPac MC91 non è più richiesta e SupportPac viene ritirato.

Questa sezione introduce “Configurazioni cluster HA” a pagina 322, la relazione tra i cluster HA e i cluster dei gestori code, “Client WebSphere MQ” a pagina 323e “WebSphere MQ che opera in un cluster HA” a pagina 323e guida l'utente attraverso i passi e fornisce script di esempio che è possibile adattare per configurare i gestori code con un cluster HA.

Fare riferimento alla documentazione del cluster HA specifica per il proprio ambiente per assistenza con i passi di configurazione descritti in questa sezione.

Configurazioni cluster HA

In questa sezione, il termine *nodo* viene utilizzato per fare riferimento all'entità che sta eseguendo un sistema operativo e il software HA; "computer", "sistema" o "macchina" o "partizione" o "blade" potrebbero essere considerati sinonimi in questo utilizzo. È possibile utilizzare WebSphere MQ per configurare le configurazioni di standby o di takeover, incluso il takeover reciproco in cui tutti i nodi cluster eseguono il carico di lavoro WebSphere MQ .

Una configurazione *standby* è la configurazione cluster HA di base in cui un nodo esegue il lavoro mentre l'altro nodo agisce solo come standby. Il nodo standby non esegue il lavoro ed è indicato come inattivo; questa configurazione è talvolta denominata *standby a freddo*. Tale configurazione richiede un alto grado

di ridondanza hardware. Per risparmiare sull'hardware, è possibile estendere questa configurazione per avere più nodi di lavoro con un singolo nodo di standby. Il punto è che il nodo di standby può assumere il controllo del lavoro di qualsiasi altro nodo di lavoro. Questa configurazione è ancora indicata come configurazione standby e a volte come configurazione "N+1".

Una configurazione di *takeover* è una configurazione più avanzata in cui tutti i nodi eseguono del lavoro e il lavoro critico può essere assunto in caso di un errore del nodo.

Una configurazione di *takeover unilaterale* è una configurazione in cui un nodo standby esegue del lavoro aggiuntivo, non critico e non rimovibile. Questa configurazione è simile a una configurazione standby, ma con un lavoro (non critico) eseguito dal nodo standby.

Una configurazione di *takeover reciproco* è una configurazione in cui tutti i nodi eseguono operazioni ad alta disponibilità (mobili). Questo tipo di configurazione del cluster HA è anche a volte indicato come "Attivo / Attivo" per indicare che tutti i nodi stanno elaborando attivamente il carico di lavoro critico.

Con la configurazione di standby estesa o con una delle configurazioni di takeover, è importante considerare il carico di picco che potrebbe essere posizionato su un nodo che può assumere il controllo del lavoro di altri nodi. Tale nodo deve disporre di una capacità sufficiente per mantenere un livello di prestazioni accettabile.

Relazione tra cluster HA e cluster del gestore code

I cluster del gestore code riducono l'amministrazione e forniscono il bilanciamento del carico dei messaggi tra le istanze delle code del cluster del gestore code. Inoltre, offrono una disponibilità superiore rispetto a un singolo gestore code poiché, in seguito a un malfunzionamento di un gestore code, le applicazioni di messaggistica possono ancora accedere alle istanze rimanenti di una coda cluster del gestore code. Tuttavia, i cluster del gestore code da soli non forniscono il rilevamento automatico dell'errore del gestore code e l'attivazione automatica del riavvio o del failover del gestore code. I cluster HA forniscono queste funzioni. I due tipi di cluster possono essere utilizzati insieme per un buon effetto.

Client WebSphere MQ

WebSphere I client MQ che stanno comunicando con un gestore code che potrebbe essere soggetto a un riavvio o a un takeover devono essere scritti per tollerare una connessione interrotta e devono tentare ripetutamente di riconnettersi. WebSphere MQ Versione 7 ha introdotto funzioni nell'elaborazione di CCDT (Client Channel Definition Table) che assistono la disponibilità della connessione e il bilanciamento del carico di lavoro; tuttavia, queste non sono direttamente rilevanti quando si utilizza un sistema di failover.

L'ETC (Extended Transactional Client), che consente a un client WebSphere MQ MQI di partecipare a transazioni a due fasi, deve sempre connettersi allo stesso gestore code. ETC non può utilizzare tecniche come un programma di bilanciamento del carico IP per selezionare da un elenco di gestori code. Quando si utilizza un prodotto HA, un gestore code conserva la sua identità (nome e indirizzo) indipendentemente dal nodo su cui è in esecuzione, in modo che l'ETC possa essere utilizzato con i gestori code che sono sotto il controllo HA.

WebSphere MQ che opera in un cluster HA

Tutti i cluster HA hanno il concetto di un'unità di failover. Questa è una serie di definizioni che contiene tutte le risorse che costituiscono il servizio ad elevata disponibilità. L'unità di failover comprende il servizio stesso e tutte le altre risorse da cui dipende.

Le soluzioni HA utilizzano termini differenti per un'unità di failover:

- In PowerHA per AIX l'unità di failover è denominata *gruppo di risorse*.
- Su Veritas Cluster Server è noto come *gruppo di servizio*.
- Su Serviceguard viene chiamato *pacchetto*.

Questo argomento usa il termine *gruppo di risorse* per indicare un'unità di failover.

L'unità di failover più piccola per WebSphere MQ è un gestore code. Generalmente, il gruppo di risorse che contiene il gestore code contiene anche dischi condivisi in un gruppo di volumi o in un gruppo di dischi riservato esclusivamente per l'utilizzo da parte del gruppo di risorse e l'indirizzo IP utilizzato per la connessione al gestore code. È inoltre possibile includere altre risorse WebSphere MQ , come un listener o un controllo trigger nello stesso gruppo di risorse, come risorse separate o sotto il controllo del gestore code stesso.

Un gestore code che deve essere utilizzato in un cluster HA deve avere i propri dati e log sui dischi condivisi tra i nodi nel cluster. Il cluster HA garantisce che solo un nodo alla volta possa scrivere sui dischi. Il cluster HA può utilizzare uno script di controllo per monitorare lo stato del gestore code.

È possibile utilizzare un singolo disco condiviso sia per i dati che per i log correlati al gestore code. Tuttavia, è normale utilizzare file system condivisi separati in modo che possano essere ridimensionati e ottimizzati in modo indipendente.

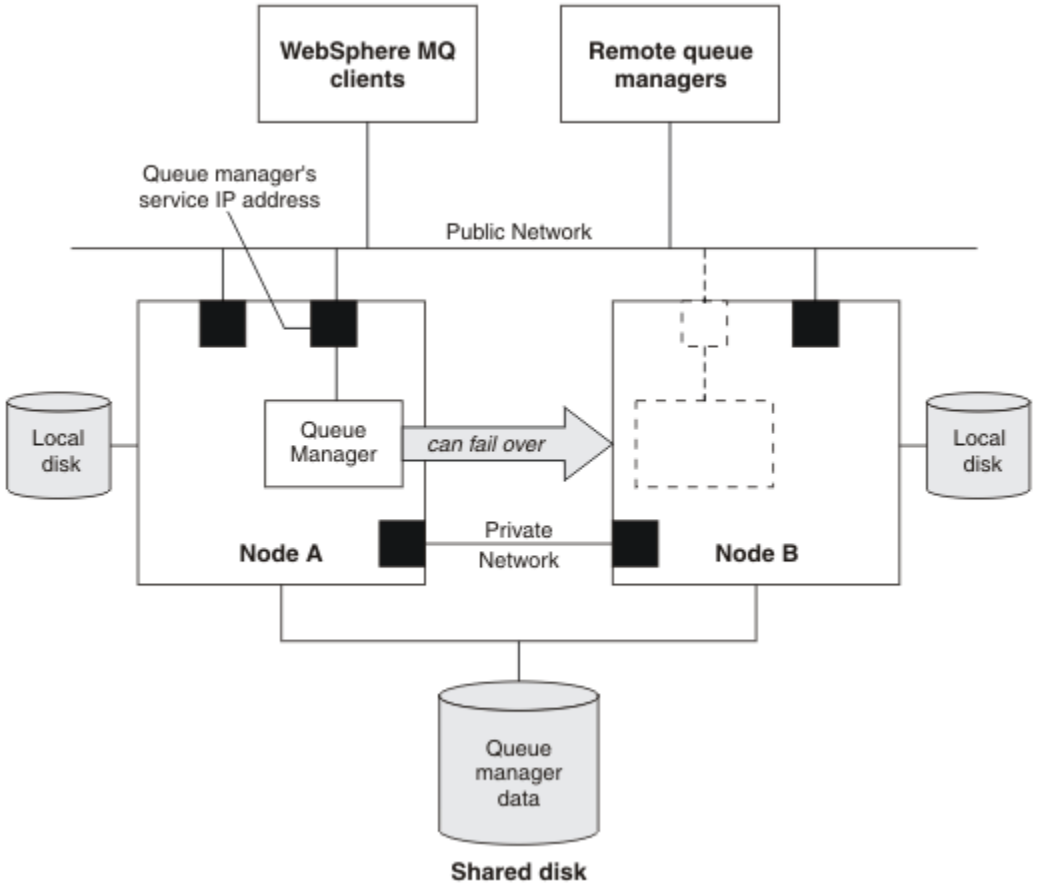


Figura 60. Cluster HA

La Figura 1 illustra un cluster HA con due nodi. Il cluster HA sta gestendo la disponibilità di un gestore code che è stato definito in un gruppo di risorse. Si tratta di una configurazione attiva / passiva o di standby a freddo, poiché solo un nodo, il nodo A, sta attualmente eseguendo un gestore code. Il gestore code è stato creato con dati e file di log su un disco condiviso. Il gestore code ha un indirizzo IP del servizio che è anche gestito dal cluster HA. Il gestore code dipende dal disco condiviso e dall'indirizzo IP del servizio. Quando il cluster HA riporta un errore sul gestore code dal nodo A al nodo B, sposta prima le risorse dipendenti del gestore code sul nodo B, quindi avvia il gestore code.

Se il cluster HA contiene più di un gestore code, la configurazione del cluster HA potrebbe comportare l'esecuzione di due o più gestori code sullo stesso nodo dopo un failover. A ogni gestore code nel cluster HA deve essere assegnato il suo proprio numero di porta, che utilizza su qualsiasi nodo cluster che sia attivo in un determinato momento.

Generalmente, il cluster HA viene eseguito come utente root. WebSphere MQ viene eseguito come utente mqm. La gestione di WebSphere MQ è concessa ai membri del gruppo mq. Verificare che l'utente e il gruppo mqm esistano entrambi su tutti i nodi cluster HA. L'ID utente e l'ID gruppo devono essere congruenti nel cluster. L'amministrazione di WebSphere MQ da parte dell'utente root non è consentita; gli script che avviano, arrestano o monitorano gli script devono passare all'utente mqm.

Nota: WebSphere MQ deve essere installato correttamente su tutti i nodi; non è possibile condividere file eseguibili del prodotto.

Configurazione dei dischi condivisi

Un gestore code WebSphere MQ in un cluster HA richiede che i file di dati e i file di log si trovino in file system remoti denominati comuni su un disco condiviso.

Per configurare i dischi condivisi, completare la seguente procedura:

1. Decidere i nomi dei punti di montaggio per i filesystem del gestore code. Ad esempio, `/MQHA/qmgrname/data` per i file di dati del gestore code e `/MQHA/qmgrname/log` per i relativi file di log.
2. Creare un gruppo di volumi (o un gruppo di dischi) per contenere i dati del gestore code e i file di log. Questo gruppo di volume è gestito da un cluster HA (High Availability) nello stesso gruppo di risorse del gestore code.
3. Creare i file system per i dati del gestore code e i file di log nel gruppo volumi.
4. Per ogni nodo a turno, creare i punti di montaggio per i filesystem e assicurarsi che i filesystem possano essere montati. L'utente mqm deve possedere i punti di montaggio.

La Figura 1 mostra un layout possibile per un gestore code in un cluster HA. I dati del gestore code e le directory di log si trovano entrambi sul disco condiviso montato su /MQHA/QM1. Questo disco viene commutato tra i nodi del cluster HA quando si verifica il failover in modo che i dati siano disponibili ovunque venga riavviato il gestore code. Il file `mqs.ini` ha una stanza per il gestore code QM1 . La stanza Log nel file `qm.ini` ha un valore per LogPath.

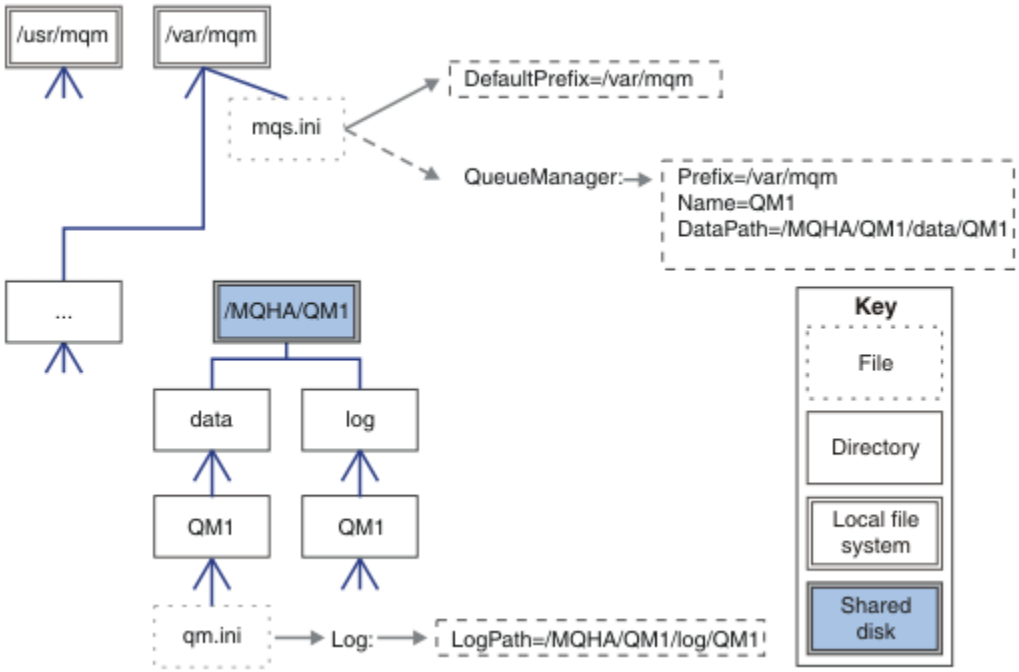


Figura 61. Directory `data` e `log` denominate condivise

Creazione di un gestore code da utilizzare in un cluster HA (High Availability)

Il primo passo per utilizzare un gestore code in un cluster ad alta disponibilità consiste nel creare il gestore code su uno dei nodi.

Per creare un gestore code da utilizzare in un cluster HA, selezionare uno dei nodi nel cluster su cui creare il gestore code. Su questo nodo completare la procedura riportata di seguito:

1. Montare i file system del gestore code sul nodo.
2. Creare il gestore code utilizzando il comando **crtmqm** . Ad esempio:

   ```
   crtmqm -md /MQHA/qmgrname/data -ld /MQHA/qmgrname/log qmgrname
   ```

3. Avviare manualmente il gestore code utilizzando il comando **strmqm** .
4. Completare qualsiasi configurazione iniziale del gestore code, ad esempio la creazione di code e canali e l'impostazione del gestore code per avviare automaticamente un listener all'avvio del gestore code.
5. Arrestare il gestore code utilizzando il comando **endmqm** .
6. Utilizzare il comando **dspmqinf** per visualizzare il comando **addmqinf** che è possibile utilizzare in un'attività successiva, documentata in "Aggiunta delle informazioni di configurazione del gestore code ad altri nodi in un cluster HA (High Availability)" a pagina 326:

   ```
   dspmqinf -o command qmgrname
   ```

   dove `qmgrname` è il nome del gestore code.
7. Il comando **addmqinf** visualizzato sarà simile al seguente esempio:

   ```
   addmqinf -sQueueManager -vName=qmgrname -vDirectory=qmgrname \
            -vPrefix=/var/mqm -vDataPath=/MQHA/qmgrname/data/qmgrname
   ```

   Prendere nota del comando visualizzato.
8. Smontare i filesystem del gestore code.

Si è ora pronti a completare i passi descritti in "Aggiunta delle informazioni di configurazione del gestore code ad altri nodi in un cluster HA (High Availability)" a pagina 326.

Aggiunta delle informazioni di configurazione del gestore code ad altri nodi in un cluster HA (High Availability)

È necessario aggiungere la configurazione del gestore code agli altri nodi nel cluster HA.

Prima di completare questa attività, è necessario aver completato i passi in "Creazione di un gestore code da utilizzare in un cluster HA (High Availability)" a pagina 325.

Per aggiungere le informazioni di configurazione per il gestore code a ciascuno degli altri nodi nel cluster HA, completare la seguente procedura su ognuno degli altri nodi:

1. Montare i filesystem del gestore code.
2. Aggiungere le informazioni di configurazione del gestore code al nodo, modificando direttamente `/var/mqm/mqs.ini` o immettendo il comando **addmqinf** visualizzato dal comando **dspmqinf** nei passi 6 e 7 in "Creazione di un gestore code da utilizzare in un cluster HA (High Availability)" a pagina 325.
3. Avviare e arrestare il gestore code per verificare la configurazione.

   I comandi utilizzati per avviare e arrestare il gestore code devono essere emessi dalla stessa installazione IBM WebSphere MQ del comando **addmqinf** . Per avviare e arrestare il gestore code da una installazione diversa, è necessario prima impostare l'installazione associata al gestore code utilizzando il comando **setmqm** . Per ulteriori informazioni, vedere setmqm.
4. Smontare i filesystem del gestore code.

Avvio di un gestore code sotto il controllo di un cluster HA (High Availability)

Il gestore code è rappresentato nel cluster HA come risorsa. Il cluster HA deve essere in grado di avviare e arrestare il gestore code. Nella maggior parte dei casi, è possibile utilizzare uno script shell per avviare il gestore code. È necessario rendere questi script disponibili nella stessa ubicazione su tutti i nodi nel cluster, utilizzando un file system di rete o copiandoli su ciascuno dei dischi locali.

Nota: Prima di riavviare un gestore code non riuscito, è necessario disconnettere le applicazioni da tale istanza del gestore code. In caso contrario, il gestore code potrebbe non essere riavviato correttamente.

Di seguito sono riportati esempi di script shell adatti. Puoi personalizzarli in base alle tue esigenze e utilizzarli per avviare il gestore code sotto il controllo del tuo cluster HA.

Il seguente script di shell è un esempio di come passare dall'utente cluster HA all'utente mqm in modo che il gestore code possa essere correttamente avviato:

```
#!/bin/ksh

# A simple wrapper script to switch to the mqm user.

su mqm -c name_of_your_script $*
```

Il seguente script di shell è un esempio di come avviare un gestore code senza fare supposizioni sullo stato corrente del gestore code. Si noti che utilizza un metodo estremamente brusco per terminare i processi che appartengono al gestore code:

```
#!/bin/ksh
#
# This script robustly starts the queue manager.
#
# The script must be run by the mqm user.

# The only argument is the queue manager name. Save it as QM variable
QM=$1

if [ -z "$QM" ]
then
  echo "ERROR! No queue manager name supplied"
  exit 1
fi

# End any queue manager processes which might be running.

srchstr="( |-m)$QM *.*$"
for process in amqzmuc0 amqzxma0 amqfcxba amqfqpub amqpcsea amqzlaa0 \
               amqzlsa0 runmqchi runmqlsr amqcrsta amqrrmfa amqrmppa \
               amqzfuma amqzdmaa amqzmuf0 amqzmur0 amqzmgr0
 do
  ps -ef | tr "\t" " " | grep $process | grep -v grep | \
    egrep "$srchstr" | awk '{print $2}'| \
       xargs kill -9 > /dev/null 2>&1
done

# It is now safe to start the queue manager.
# The strmqm command does not use the -x flag.
strmqm ${QM}
```

È possibile modificare lo script per avviare altri programmi correlati.

Arresto di un gestore code sotto il controllo di un cluster HA (High Availability)

Nella maggior parte dei casi, è possibile utilizzare uno script di shell per arrestare un gestore code. Di seguito sono riportati esempi di script shell adatti. Puoi personalizzarli in base alle tue esigenze e utilizzarli per arrestare il gestore code sotto il controllo del tuo cluster HA.

Il seguente script è un esempio di come arrestarsi immediatamente senza fare supposizioni sullo stato corrente del gestore code. Lo script deve essere eseguito dall'utente mqm; potrebbe quindi essere necessario racchiudere questo script in uno script della shell per passare dall'utente del cluster HA a mqm (uno script della shell di esempio viene fornito in “Avvio di un gestore code sotto il controllo di un cluster HA (High Availability)” a pagina 326):

```
#!/bin/ksh
#
# The script ends the QM by using two phases, initially trying an immediate
# end with a time-out and escalating to a forced stop of remaining
# processes.
#
# The script must be run by the mqm user.
#
# There are two arguments: the queue manager name and a timeout value.
QM=$1
TIMEOUT=$2
```

```
if [ -z "$QM" ]
then
  echo "ERROR! No queue manager name supplied"
  exit 1
fi

if [ -z "$TIMEOUT" ]
then
  echo "ERROR! No timeout specified"
  exit 1
fi

for severity in immediate brutal
do
  # End the queue manager in the background to avoid
  # it blocking indefinitely. Run the TIMEOUT timer
  # at the same time to interrupt the attempt, and try a
  # more forceful version. If the brutal version fails,
  # nothing more can be done here.

  echo "Attempting ${severity} end of queue manager '${QM}'"
  case $severity in

  immediate)
    # Minimum severity of endmqm is immediate which severs connections.
    # HA cluster should not be delayed by clients
    endmqm -i ${QM} &
    ;;

  brutal)
    # This is a forced means of stopping queue manager processes.

    srchstr="( |-m)$QM *.*$"
    for process in amqzmuc0 amqzxma0 amqfcxba amqfqpub amqpcsea amqzlaa0 \
                amqzlsa0 runmqchi runmqlsr amqcrsta amqrrmfa amqrmppa \
                amqzfuma amqzdmaa amqzmuf0 amqzmur0 amqzmgr0
    do
      ps -ef | tr "\t" " " | grep $process | grep -v grep | \
         egrep "$srchstr" | awk '{print $2}'| \
            xargs kill -9 > /dev/null 2>&1
    done

  esac

  TIMED_OUT=yes
  SECONDS=0
  while (( $SECONDS < ${TIMEOUT} ))
  do
   TIMED_OUT=yes
   i=0
   while [ $i -lt 5 ]
   do
     # Check for execution controller termination
     srchstr="( |-m)$QM *.*$"
     cnt=`ps -ef | tr "\t" " " | grep amqzxma0 | grep -v grep | \
       egrep "$srchstr" | awk '{print $2}' | wc -l `
     i=`expr $i + 1`
     sleep 1
     if [ $cnt -eq 0 ]
     then
       TIMED_OUT=no
       break
     fi
   done

   if [ ${TIMED_OUT} = "no" ]
   then
     break
   fi

   echo "Waiting for ${severity} end of queue manager '${QM}'"
   sleep 1
  done # timeout loop

  if [ ${TIMED_OUT} = "yes" ]
  then
    continue        # to next level of urgency
  else
    break           # queue manager is ended, job is done
  fi
```

```
done # next phase
```

Monitoraggio di un gestore code

Generalmente, il cluster HA (High Availability) può monitorare periodicamente lo stato del gestore code. Nella maggior parte dei casi, è possibile utilizzare uno script di shell per questo. Di seguito sono riportati esempi di script shell adatti. È possibile personalizzare questi script in base alle proprie esigenze e utilizzarli per effettuare ulteriori controlli di monitoraggio specifici per il proprio ambiente.

Da WebSphere MQ versione 7.1, è possibile che più installazioni di WebSphere MQ coesistano su un sistema. Per ulteriori informazioni su più installazioni, consultare Più installazioni. Se si intende utilizzare lo script di monitoraggio su più installazioni, incluse le installazioni alla versione 7.1o superiore, potrebbe essere necessario eseguire alcune operazioni aggiuntive. Se si dispone di un'installazione primaria o si utilizza lo script con versioni precedenti alla versione 7.1, non è necessario specificare*MQ_INSTALLATION_PATH* per utilizzare lo script. In caso contrario, la seguente procedura garantisce che *MQ_INSTALLATION_PATH* venga identificato in modo corretto:

1. Utilizzare il comando **crtmqenv** da un'istallazione della versione 7.1 per identificare il corretto *MQ_INSTALLATION_PATH* per un gestore code:

   ```
   crtmqenv -m qmname
   ```

   Questo comando restituisce il valore *MQ_INSTALLATION_PATH* corretto per il gestore code specificato da *qmname*.
2. Eseguire lo script di monitoraggio con i parametri *qmname* e *MQ_INSTALLATION_PATH* appropriati.

Nota: PowerHA per AIX non fornisce un modo per fornire un parametro al programma di controllo per il gestore code. È necessario creare un programma di monitoraggio separato per ogni gestore code, che incapsula il nome del gestore code. Di seguito è riportato un esempio di script utilizzato su AIX per incapsulare il nome del gestore code:

```
#!/bin/ksh
su mqm -c name_of_monitoring_script qmname MQ_INSTALLATION_PATH
```

dove *MQ_INSTALLATION_PATH* è un parametro facoltativo che specifica il percorso di installazione di IBM WebSphere MQ a cui è associato il gestore code *qmname* .

Il seguente script non è valido per la possibilità che **runmqsc** si blocchi. In genere, i cluster HA trattano uno script di monitoraggio in sospeso come un errore e sono essi stessi robusti a questa possibilità.

Tuttavia, lo script tollera che il gestore code si trovi nello stato di avvio. Ciò è dovuto al fatto che è comune per il cluster HA avviare il monitoraggio del gestore code non appena viene avviato. Alcuni cluster HA distinguono tra una fase di avvio e una fase di esecuzione per le risorse, ma è necessario configurare la durata della fase di avvio. Poiché il tempo impiegato per avviare un gestore code dipende dalla quantità di lavoro che deve eseguire, è difficile scegliere il tempo massimo impiegato per avviare un gestore code. Se si sceglie un valore troppo basso, il cluster HA assume erroneamente che il gestore code abbia avuto esito negativo quando non è stato completato l'avvio. Ciò potrebbe causare una sequenza infinita di failover.

Questo script deve essere eseguito dall'utente mqm; potrebbe quindi essere necessario racchiudere questo script in uno script shell per passare l'utente dall'utente del cluster HA a mqm (uno script shell di esempio viene fornito in “Avvio di un gestore code sotto il controllo di un cluster HA (High Availability)” a pagina 326):

```
#!/bin/ksh
#
# This script tests the operation of the queue manager.
#
# An exit code is generated by the runmqsc command:
# 0  => Either the queue manager is starting or the queue manager is running and responds.
#       Either is OK.
# >0 => The queue manager is not responding and not starting.
#
# This script must be run by the mqm user.
QM=$1
MQ_INSTALLATION_PATH=$2
```

```
if [ -z "$QM" ]
then
  echo "ERROR! No queue manager name supplied"
  exit 1
fi

if [ -z "$MQ_INSTALLATION_PATH" ]
then
  # No path specified, assume system primary install or MQ level < 7.1.0.0
  echo "INFO: Using shell default value for MQ_INSTALLATION_PATH"
else
  echo "INFO: Prefixing shell PATH variable with $MQ_INSTALLATION_PATH/bin"
  PATH=$MQ_INSTALLATION_PATH/bin:$PATH
fi

# Test the operation of the queue manager. Result is 0 on success, non-zero on error.
echo "ping qmgr" | runmqsc ${QM} > /dev/null 2>&1
pingresult=$?

if [ $pingresult -eq 0 ]
then # ping succeeded

  echo "Queue manager '${QM}' is responsive"
  result=0

else # ping failed

  # Don't condemn the queue manager immediately, it might be starting.
  srchstr="( |-m)$QM *.*$"
  cnt=`ps -ef | tr "\t" " " | grep strmqm | grep "$srchstr" | grep -v grep \
                | awk '{print $2}' | wc -l`
  if [ $cnt -gt 0 ]
  then
    # It appears that the queue manager is still starting up, tolerate
    echo "Queue manager '${QM}' is starting"
    result=0
  else
    # There is no sign of the queue manager starting
    echo "Queue manager '${QM}' is not responsive"
    result=$pingresult
  fi

fi

exit $result
```

Inserimento del gestore code sotto il controllo del cluster HA (High Availability)

È necessario configurare il gestore code, sotto il controllo del cluster HA, con l'indirizzo IP del gestore code e i dischi condivisi.

Per definire un gruppo di risorse in modo che contenga il gestore code e tutte le risorse associate, completare la seguente procedura:

1. Creare il gruppo di risorse contenente il gestore code, il volume del gestore code o il gruppo di dischi e l'indirizzo IP del gestore code. L'indirizzo IP è un indirizzo IP virtuale, non l'indirizzo IP del computer.
2. Verificare che il cluster HA commuta correttamente le risorse tra i nodi del cluster e che sia pronto a controllare il gestore code.

Eliminazione di un gestore code da un nodo cluster HA (High Availability)

Si potrebbe voler rimuovere un gestore code da un nodo che non è più richiesto per eseguire il gestore code.

Per rimuovere il gestore code da un nodo in un cluster HA, completare la seguente procedura:

1. Rimuovere il nodo dal cluster HA in modo che il cluster HA non tenterà più di attivare il gestore code su questo nodo.
2. Utilizzare il seguente comando **rmvmqinf** per eliminare le informazioni di configurazione del gestore code:

   rmvmqinf *qmgrname*

Per eliminare completamente il gestore code, utilizzare il comando **dltmqm** . Tuttavia, tenere presente che ciò elimina completamente i file di log e i dati del gestore code. Una volta eliminato il gestore code, è possibile utilizzare il comando **rmvmqinf** per rimuovere le restanti informazioni di configurazione dagli altri nodi.

Supporto di Microsoft Cluster Service (MSCS)

Introduzione e configurazione di MSCS per supportare il failover di server virtuali.

Queste informazioni si applicano solo a WebSphere MQ per Finestre .

MSCS (Microsoft Cluster Service) consente di collegare i server in *cluster*, fornendo una maggiore disponibilità di dati e applicazioni e semplificando la gestione del sistema. MSCS è in grado di rilevare e ripristinare automaticamente gli errori del server o dell'applicazione.

MSCS supporta il *failover* di *server virtuale*, che corrispondono ad applicazioni, siti Web, code di stampa o condivisioni file (inclusi, ad esempio, i relativi mandrini del disco, i file e gli indirizzi IP).

Failover è il processo mediante il quale MSCS rileva un malfunzionamento in un'applicazione su un computer nel cluster e arresta l'applicazione interrotta in modo ordinato, trasferisce i relativi dati di stato sull'altro computer e reinizializza l'applicazione.

Questa sezione introduce i cluster MSCS e descrive l'impostazione del supporto MSCS nelle seguenti sezioni:

- “Introduzione ai cluster MSCS” a pagina 331
- “Impostazione di IBM WebSphere MQ per il clustering MSCS” a pagina 332

Quindi indica come configurare WebSphere MQ per il clustering MSCS, nelle seguenti sezioni:

- “Creazione di un gestore code da utilizzare con MSCS” a pagina 334
- “Spostamento di un gestore code nella memoria MSCS” a pagina 335
- “Inserimento di un gestore code sotto il controllo di MSCS” a pagina 336
- “Rimozione di un gestore code dal controllo MSCS” a pagina 343

Inoltre, fornisce alcuni utili suggerimenti sull'utilizzo di MSCS con WebSphere MQe dettagli sui programmi di utilità di supporto WebSphere MQ MSCS, nelle seguenti sezioni:

- “Suggerimenti e consigli sull'utilizzo di MSCS” a pagina 344
- “Programmi di utilità di supporto MSCS IBM WebSphere MQ” a pagina 347

Introduzione ai cluster MSCS

I cluster MSCS sono gruppi di due o più computer, collegati tra loro e configurati in modo tale che, in caso di errore, MSCS esegua un *failover*, trasferendo i dati di stato delle applicazioni dal computer in errore a un altro computer nel cluster e inizializzando di nuovo l'operazione.

“Utilizzo di WebSphere MQ con configurazioni ad alta disponibilità” a pagina 321 contiene un confronto tra cluster MSCS, gestori code a più istanze e cluster WebSphere MQ .

In questa sezione e nei relativi argomenti subordinati, il termine *cluster*, se utilizzato da solo, **sempre** indica un cluster MSCS. Questo è diverso da un cluster WebSphere MQ descritto altrove in questa guida.

Un cluster a due macchine comprende due computer (ad esempio, A e B) che sono collegati insieme ad una rete per l'accesso client utilizzando un *indirizzo IP virtuale*. Possono anche essere connessi tra loro da una o più reti private. A e B condividono almeno un disco per le applicazioni server da utilizzare. Esiste anche un altro disco condiviso, che deve essere un array ridondante di dischi indipendenti (*RAID*) livello 1, per l'uso esclusivo di MSCS; questo è noto come disco *quorum* . MSCS controlla entrambi i computer per verificare che l'hardware e il software siano in esecuzione correttamente.

In una configurazione semplice come questa, entrambi i computer dispongono di tutte le applicazioni installate, ma solo il computer A viene eseguito con applicazioni attive; il computer B è solo in esecuzione e in attesa. Se il computer A rileva uno qualsiasi dei problemi, MSCS arresta l'applicazione interrotta in modo ordinato, trasferisce i suoi dati di stato all'altro computer e reinizializza l'applicazione. Questo

è noto come *failover*. Le applicazioni possono essere rese *cluster - aware* in modo da interagire completamente con MSCS e failover.

Una configurazione tipica per un cluster a due computer è quella illustrata in Figura 62 a pagina 332.

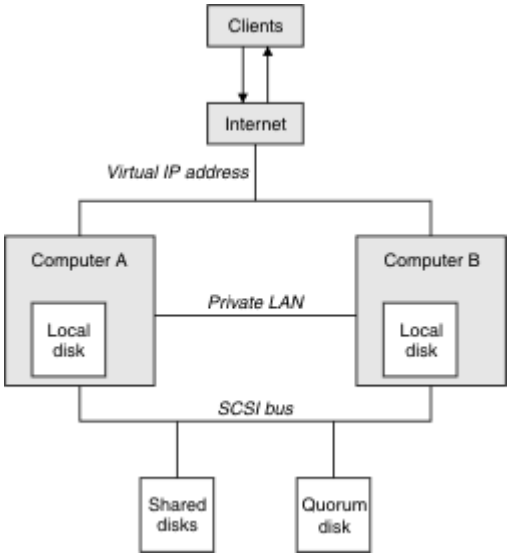


Figura 62. cluster MSCS a due computer

Ogni computer può accedere al disco condiviso, ma solo uno alla volta, sotto il controllo di MSCS. In caso di failover, MSCS cambia l'accesso all'altro computer. Il disco condiviso è di solito un RAID, ma non è necessario.

Ogni computer è collegato alla rete esterna per l'accesso client, e ognuno ha un indirizzo IP. Tuttavia, un client esterno, che comunica con questo cluster, è a conoscenza di un solo *indirizzo IP virtuale*e MSCS instrada il traffico IP all'interno del cluster in modo appropriato.

MSCS esegue anche le proprie comunicazioni tra i due computer, su una o più connessioni private o sulla rete pubblica, ad esempio per monitorare i loro stati utilizzando l'heartbeat e per sincronizzarne i database.

Impostazione di IBM WebSphere MQ per il clustering MSCS

Configurare IBM WebSphere MQ per il cluster rendendo il gestore code l'unità di failover in MSCS. Definire un gestore code come una risorsa per MSCS, che può quindi monitorarlo e trasferirlo su un altro computer nel cluster se si verifica un problema.

Per impostare il sistema, si inizia installando IBM WebSphere MQ su ogni computer del cluster.

Poiché il gestore code è associato con il nome di installazione IBM WebSphere MQ , il nome di installazione di IBM WebSphere MQ su tutti i computer nel cluster deve essere lo stesso. Consultare Installazione e disinstallazione.

I gestori code stessi devono esistere solo sul computer su cui vengono creati. In caso di failover, MSCS avvia i gestori code sull'altro computer. I gestori code, tuttavia, devono avere i propri file di log e di dati su un disco condiviso del cluster e non su un'unità locale. Se si dispone già di un gestore code installato su un'unità locale, è possibile migrarlo utilizzando uno strumento fornito con IBM WebSphere MQ; consultare “Spostamento di un gestore code nella memoria MSCS” a pagina 335. Se si desidera creare nuovi gestori code da utilizzare con MSCS, fare riferimento a “Creazione di un gestore code da utilizzare con MSCS” a pagina 334.

Dopo l'installazione e la migrazione, utilizzare MSCS Cluster Administrator per rendere MSCS consapevole dei gestori code; consultare “Inserimento di un gestore code sotto il controllo di MSCS” a pagina 336.

Se si decide di rimuovere un gestore code dal controllo MSCS, utilizzare la procedura descritta in “Rimozione di un gestore code dal controllo MSCS” a pagina 343.

Imposta simmetria
Quando un'applicazione passa da un nodo all'altro, deve comportarsi nello stesso modo, indipendentemente dal nodo. Il modo migliore per garantire ciò è rendere gli ambienti identici.

Se è possibile, impostare un cluster con hardware, software del sistema operativo, software del prodotto e configurazione identici su ciascun computer. In particolare, verificare che tutto il software richiesto installato sui due computer sia identico in termini di versione, livello di manutenzione, SupportPacs, percorsi ed uscite e che sia presente uno spazio dei nomi comune (ambiente di sicurezza) come descritto in “Sicurezza MSCS” a pagina 333.

Sicurezza MSCS
Per una corretta sicurezza MSCS, seguire queste linee guida.

Le linee guida sono le seguenti:

- Accertarsi di disporre di installazioni software identiche su ciascun computer del cluster.
- Crea uno spazio dei nomi comune (ambiente di sicurezza) nel cluster.
- Creare i nodi dei membri del cluster MSCS di un dominio, all'interno dei quali l'account utente *proprietario cluster* è un account dominio.
- Creare gli altri account utente sul cluster anche gli account di dominio, in modo che siano disponibili su entrambi i nodi. Questo è automaticamente il caso se si dispone già di un dominio e gli account rilevanti per WebSphere MQ sono account di dominio. Se al momento non si dispone di un dominio, prendere in considerazione la configurazione di un *mini - dominio* per soddisfare i nodi cluster e gli account pertinenti. Il vostro scopo è quello di rendere il vostro cluster di due computer come una singola risorsa di calcolo.

  Tenere presente che un account locale su un computer non esiste sull'altro. Anche se si crea un account con lo stesso nome sull'altro computer, il relativo SID (security identifier) è diverso, in modo che, quando l'applicazione viene spostata sull'altro nodo, le autorizzazioni non esistono su tale nodo.

Durante un failover o uno spostamento, il supporto MSCS di WebSphere MQ garantisce che tutti i file che contengono oggetti del gestore code abbiano autorizzazioni equivalenti sul nodo di destinazione. In modo esplicito, il codice verifica che gli amministratori e i gruppi mqm e l'account SYSTEM abbiano il controllo completo e che, se `Everyone` disponeva dell'accesso in lettura sul vecchio nodo, tale autorizzazione venga aggiunta sul nodo di destinazione.

È possibile utilizzare un account di dominio per eseguire il proprio servizio WebSphere MQ . Assicurarsi che esista nel gruppo mqm locale su ciascun computer nel cluster.

Utilizzo di più gestori code con MSCS
Se si sta eseguendo più di un gestore code su un computer, è possibile scegliere una di queste configurazioni.

Le configurazioni sono le seguenti:

- Tutti i gestori code in un singolo gruppo. In questa configurazione, se si verifica un problema con un qualsiasi gestore code, tutti i gestori code nel gruppo eseguano il failover sull'altro computer come un gruppo.
- Un singolo gestore code in ogni gruppo. In questa configurazione, se si verifica un problema con il gestore code, da solo esegue il failover sull'altro computer senza influire sugli altri gestori code.
- Una miscela delle prime due configurazioni.

Modalità cluster
Esistono due modalità in cui è possibile eseguire un sistema cluster con WebSphere MQ: Attivo / Passivo o Attivo / Attivo.

Nota: Se si utilizza MSCS insieme a Microsoft Transaction Server (COM +), non è possibile utilizzare la modalità Attiva / Attiva.

Modalità attiva / passiva

In modalità Attiva / Passiva, il computer A ha l'applicazione in esecuzione su di esso e il computer B è il backup, utilizzato solo quando MSCS rileva un problema.

È possibile utilizzare questa modalità con un solo disco condiviso, ma, se un'applicazione causa un failover, **tutte** le applicazioni devono essere trasferite come un gruppo (poiché solo un computer può accedere al disco condiviso alla volta).

È possibile configurare MSCS con A come computer *preferito* . Quindi, quando il computer A è stato riparato o sostituito e funziona di nuovo correttamente, MSCS lo rileva e ripassa automaticamente l'applicazione al computer A.

Se si esegue più di un gestore code, considerare la possibilità di avere un disco condiviso separato per ciascuno di essi. Quindi, inserire ciascun gestore code in un gruppo separato in MSCS. In questo modo, qualsiasi gestore code può eseguire il failover sull'altro computer senza influire sugli altri gestori code.

Modalità Attiva / Attiva

In modalità Attiva / Attiva, i computer A e B hanno entrambe applicazioni in esecuzione e i gruppi su ciascun computer sono impostati per utilizzare l'altro computer come backup. Se viene rilevato un errore sul computer A, MSCS trasferisce i dati di stato sul computer B e reinizializza l'applicazione. computer B esegue quindi la propria applicazione e quella di A.

Per questa configurazione sono necessari almeno due dischi condivisi. È possibile configurare MSCS con A come computer preferito per le applicazioni di A e B come computer preferito per le applicazioni di B. Dopo il failover e la riparazione, ogni applicazione finisce automaticamente sul proprio computer.

Per WebSphere MQ , ciò significa che è possibile, ad esempio, eseguire due gestori code, uno su ciascuno di A e B, ciascuno dei quali sfrutta appieno la potenza del proprio computer. Dopo un errore sul computer A, entrambi i gestori code verranno eseguiti sul computer B. Ciò significa condividere la potenza di un computer, con una capacità ridotta di elaborare grandi quantità di dati a velocità. Tuttavia, le applicazioni critiche saranno ancora disponibili mentre si trova e si ripara l'errore su A.

Creazione di un gestore code da utilizzare con MSCS

Questa procedura garantisce che un nuovo gestore code venga creato in modo da essere adatto per la preparazione e l'inserimento sotto il controllo di MSCS.

Si inizia creando il gestore code con tutte le relative risorse su un'unità locale, quindi si migrano i file di log e i file di dati su un disco condiviso. (È possibile invertire questa operazione.) **Non** tentare di creare un gestore code con le relative risorse su un'unità condivisa.

È possibile creare un gestore code da utilizzare con MSCS in due modi, da un prompt dei comandi o in WebSphere MQ Explorer. Il vantaggio di utilizzare un prompt dei comandi è che il gestore code viene creato *arrestato* e impostato su *avvio manuale*, che è pronto per MSCS. (Esplora risorse di IBM WebSphere MQ avvia automaticamente un nuovo gestore code e lo imposta sull'avvio automatico dopo la creazione. Devi cambiare questo.)

Creazione di un gestore code da un prompt dei comandi

Attenersi alla seguente procedura per creare un gestore code da un prompt dei comandi, da utilizzare con MSCS:

1. Assicurarsi che la variabile di ambiente `MQSPREFIX` sia impostata per fare riferimento a un'unità locale, ad esempio `C:\WebSphere MQ`. Se si modifica, riavviare la macchina in modo che l'account di sistema acquisisca la modifica. Se non si imposta la variabile, il gestore code viene creato nella directory predefinita WebSphere MQ per i gestori code.

2. Creare il gestore code utilizzando il comando **crtmqm** . Ad esempio, per creare un gestore code denominato `mscs_test` nella directory predefinita, utilizzare:

```
crtmqm mscs_test
```

3. Procedere con "Spostamento di un gestore code nella memoria MSCS" a pagina 335.

Creazione di un gestore code mediante WebSphere MQ Explorer

Attenersi alla seguente procedura per creare un gestore code utilizzando IBM WebSphere MQ Explorer, da utilizzare con MSCS:

1. Avviare IBM WebSphere MQ Explorer dal menu Start.
2. Nella vista Navigator , espandere i nodi della struttura ad albero per trovare il nodo della struttura ad albero `Queue Managers` .
3. Fare clic con il pulsante destro del mouse sul nodo della struttura ad albero `Queue Managers` e selezionare `New->Queue Manager`. Viene visualizzato il pannello Crea gestore code.
4. Completare la finestra (passo 1), quindi fare clic su `Next>`.
5. Completare la dialogo (Passo 2), quindi fare clic su `Next>`.
6. Completare la finestra di dialogo (Passo 3), verificando che `Start Queue Manager` e `Create Server Connection Channel` non siano selezionati, quindi fare clic su `Next>`.
7. Completare la finestra di dialogo (passo 4), quindi fare clic su `Finish`.
8. Procedere con "Spostamento di un gestore code nella memoria MSCS" a pagina 335.

Spostamento di un gestore code nella memoria MSCS

Questa procedura configura un gestore code esistente per renderlo adatto per l'inserimento sotto il controllo MSCS.

A tale scopo, spostare i file di log e i file di dati su dischi condivisi per renderli disponibili all'altro computer in caso di errore. Ad esempio, il gestore code esistente potrebbe avere percorsi come `C:\WebSphere MQ\log\<QMname>` e `C:\WebSphere MQ\qmgrs\<QMname>`. ***non*** provare a spostare i file manualmente; utilizzare il programma di utilità fornito come parte del WebSphere MQ MSCS come descritto in questo argomento.

Se il gestore code che viene spostato utilizza connessioni SSL e il repository delle chiavi SSL si trova nella directory dei dati del gestore code sulla macchina locale, il repository delle chiavi verrà spostato con il resto del gestore code sul disco condiviso. Per impostazione predefinita, l'attributo del gestore code che specifica l'ubicazione del contenitore chiavi SSL, SSLKEYR, è impostato su *MQ_INSTALLATION_PATH*`\qmgrs\QMGRNAME\ssl\key`, che si trova nella directory dei dati del gestore code. *MQ_INSTALLATION_PATH* rappresenta la directory di alto livello in cui è installato WebSphere MQ . Il comando `hamvmqm` non modifica questo attributo del gestore code. In questa situazione, è necessario modificare l'attributo del gestore code, SSLKEYR, utilizzando il comando IBM WebSphere MQ Explorer o MQSC `ALTER QMGR`, per puntare al nuovo file del repository delle chiavi SSL.

La procedura è la seguente:

1. Chiudere il gestore code e controllare che non vi siano errori.
2. Se i file di log del gestore code o i file di coda sono già archiviati su un disco condiviso, saltare il resto di questa procedura e passare direttamente a "Inserimento di un gestore code sotto il controllo di MSCS" a pagina 336.
3. Eseguire un backup completo dei file di coda e dei file di log e memorizzare il backup in un luogo sicuro (consultare "File di log del gestore code" a pagina 345 per i motivi per cui ciò è importante).
4. Se si dispone già di una risorsa disco condivisa adatta, procedere con il passo 6. In caso contrario, utilizzare MSCS Cluster Administrator per creare una risorsa di tipo *disco condiviso* con capacità sufficiente per memorizzare i file di log del gestore code e i file di dati (coda).

5. Verificare il disco condiviso utilizzando MSCS Cluster Administrator per spostarlo da un nodo cluster all'altro e viceversa.
6. Verificare che il disco condiviso sia in linea sul nodo cluster in cui i file di dati e di log del gestore code sono memorizzati localmente.
7. Eseguire il programma di utilità per spostare il gestore code nel modo seguente:

```
 hamvmqm /m qmname /dd "e:\
WebSphere MQ" /ld "e:\
WebSphere MQ\log"
```

   sostituire il nome del gestore code con *qmname*, la lettera dell'unità disco condivisa per *e*e la directory scelta per *WebSphere MQ*. Le directory vengono create se non esistono già.
8. Verificare il funzionamento del gestore code utilizzando Esplora risorse di IBM WebSphere MQ . Ad esempio:
   a. Fare clic con il pulsante destro del mouse sul nodo della struttura ad albero del gestore code, quindi selezionare `Start`. Il gestore code viene avviato.
   b. Fare clic con il tasto destro del mouse su `Queues` tree node, quindi selezionare `New->Local Queue...`e assegnare un nome alla coda.
   c. Fare clic su `Finish`.
   d. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Put Test Message...`. Viene visualizzato il pannello Inserisci messaggio di prova.
   e. Immettere del testo di messaggio, quindi fare clic su `Put Test Message`e chiudere il pannello.
   f. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Browse Messages...`. Viene visualizzato il pannello Browser messaggi.
   g. Assicurarsi che il messaggio sia sulla coda, quindi fare clic su `Close` . Il pannello Browser messaggi viene chiuso.
   h. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Clear Messages...`. I messaggi sulla coda vengono eliminati.
   i. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Delete...`. Viene visualizzato un pannello di conferma, fare clic su OK. La coda è stata eliminata.
   j. Fare clic con il pulsante destro del mouse sul nodo della struttura ad albero del gestore code, quindi selezionare `Stop...`. Viene visualizzato il pannello Fine gestore code.
   k. Fare clic su OK. Il gestore code viene arrestato.
9. Come amministratore di WebSphere MQ , assicurarsi che l'attributo di avvio del gestore code sia impostato su manuale. In Esplora risorse di IBM WebSphere MQ , impostare il campo Avvio su `manual` nel pannello delle proprietà del gestore code.
10. Procedere con "Inserimento di un gestore code sotto il controllo di MSCS" a pagina 336.

Inserimento di un gestore code sotto il controllo di MSCS

Le attività coinvolte nel posizionamento di un gestore code sotto il controllo di MSCS, incluse le attività prerequisite.

Prima di inserire un gestore code sotto il controllo di MSCS

Prima di inserire un gestore code sotto il controllo di MSCS, effettuare le operazioni riportate di seguito:

1. Assicurarsi che IBM WebSphere MQ e il suo supporto MSCS siano installati su entrambe le macchine nel cluster e che il software su ciascun computer sia identico, come descritto in "Impostazione di IBM WebSphere MQ per il clustering MSCS" a pagina 332.
2. Utilizzare il programma di utilità **haregtyp** per registrare WebSphere MQ come tipo di risorsa MSCS su tutti i nodi cluster. Consultare "Programmi di utilità di supporto MSCS IBM WebSphere MQ" a pagina 347 per ulteriori informazioni.

3. Se il gestore code non è stato ancora creato, consultare “Creazione di un gestore code da utilizzare con MSCS” a pagina 334.
4. Se il gestore code è stato creato o esiste già, assicurarsi di aver eseguito la procedura in “Spostamento di un gestore code nella memoria MSCS” a pagina 335.
5. Arrestare il gestore code, se è in esecuzione, utilizzando un prompt dei comandi o IBM WebSphere MQ Explorer.
6. Verificare l'operazione MSCS delle unità condivise prima di passare a una delle seguenti procedure Windows in questo argomento.

Windows Server 2012

Attenzione: Il supporto MSCS viene fornito in WebSphere MQ 7.5 utilizzando una DLL a 32 bit. A causa di una limitazione in Windows 2012, il gestore code IBM WebSphere MQ non esegue il failover dopo un riavvio.

Microsoft ha reso obsoleto l'utilizzo di DLL a 32 - bit con Windows 2012 e, pertanto, non è attualmente disponibile alcuna correzione del sistema operativo per questo problema. IBM non fornisce una libreria a 64 bit per IBM WebSphere MQ 7.5.

Da IBM MQ 8.0 è disponibile una libreria a 64-bit, quindi è necessario utilizzare questa versione del prodotto per la piena funzionalità MSCS con Windows 2012 e versioni successive.

Per posizionare un gestore code sotto il controllo di MSCS su Windows Server 2012, utilizzare la seguente procedura:

1. Accedere al computer del nodo cluster che ospita il gestore code oppure accedere a una workstation remota come utente con autorizzazioni di amministrazione del cluster e connettersi al nodo cluster che ospita il gestore code.
2. Avviare lo strumento di gestione cluster di failover.
3. Fare clic con il tasto destro del mouse su **Gestione cluster di failover> Connetti cluster** per aprire una connessione al cluster.
4. A differenza dello schema di gruppi utilizzato in MSCS Cluster Administrator nelle versioni precedenti di Windows, lo strumento Gestione cluster di failover utilizza il concetto di servizi e applicazioni. Un'applicazione o un servizio configurato contiene tutte le risorse necessarie per un'applicazione da raggruppare in cluster. È possibile configurare un gestore code in MSCS nel modo seguente:
   a. Fare clic con il pulsante destro del mouse sul cluster e selezionare **Configura ruolo** per avviare la configurazione guidata.
   b. Selezionare **Altro server** nel pannello "Seleziona servizio o applicazione".
   c. Selezionare un indirizzo IP appropriato come punto di accesso client.

      Questo indirizzo deve essere un indirizzo IP non utilizzato che deve essere utilizzato dai client e da altri gestori code per connettersi al gestore code *virtuale* . Questo indirizzo IP non è l'indirizzo normale (statico) di entrambi i nodi; è un ulteriore indirizzo che *mobile* tra di essi. Sebbene MSCS gestisca l'instradamento di questo indirizzo, **non** verifica che l'indirizzo possa essere raggiunto.
   d. Assegnare una periferica di memoria per l'uso esclusivo da parte del gestore code. Questo dispositivo deve essere creato come istanza di risorsa prima di poter essere assegnato.

      È possibile utilizzare un'unità per memorizzare sia i file di log che i file di coda, oppure è possibile suddividerli tra le unità. In entrambi i casi, se ogni gestore code ha il proprio disco condiviso, assicurarsi che tutte le unità utilizzate da questo gestore code siano esclusive per questo gestore code, ossia che nessun altro si basi sulle unità. Assicurarsi inoltre di creare un'istanza di risorsa per ogni unità utilizzata dal gestore code.

      Il tipo di risorsa per un'unità dipende dal supporto SCSI che si utilizza; fare riferimento alle istruzioni dell'adattatore SCSI. Potrebbero essere già presenti gruppi e risorse per ciascuna delle unità condivise. In tal caso, non è necessario creare l'istanza della risorsa per ogni unità. Spostarlo dal gruppo corrente a quello creato per il gestore code.

Per ogni risorsa unità, impostare i proprietari possibili su entrambi i nodi. Impostare le risorse dipendenti su nessuna.

e. Selezionare la risorsa **IBM MQSeries MSCS** sul pannello "Seleziona tipo di risorsa".

f. Completare i passi rimanenti nella procedura guidata.

5. Prima di portare la risorsa in linea, la risorsa MSCS IBM MQSeries necessita di ulteriore configurazione:

   a. Selezionare il servizio appena definito che contiene una risorsa denominata 'Nuovo IBM MQSeries MSCS'.

   b. Fare clic con il tasto destro del mouse su **Proprietà** nella risorsa MQ .

   c. Configurare la risorsa:

      - `Name`; scegliere un nome che facilita l'individuazione del relativo gestore code.
      - `Run in a separate Resource Monitor`; per un migliore isolamento
      - `Possible owners`; impostare entrambi i nodi
      - `Dependencies`; aggiungere l'unità e l'indirizzo IP per questo gestore code.

        Avviso: Se non si riesce ad aggiungere queste dipendenze, IBM WebSphere MQ tenta di scrivere lo stato del gestore code sul disco del cluster errato durante i failover. Poiché molti processi potrebbero tentare di scrivere simultaneamente su questo disco, l'esecuzione di alcuni processi IBM WebSphere MQ potrebbe essere bloccata.

      - `Parameters`; come segue:

        – `QueueManagerName` (obbligatorio); il nome del gestore code che questa risorsa deve controllare. Questo gestore code deve essere presente sul computer locale.

        – `PostOnlineCommand` (facoltativo); è possibile specificare un programma da eseguire ogni volta che la risorsa del gestore code modifica il proprio stato da non in linea a in linea. Per ulteriori dettagli, consultare “Comando PostOnlinee comando PreOffline” a pagina 346.

        – `PreOfflineCommand` (facoltativo); è possibile specificare un programma da eseguire ogni volta che la risorsa del gestore code modifica il proprio stato da online a offline. Per ulteriori dettagli, consultare “Comando PostOnlinee comando PreOffline” a pagina 346.

        Nota: L'intervallo di polling *looksAlive* è impostato sul valore predefinito di 5000 ms. L'intervallo di polling *isAlive* è impostato sul valore predefinito di 60 000 ms. Questi valori predefiniti possono essere modificati solo dopo che la definizione della risorsa è stata completata. Per ulteriori dettagli, consultare “Riepilogo del polling looksAlive e isAlive” a pagina 343.

   d. Facoltativamente, impostare un nodo preferito (ma notare i commenti in “Utilizzo dei nodi preferiti” a pagina 346)

   e. La *Politica di failover* è impostata per default su valori sensibili, ma è possibile ottimizzare le soglie e i periodi che controllano *Failover risorse* e *Failover gruppi* in modo che corrispondano ai carichi collocati sul gestore code.

6. Verificare il gestore code portandolo in linea in MSCS Cluster Administrator e sottoponendolo ad un carico di lavoro di verifica. Se si sta sperimentando con un gestore code di verifica, utilizzare Esplora risorse di IBM WebSphere MQ . Ad esempio:

   a. Fare clic con il tasto destro del mouse su `Queues` tree node, quindi selezionare `New->Local Queue...`e assegnare un nome alla coda.

   b. Fare clic su `Finish`. La coda viene creata e visualizzata nella vista Contenuto.

   c. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Put Test Message...`. Viene visualizzato il pannello Inserisci messaggio di prova.

   d. Immettere del testo di messaggio, quindi fare clic su `Put Test Message`e chiudere il pannello.

   e. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Browse Messages...`. Viene visualizzato il pannello Browser messaggi.

f. Assicurarsi che il proprio messaggio sia sulla coda, quindi fare clic su `Close` . Il pannello Browser messaggi viene chiuso.

g. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Clear Messages...`. I messaggi sulla coda vengono eliminati.

h. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Delete...`. Viene visualizzato un pannello di conferma, fare clic su OK. La coda è stata eliminata.

7. Verificare che il gestore code possa essere portato offline e di nuovo online utilizzando MSCS Cluster Administrator.
8. Simula un failover.

   In MSCS Cluster Administrator, fare clic con il tasto destro del mouse sul gruppo contenente il gestore code e selezionare `Move Group`. Questa operazione può richiedere alcuni minuti. Se in altre occasioni si desidera spostare rapidamente un gestore code su un altro nodo, seguire la procedura in "Spostamento di un gestore code nella memoria MSCS" a pagina 335. È anche possibile fare clic con il pulsante destro del mouse e selezionare `Initiate Failure`; l'azione (riavvio locale o failover) dipende dallo stato corrente e dalle impostazioni di configurazione.

Windows Server 2008

Per collocare un gestore code sotto il controllo di MSCS su Windows Server 2008, utilizzare la seguente procedura:

1. Accedere al computer del nodo cluster che ospita il gestore code oppure accedere a una workstation remota come utente con autorizzazioni di amministrazione del cluster e connettersi al nodo cluster che ospita il gestore code.
2. Avviare lo strumento di gestione cluster di failover.
3. Fare clic con il tasto destro del mouse su **Gestione cluster di failover> Gestisci cluster ...** per aprire una connessione al cluster.
4. A differenza dello schema di gruppi utilizzato in MSCS Cluster Administrator nelle versioni precedenti di Windows, lo strumento Gestione cluster di failover utilizza il concetto di servizi e applicazioni. Un'applicazione o un servizio configurato contiene tutte le risorse necessarie per un'applicazione da raggruppare in cluster. È possibile configurare un gestore code in MSCS nel modo seguente:

   a. Fare clic con il tasto destro del mouse su **Servizi e applicazioni> Configura un servizio o un'applicazione ...** per avviare la procedura guidata di configurazione.

   b. Selezionare **Altro server** nel pannello "Seleziona servizio o applicazione".

   c. Selezionare un indirizzo IP appropriato come punto di accesso client.

      Questo indirizzo deve essere un indirizzo IP non utilizzato che deve essere utilizzato dai client e da altri gestori code per connettersi al gestore code *virtuale* . Questo indirizzo IP non è l'indirizzo normale (statico) di entrambi i nodi; è un ulteriore indirizzo che *mobile* tra di essi. Sebbene MSCS gestisca l'instradamento di questo indirizzo, **non** verifica che l'indirizzo possa essere raggiunto.

   d. Assegnare una periferica di memoria per l'uso esclusivo da parte del gestore code. Questo dispositivo deve essere creato come istanza di risorsa prima di poter essere assegnato.

      È possibile utilizzare un'unità per memorizzare sia i file di log che i file di coda, oppure è possibile suddividerli tra le unità. In entrambi i casi, se ogni gestore code ha il proprio disco condiviso, assicurarsi che tutte le unità utilizzate da questo gestore code siano esclusive per questo gestore code, ossia che nessun altro si basi sulle unità. Assicurarsi inoltre di creare un'istanza di risorsa per ogni unità utilizzata dal gestore code.

      Il tipo di risorsa per un'unità dipende dal supporto SCSI che si utilizza; fare riferimento alle istruzioni dell'adattatore SCSI. Potrebbero essere già presenti gruppi e risorse per ciascuna delle unità condivise. In tal caso, non è necessario creare l'istanza della risorsa per ogni unità. Spostarlo dal gruppo corrente a quello creato per il gestore code.

      Per ogni risorsa unità, impostare i proprietari possibili su entrambi i nodi. Impostare le risorse dipendenti su nessuna.

e. Selezionare la risorsa **IBM MQSeries MSCS** sul pannello "Seleziona tipo di risorsa".

f. Completare i passi rimanenti nella procedura guidata.

5. Prima di portare la risorsa in linea, la risorsa MSCS IBM MQSeries necessita di ulteriore configurazione:

   a. Selezionare il servizio appena definito che contiene una risorsa denominata 'Nuovo IBM MQSeries MSCS'.

   b. Fare clic con il tasto destro del mouse su **Proprietà** nella risorsa MQ .

   c. Configurare la risorsa:

      - `Name`; scegliere un nome che facilita l'individuazione del relativo gestore code.
      - `Run in a separate Resource Monitor`; per un migliore isolamento
      - `Possible owners`; impostare entrambi i nodi
      - `Dependencies`; aggiungere l'unità e l'indirizzo IP per questo gestore code.

        Avviso: L'errore nell'aggiunta di queste dipendenze indica che WebSphere MQ tenta di scrivere lo stato del gestore code sul disco del cluster errato durante i failover. Poiché molti processi potrebbero tentare di scrivere simultaneamente su questo disco, l'esecuzione di alcuni processi IBM WebSphere MQ potrebbe essere bloccata.

      - `Parameters`; come segue:

        – `QueueManagerName` (obbligatorio); il nome del gestore code che questa risorsa deve controllare. Questo gestore code deve essere presente sul computer locale.

        – `PostOnlineCommand` (facoltativo); è possibile specificare un programma da eseguire ogni volta che la risorsa del gestore code modifica il proprio stato da non in linea a in linea. Per ulteriori dettagli, consultare “Comando PostOnlinee comando PreOffline” a pagina 346.

        – `PreOfflineCommand` (facoltativo); è possibile specificare un programma da eseguire ogni volta che la risorsa del gestore code modifica il proprio stato da online a offline. Per ulteriori dettagli, consultare “Comando PostOnlinee comando PreOffline” a pagina 346.

          Nota: L'intervallo di polling *looksAlive* è impostato sul valore predefinito di 5000 ms. L'intervallo di polling *isAlive* è impostato sul valore predefinito di 60 000 ms. Questi valori predefiniti possono essere modificati solo dopo che la definizione della risorsa è stata completata. Per ulteriori dettagli, consultare “Riepilogo del polling looksAlive e isAlive” a pagina 343.

   d. Facoltativamente, impostare un nodo preferito (ma notare i commenti in “Utilizzo dei nodi preferiti” a pagina 346)

   e. La *Politica di failover* è impostata per default su valori sensibili, ma è possibile ottimizzare le soglie e i periodi che controllano *Failover risorse* e *Failover gruppi* in modo che corrispondano ai carichi collocati sul gestore code.

6. Verificare il gestore code portandolo in linea in MSCS Cluster Administrator e sottoponendolo ad un carico di lavoro di verifica. Se si sta sperimentando con un gestore code di verifica, utilizzare Esplora risorse di IBM WebSphere MQ . Ad esempio:

   a. Fare clic con il tasto destro del mouse su `Queues` tree node, quindi selezionare `New->Local Queue...`e assegnare un nome alla coda.

   b. Fare clic su `Finish`. La coda viene creata e visualizzata nella vista Contenuto.

   c. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Put Test Message...`. Viene visualizzato il pannello Inserisci messaggio di prova.

   d. Immettere del testo di messaggio, quindi fare clic su `Put Test Message`e chiudere il pannello.

   e. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Browse Messages...`. Viene visualizzato il pannello Browser messaggi.

   f. Assicurarsi che il proprio messaggio sia sulla coda, quindi fare clic su `Close` . Il pannello Browser messaggi viene chiuso.

g. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Clear Messages...`. I messaggi sulla coda vengono eliminati.

h. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Delete...`. Viene visualizzato un pannello di conferma, fare clic su OK. La coda è stata eliminata.

7. Verificare che il gestore code possa essere portato offline e di nuovo online utilizzando MSCS Cluster Administrator.
8. Simula un failover.

   In MSCS Cluster Administrator, fare clic con il tasto destro del mouse sul gruppo contenente il gestore code e selezionare `Move Group`. Questa operazione può richiedere alcuni minuti. Se in altre occasioni si desidera spostare rapidamente un gestore code su un altro nodo, seguire la procedura in "Spostamento di un gestore code nella memoria MSCS" a pagina 335. È anche possibile fare clic con il pulsante destro del mouse e selezionare `Initiate Failure`; l'azione (riavvio locale o failover) dipende dallo stato corrente e dalle impostazioni di configurazione.

Windows 2003

Per inserire un gestore code sotto il controllo di MSCS in Windows 2003, utilizzare la seguente procedura:

1. Accedere al computer del nodo cluster che ospita il gestore code oppure accedere a una workstation remota come utente con autorizzazioni di amministrazione del cluster e connettersi al nodo cluster che ospita il gestore code.
2. Avviare MSCS Cluster Administrator.
3. Aprire una connessione al cluster.
4. Creare un gruppo MSCS da utilizzare per contenere le risorse per il gestore code. Denominare il gruppo in modo tale che sia ovvio a quale gestore code è correlato. Ogni gruppo può contenere più gestori code, come descritto in "Utilizzo di più gestori code con MSCS" a pagina 333.

   Utilizzare il gruppo per tutti i passi rimanenti.
5. Creare un'istanza di risorsa per ciascuna unità logica SCSI utilizzata dal gestore code.

   È possibile utilizzare un'unità per memorizzare sia i file di log che i file di coda, oppure è possibile suddividerli tra le unità. In entrambi i casi, se ogni gestore code ha il proprio disco condiviso, assicurarsi che tutte le unità utilizzate da questo gestore code siano esclusive per questo gestore code, ossia che nessun altro si basi sulle unità. Assicurarsi inoltre di creare un'istanza di risorsa per ogni unità utilizzata dal gestore code.

   Il tipo di risorsa per un'unità dipende dal supporto SCSI che si utilizza; fare riferimento alle istruzioni dell'adattatore SCSI. Potrebbero essere già presenti gruppi e risorse per ciascuna delle unità condivise. In tal caso, non è necessario creare l'istanza della risorsa per ogni unità. Spostarlo dal gruppo corrente a quello creato per il gestore code.

   Per ogni risorsa unità, impostare i proprietari possibili su entrambi i nodi. Impostare le risorse dipendenti su nessuna.
6. Creare un'istanza di risorsa per l'indirizzo IP.

   Creare una risorsa indirizzo IP (tipo di risorsa *indirizzo IP*). Questo indirizzo deve essere un indirizzo IP non utilizzato che deve essere utilizzato dai client e da altri gestori code per connettersi al gestore code *virtuale* . Questo indirizzo IP non è l'indirizzo normale (statico) di entrambi i nodi; è un ulteriore indirizzo che *mobile* tra di essi. Sebbene MSCS gestisca l'instradamento di questo indirizzo, **non** verifica che l'indirizzo possa essere raggiunto.
7. Creare un'istanza di risorsa per il gestore code.

   Creare una risorsa di tipo *IBM WebSphere MQ MSCS*. La procedura guidata richiede diversi elementi, tra cui:

   - `Name`; scegliere un nome che facilita l'individuazione del relativo gestore code.
   - `Add to group`; utilizzare il gruppo creato
   - `Run in a separate Resource Monitor`; per un migliore isolamento

- `Possible owners`; impostare entrambi i nodi
- `Dependencies`; aggiungere l'unità e l'indirizzo IP per questo gestore code.

  Avviso: L'errore nell'aggiunta di queste dipendenze indica che WebSphere MQ tenta di scrivere lo stato del gestore code sul disco del cluster errato durante i failover. Poiché molti processi potrebbero tentare di scrivere simultaneamente su questo disco, l'esecuzione di alcuni processi IBM WebSphere MQ potrebbe essere bloccata.
- `Parameters`; come segue:
  - `QueueManagerName` (obbligatorio); il nome del gestore code che questa risorsa deve controllare. Questo gestore code deve essere presente sul computer locale.
  - `PostOnlineCommand` (facoltativo); è possibile specificare un programma da eseguire ogni volta che la risorsa del gestore code modifica il proprio stato da non in linea a in linea. Per ulteriori dettagli, consultare "Comando PostOnlinee comando PreOffline" a pagina 346.
  - `PreOfflineCommand` (facoltativo); è possibile specificare un programma da eseguire ogni volta che la risorsa del gestore code modifica il proprio stato da online a offline. Per ulteriori dettagli, consultare "Comando PostOnlinee comando PreOffline" a pagina 346.

    Nota: L'intervallo di polling *looksAlive* è impostato sul valore predefinito di 5000 ms. L'intervallo di polling *isAlive* è impostato sul valore predefinito di 30000 ms. Questi valori predefiniti possono essere modificati solo dopo che la definizione della risorsa è stata completata. Per ulteriori dettagli, consultare "Riepilogo del polling looksAlive e isAlive" a pagina 343.

8. Facoltativamente, impostare un nodo preferito (ma notare i commenti in "Utilizzo dei nodi preferiti" a pagina 346)
9. La *Politica di failover* (come definita nelle proprietà per il gruppo) è impostata per impostazione predefinita su valori sensibili, ma è possibile ottimizzare le soglie e i periodi che controllano *Failover risorse* e *Failover gruppi* in modo che corrispondano ai caricamenti posizionati sul gestore code.
10. Verificare il gestore code portandolo in linea in MSCS Cluster Administrator e sottoponendolo ad un carico di lavoro di verifica. Se si sta sperimentando con un gestore code di verifica, utilizzare Esplora risorse di IBM WebSphere MQ . Ad esempio:
    a. Fare clic con il tasto destro del mouse su `Queues` tree node, quindi selezionare `New->Local Queue...`e assegnare un nome alla coda.
    b. Fare clic su `Finish`. La coda viene creata e visualizzata nella vista Contenuto.
    c. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Put Test Message...`. Viene visualizzato il pannello Inserisci messaggio di prova.
    d. Immettere del testo di messaggio, quindi fare clic su `Put Test Message`e chiudere il pannello.
    e. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Browse Messages...`. Viene visualizzato il pannello Browser messaggi.
    f. Assicurarsi che il proprio messaggio sia sulla coda, quindi fare clic su `Close` . Il pannello Browser messaggi viene chiuso.
    g. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Clear Messages...`. I messaggi sulla coda vengono eliminati.
    h. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare `Delete...`. Viene visualizzato un pannello di conferma, fare clic su OK. La coda è stata eliminata.
11. Verificare che il gestore code possa essere portato offline e di nuovo online utilizzando MSCS Cluster Administrator.
12. Simula un failover.

    In MSCS Cluster Administrator, fare clic con il tasto destro del mouse sul gruppo contenente il gestore code e selezionare `Move Group`. Questa operazione può richiedere alcuni minuti. (Se in altre occasioni si desidera spostare rapidamente un gestore code su un altro nodo, seguire la procedura in "Spostamento di un gestore code nella memoria MSCS" a pagina 335.) È anche possibile fare clic con il pulsante destro del mouse e selezionare `Initiate Failure`; l'azione (riavvio locale o failover) dipende dallo stato corrente e dalle impostazioni di configurazione.

Riepilogo del polling looksAlive e isAlive

looksAlive e *isAlive* sono intervalli in cui MSCS richiama il codice della libreria fornito dei tipi di risorsa e richiede che la risorsa esegua controlli per determinare lo stato di funzionamento di se stessa. Ciò determina se MSCS tenta di eseguire il failover della risorsa.

Ogni volta che trascorre l'intervallo *looksAlive* (valore predefinito 5000 ms), la risorsa del gestore code viene richiamata per eseguire il proprio controllo per determinare se il suo stato è soddisfacente.

Ogni volta che trascorre l'intervallo *isAlive* (valore predefinito 30000 ms), viene effettuata un'altra chiamata alla risorsa del gestore code per eseguire un altro controllo per determinare se la risorsa sta funzionando correttamente. Ciò abilita due livelli di controllo del tipo di risorsa.

1. Un controllo di stato *looksAlive* per stabilire se la risorsa sembra funzionare.
2. Un controllo *isAlive* più significativo che determina se la risorsa del gestore code è attiva.

Se si determina che la risorsa del gestore code non è attiva, MSCS, in base ad altre opzioni avanzate di MSCS, attiva un failover per la risorsa e le risorse dipendenti associate ad un altro nodo nel cluster. Per ulteriori informazioni, consultare la documentazione MSCS.

Rimozione di un gestore code dal controllo MSCS

È possibile rimuovere i gestori code dal controllo MSCS e riportarli alla gestione manuale.

Non è necessario rimuovere i gestori code dal controllo MSCS per le operazioni di manutenzione. È possibile farlo portando un gestore code offline temporaneamente, utilizzando MSCS Cluster Administrator. La rimozione di un gestore code dal controllo MSCS è una modifica più permanente; eseguire tale operazione solo se si decide che non si desidera più che MSCS disponga di un ulteriore controllo del gestore code.

Se il gestore code da rimuovere utilizza connessioni SSL, è necessario modificare l'attributo del gestore code, SSLKEYR, utilizzando WebSphere MQ Explorer o il comando MQSC `ALTER QMGR`, per puntare al file del repository delle chiavi SSL nella directory locale.

La procedura è:

1. Portare offline la risorsa del gestore code utilizzando MSCS Cluster Administrator, come descritto in "Portare un gestore code non in linea da MSCS" a pagina 343
2. Eliminare l'istanza di risorsa. Questa operazione non elimina il gestore code.
3. Facoltativamente, migrare di nuovo i file del gestore code dalle unità condivise alle unità locali. Per fare ciò, consultare "Restituzione di un gestore code dalla memoria MSCS" a pagina 343.
4. Verificare il gestore code.

Portare un gestore code non in linea da MSCS

Per disattivare un gestore code da MSCS, effettuare le seguenti operazioni:

1. Avviare MSCS Cluster Administrator.
2. Aprire una connessione al cluster.
3. Selezionare `Groupse` aprire il gruppo contenente il gestore code da spostare.
4. Selezionare la risorsa gestore code.
5. Fare clic con il pulsante destro del mouse e selezionare `Offline`.
6. Attendere il completamento.

Restituzione di un gestore code dalla memoria MSCS

Questa procedura configura il gestore code in modo che sia di nuovo sull'unità locale del computer, ovvero diventa un gestore code *normale* WebSphere MQ . A tale scopo, spostare i file di log e i file di dati dai dischi condivisi. Ad esempio, il gestore code esistente potrebbe avere percorsi come `E:\WebSphere MQ\log\<QMname>` e `E:\WebSphere MQ\qmgrs\<QMname>`. Non tentare di spostare i

file manualmente; utilizzare il programma di utilità **hamvmqm** fornito come parte di WebSphere MQ MSCS Support:

1. Chiudere il gestore code e controllare che non vi siano errori.
2. Eseguire un backup completo dei file di coda e dei file di log e memorizzare il backup in un luogo sicuro (consultare "File di log del gestore code" a pagina 345 per i motivi per cui ciò è importante).
3. Decidere quale unità locale utilizzare e verificare che disponga di capacità sufficiente per memorizzare i file di log del gestore code e i file di dati (coda).
4. Assicurarsi che il disco condiviso su cui si trovano attualmente i file sia in linea sul nodo cluster in cui spostare i file di dati e di log del gestore code.
5. Eseguire il programma di utilità per spostare il gestore code nel modo seguente:

   ```
   hamvmqm /m qmname /dd "c:\
   WebSphere MQ" /ld "c:\
   WebSphere MQ\log"
   ```

   sostituire il nome del gestore code con *qmname*, la lettera dell'unità disco locale per *c* e la directory scelta per *WebSphere MQ* (le directory vengono create se non esistono già).
6. Verificare il funzionamento del gestore code (come descritto in "Spostamento di un gestore code nella memoria MSCS" a pagina 335).

Suggerimenti e consigli sull'utilizzo di MSCS

Questa sezione contiene alcune informazioni generali che consentono di utilizzare il supporto WebSphere MQ per MSCS in modo efficace.

Questa sezione contiene alcune informazioni generali che consentono di utilizzare il supporto WebSphere MQ per MSCS in modo efficace.

Quanto tempo ci vuole per far fallire un gestore code da una macchina all'altra? Ciò dipende fortemente dalla quantità di carico di lavoro sul gestore code e dalla combinazione di traffico, ad esempio, la quantità di traffico persistente, all'interno del punto di sincronizzazione e la quantità di commit prima dell'errore. I test IBM hanno fornito tempi di failover e failback di circa un minuto. Questo si trovava su un gestore code caricato in modo molto leggero e i tempi effettivi variano notevolmente a seconda del carico.

Verifica del funzionamento di MSCS

Seguire questa procedura per assicurarsi di avere un cluster MSCS in esecuzione.

Le descrizioni delle attività che iniziano con "Creazione di un gestore code da utilizzare con MSCS" a pagina 334 presuppongono che si disponga di un cluster MSCS in esecuzione in cui è possibile creare, migrare ed eliminare le risorse. Se si desidera assicurarsi di disporre di un cluster di questo tipo:

1. Utilizzando MSCS Cluster Administrator, creare un gruppo.
2. All'interno di tale gruppo, creare una istanza di una risorsa dell'applicazione generica, specificando l'orologio di sistema (nome percorso `C:\winnt\system32\clock.exe` e directory di lavoro `C:\`).
3. Assicurarsi di poter portare la risorsa in linea, di poter spostare il gruppo che la contiene sull'altro nodo e di poter portare la risorsa fuori linea.

Avvio manuale

Per un gestore code gestito da MSCS, è ***necessario*** impostare l'attributo di avvio su manuale. Ciò garantisce che il supporto MSCS WebSphere MQ possa riavviare il servizio IBM MQSeries senza avviare immediatamente il gestore code.

Il supporto MSCS WebSphere MQ deve essere in grado di riavviare il servizio in modo che possa eseguire il monitoraggio e il controllo, ma deve rimanere esso stesso in controllo di quali gestori code sono in esecuzione e su quali macchine. Per ulteriori informazioni, fare riferimento a "Spostamento di un gestore code nella memoria MSCS" a pagina 335.

MSCS ed i gestori code

Considerazioni relative ai gestori code quando si utilizza MSCS.

Creazione di un gestore code corrispondente sull'altro nodo

Perché il cluster funzioni con WebSphere MQ, è necessario un gestore code identico sul nodo B per ogni gestore code sul nodo A. Tuttavia, non è necessario creare esplicitamente la seconda. È possibile creare o preparare un gestore code su un nodo, spostarlo sull'altro nodo come descritto in "Spostamento di un gestore code nella memoria MSCS" a pagina 335ed è completamente duplicato su tale nodo.

Gestori code predefiniti

Non utilizzare un gestore code predefinito sotto il controllo di MSCS. Un gestore code non dispone di una proprietà che lo rende il valore predefinito; WebSphere MQ conserva il proprio record separato. Se si sposta un set di gestori code in modo che sia il valore predefinito sull'altro computer in failover, non diventa il valore predefinito. Tutte le applicazioni fanno riferimento a gestori code specifici in base al nome.

Eliminazione di un gestore code

Una volta che un gestore code ha spostato il nodo, i relativi dettagli sono presenti nel registro su entrambi i computer. Quando si desidera eliminarlo, eseguire tale operazione normalmente su un computer, quindi eseguire il programma di utilità descritto in "Programmi di utilità di supporto MSCS IBM WebSphere MQ" a pagina 347 per ripulire il registro sull'altro computer.

Supporto per i gestori code esistenti

È possibile inserire un Gestore code esistente sotto il controllo di MSCS, purché sia possibile inserire i file di log del gestore code e i file di coda su un disco che si trova sul bus SCSI condiviso tra le due macchine (consultare Figura 62 a pagina 332). È necessario disattivare brevemente il gestore code durante la creazione della risorsa MSCS.

Se si desidera creare un nuovo gestore code, crearlo indipendentemente da MSCS, verificarlo, quindi metterlo sotto controllo MSCS. Consultare:

- "Creazione di un gestore code da utilizzare con MSCS" a pagina 334
- "Spostamento di un gestore code nella memoria MSCS" a pagina 335
- "Inserimento di un gestore code sotto il controllo di MSCS" a pagina 336

Come comunicare a MSCS quali gestori code gestire

È possibile scegliere quali gestori code vengono posti sotto il controllo di MSCS utilizzando MSCS Cluster Administrator per creare un'istanza della risorsa per ciascun gestore code. Questo processo presenta un elenco di risorse da cui selezionare il gestore code che si desidera venga gestito da tale istanza.

File di log del gestore code

Quando si sposta un gestore code nella memoria MSCS, si spostano i relativi file di log e di dati su un disco condiviso (ad esempio, consultare "Spostamento di un gestore code nella memoria MSCS" a pagina 335).

Si consiglia di chiudere il gestore code in modo pulito e di eseguire un backup completo dei file di dati e dei file di log.

Più gestori code

Il supporto MSCS di WebSphere MQ consente di eseguire più gestori code su ciascuna macchina e di porre singoli gestori code sotto il controllo MSCS.

Utilizza sempre MSCS per gestire i cluster
Non tentare di eseguire operazioni di avvio e arresto direttamente su qualsiasi gestore code sotto il controllo di MSCS, utilizzando i comandi di controllo o IBM WebSphere MQ Explorer. Utilizzare invece MSCS Cluster Administrator per portare il gestore code online o offline.

L'utilizzo di MSCS Cluster Administrator è in parte per evitare possibili confusioni causate dal fatto che MSCS riporta che il gestore code è offline, quando in realtà è stato avviato al di fuori del controllo di MSCS. Più seriamente, l'arresto di un gestore code senza utilizzare MSC viene rilevato da MSCS come un errore, avviando il failover sull'altro nodo.

Lavorare in modalità Attiva / Attiva
Entrambi i computer nel cluster MSCS possono eseguire gestori code in modalità Attiva / Attiva. Non è necessario avere una macchina completamente inattiva che funge da standby (ma è possibile, se si desidera, in modalità Attiva / Passiva).

Se si intende utilizzare entrambe le macchine per eseguire il carico di lavoro, fornire a ciascuna di esse una capacità sufficiente (processore, memoria, memoria secondaria) per eseguire l'intero carico di lavoro del cluster ad un livello di prestazioni soddisfacente.

Nota: Se si utilizza MSCS insieme a Microsoft Transaction Server (COM +), **non è possibile** utilizzare la modalità Attiva / Attiva. Questo perché, per utilizzare WebSphere MQ con MSCS e COM +:

- I componenti dell'applicazione che utilizzano il supporto COM + di WebSphere MQdevono essere eseguiti sullo stesso computer di DTC (Distributed Transaction Coordinator), una parte di COM +.
- Il gestore code deve essere eseguito anche sullo stesso computer.
- Il DTC deve essere configurato come una risorsa MSCS e può quindi essere eseguito solo su uno dei computer nel cluster in qualsiasi momento.

Comando PostOnlinee comando PreOffline
Utilizzare questi comandi per integrare il supporto MSCS WebSphere MQ con altri sistemi. È possibile utilizzarle per immettere i comandi WebSphere MQ , con alcune limitazioni.

Specificare questi comandi nei parametri per una risorsa di tipo `IBM WebSphere MQ MSCS`. È possibile utilizzarli per integrare il supporto WebSphere MQ MSCS con altri sistemi o procedure. Ad esempio, è possibile specificare il nome di un programma che invia un messaggio di posta, attiva un cercapersone o genera un'altra forma di avviso da catturare da un altro sistema di controllo.

Il comando PostOnlineviene richiamato quando la risorsa passa da offline a online; il comando PreOfflineviene richiamato per una modifica da online a offline. Quando vengono richiamati, questi comandi vengono eseguiti, per impostazione predefinita, dalla directory di sistema Windows. Poiché WebSphere MQ utilizza un processo di controllo delle risorse a 32 bit, su sistemi Windows a 64 bit, questa è la directory `\Windows\SysWOW64` piuttosto che `\Windows\system32`. Per ulteriori informazioni, consultare la documentazione Microsoft sul reindirizzamento dei file in un ambiente Windows x64 . Entrambi i comandi vengono eseguiti con l'account dell'utente utilizzato per eseguire il servizio cluster MSCS e vengono richiamati in modo asincrono; il supporto WebSphere MQ MSCS non attende il completamento prima di continuare. Ciò elimina qualsiasi rischio che possano bloccare o ritardare ulteriori operazioni del cluster.

È anche possibile utilizzare questi comandi per immettere comandi WebSphere MQ , ad esempio per riavviare i canali del richiedente. Tuttavia, i comandi vengono eseguiti nel momento in cui lo stato del gestore code cambia in modo che non siano destinati ad eseguire funzioni di lunga durata e non devono fare ipotesi sullo stato corrente del gestore code; è possibile che, immediatamente dopo che il gestore code è stato portato in linea, un amministratore abbia emesso un comando non in linea.

Se si desidera eseguire programmi che dipendono dallo stato del gestore code, creare istanze del tipo di risorsa `MSCS Generic Application` , collocarle nello stesso gruppo MSCS della risorsa del gestore code e renderle dipendenti dalla risorsa del gestore code.

Utilizzo dei nodi preferiti
Può essere utile quando si utilizza la modalità Attiva / Attiva per configurare un *nodo preferito* per ciascun gestore code. Tuttavia, in generale, è meglio non impostare un nodo preferito, ma affidarsi a un failback manuale.

A differenza di alcune altre risorse relativamente stateless, un gestore code può impiegare del tempo per eseguire il failover (o il backover) da un nodo all'altro. Per evitare interruzioni non necessarie, verificare il nodo ripristinato prima di ripristinare un gestore code. Ciò impedisce l'utilizzo dell'impostazione di

failback `immediate` . È possibile configurare il failback in modo che si verifichi tra determinate ore del giorno.

Probabilmente l'instradamento più sicuro consiste nello spostare il gestore code manualmente sul nodo richiesto, quando si è certi che il nodo è completamente ripristinato. Ciò impedisce l'utilizzo dell'opzione `preferred node` .

Se si verificano errori COM + nel log eventi dell'applicazione
Quando si installa WebSphere MQ su un cluster MSCS appena installato, è possibile che venga rilevato un errore con COM + di origine e ID evento 4691 riportato nel log eventi dell'applicazione.

Ciò significa che si sta tentando di eseguire WebSphere MQ in un ambiente MSCS (Microsoft Cluster Server) quando MSDTC (Distributed Transaction Coordinator) di Microsoft non è configurato per l'esecuzione in tale ambiente. Per informazioni sulla configurazione di MSDTC in un ambiente cluster, fare riferimento alla documentazione Microsoft .

Programmi di utilità di supporto MSCS IBM WebSphere MQ

Un elenco del supporto IBM WebSphere MQ per i programmi di utilità MSCS che è possibile eseguire in una richiesta comandi.

Il supporto IBM WebSphere MQ per MSCS include i seguenti programmi di utilità:

Registrazione/Annullamento della registrazione del tipo di risorsa
`haregtyp.exe`

Dopo aver *annullato la registrazione* del tipo di risorsa MSCS IBM WebSphere MQ , non è più possibile creare risorse di quel tipo. MSCS non consente di annullare la registrazione di un tipo di risorsa se si dispone ancora di istanze di quel tipo nel cluster:

1. Utilizzando MSCS Cluster Administrator, arrestare tutti i gestori code in esecuzione sotto il controllo di MSCS, portandoli offline come descritto in “Portare un gestore code non in linea da MSCS” a pagina 343.
2. Utilizzando MSCS Cluster Administrator, eliminare le istanze della risorsa.
3. Al prompt dei comandi, annullare la registrazione del tipo di risorsa immettendo il seguente comando:

```
haregtyp /u
```

Se si desidera *registrare* il tipo (o registrarlo di nuovo in un secondo momento), immettere il seguente comando da un prompt dei comandi:

```
haregtyp /r
```

Dopo aver registrato correttamente le librerie MSCS, è necessario riavviare il sistema se non lo si è fatto dall'installazione di IBM WebSphere MQ.

Spostare un gestore code nella memoria MSCS
`hamvmqm.exe`

Consultare “Spostamento di un gestore code nella memoria MSCS” a pagina 335.

Eliminare un gestore code da un nodo
`hadltmqm.exe`

Considera il caso in cui hai avuto un gestore code nel tuo cluster, è stato spostato da un nodo a un altro e ora vuoi distruggerlo. Utilizzare IBM WebSphere MQ Explorer per eliminarlo sul nodo in cui si trova attualmente. Le voci di registro per esso esistono ancora sull'altro computer. Per eliminarli, immettere il seguente comando in un prompt su tale computer:

```
hadltmqm /m qmname
```

dove qmname è il nome del gestore code da eliminare.

Controllare e salvare i dettagli di configurazione

`amqmsysn.exe`

Questo programma di utilità presenta una finestra di dialogo che mostra i dettagli completi della configurazione del supporto MSCS IBM WebSphere MQ , come potrebbe essere richiesto se si chiama il supporto IBM . È disponibile un'opzione per salvare i dettagli in un file.

Gestori code a più istanze

I gestori code a più istanze sono istanze dello stesso gestore code configurato su server differenti. Un'istanza del gestore code è definita come istanza attiva e un'istanza è definita come istanza in standby. Se l'istanza attiva ha esito negativo, il gestore code a più istanze viene riavviato automaticamente sul server di standby.

Figura 63 a pagina 348 mostra una configurazione a più istanze per QM1. IBM WebSphere MQ è installato su due server, uno dei quali è di riserva. È stato creato un gestore code, QM1. Un'istanza di QM1 è attiva ed è in esecuzione su un server. L'altra istanza di QM1 è in esecuzione in standby sull'altro server, non eseguendo alcuna elaborazione attiva, ma è pronta a subentrare all'istanza attiva di QM1, se l'istanza attiva ha esito negativo.

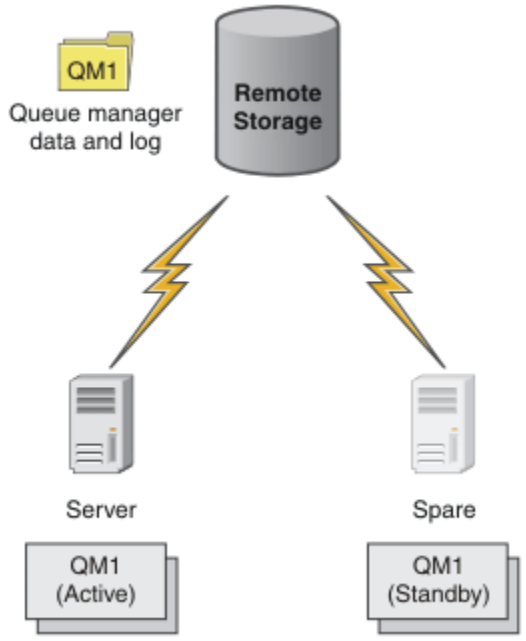


Figura 63. gestore code a più istanze

Quando si intende utilizzare un gestore code come gestore code a più istanza, creare un singolo gestore code su uno dei server utilizzando il comando **crtmqm** , inserendo i relativi dati del gestore code e log nella memoria di rete condivisa. Sull'altro server, piuttosto che creare nuovamente il gestore code, utilizzare il comando **addmqinf** per creare un riferimento ai log e ai dati del gestore code nella memoria di rete.

Ora è possibile eseguire il gestore code da entrambi i server. Ciascuno dei server fa riferimento agli stessi dati e log del gestore code; esiste un solo gestore code ed è attivo su un solo server alla volta.

Il gestore code può essere eseguito come gestore code a istanza singola o come gestore code a più istanze. In entrambi i casi è in esecuzione una sola istanza del gestore code, che elabora le richieste. La differenza è che quando viene eseguito come gestore code a più istanze, il server che non sta eseguendo l'istanza attiva del gestore code viene eseguito come un'istanza in standby, pronta a prendere il posto dell'istanza attiva automaticamente se il server attivo ha esito negativo.

L'unico controllo che si ha su quale istanza diventa attiva per prima è l'ordine in cui si avvia il gestore code sui due server. La prima istanza per acquisire i blocchi di lettura / scrittura sui dati del gestore code diventa l'istanza attiva.

È possibile scambiare l'istanza attiva con l'altro server, una volta avviata, arrestando l'istanza attiva utilizzando l'opzione di commutazione per trasferire il controllo allo standby.

L'istanza attiva di QM1 ha accesso esclusivo ai dati del gestore code condiviso e alle cartelle di log quando è in esecuzione. L'istanza standby di QM1 rileva quando l'istanza attiva ha avuto esito negativo e diventa l'istanza attiva. Assume il controllo dei dati e dei log QM1 nello stato in cui sono stati lasciati dall'istanza attiva e accetta le riconnessioni da client e canali.

L'istanza attiva potrebbe avere esito negativo per vari motivi che determinano l'assunzione del controllo da parte dello standby:

- Errore del server che ospita l'istanza del gestore code attivo.
- Errore di connettività tra il server che ospita l'istanza del gestore code attivo e il filesystem.
- Mancata risposta dei processi del gestore code, rilevata da WebSphere MQ, che chiude il gestore code.

È possibile aggiungere le informazioni di configurazione del gestore code a più server e scegliere due server qualsiasi da eseguire come coppia attivo / standby. Esiste un limite di un totale di due istanze. Non è possibile avere due istanze in standby e una attiva.

Un gestore code a più istanze è una parte di una soluzione alta disponibilità. Sono necessari alcuni componenti aggiuntivi per creare un'utile soluzione alta disponibilità.

- Riconnessione client e canale per trasferire WebSphere MQ connessioni al computer che assume il controllo dell'esecuzione dell'istanza del gestore code attivo.
- Un file system di rete condiviso ad alte prestazioni (NFS) che gestisce correttamente i blocchi e fornisce la protezione contro gli errori del supporto e del server di file.

  Importante: È necessario arrestare tutte le istanze del gestore code a più istanze in esecuzione nel proprio ambiente prima di eseguire la manutenzione sull'unità NFS . Verificare di disporre di backup di configurazione del gestore code da ripristinare, in caso di errore NFS .
- Reti e alimentatori resilienti per eliminare i singoli punti di errore nell'infrastruttura base.
- Applicazioni che tollerano il failover. In particolare, è necessario prestare molta attenzione al comportamento delle applicazioni transazionali e alle applicazioni che sfogliano code WebSphere MQ .
- Monitoraggio e gestione delle istanze attive e standby per garantire che siano in esecuzione e per riavviare le istanza attive che hanno avuto esito negativo. Sebbene i gestori code a più istanze si riavviino automaticamente, è necessario essere certi che le istanze in standby siano in esecuzione, pronte a prendere il controllo e che le istanze in errore vengano riportate in linea come nuove istanze in standby.

WebSphere MQ I client e i canali MQI si riconnettono automaticamente al gestore code in standby quando diventa attivo. Ulteriori informazioni sulla riconnessione e sugli altri componenti in una soluzione alta disponibilità sono disponibili negli argomenti correlati. La riconnessione automatica del client non è supportata dalle classi IBM WebSphere MQ per Java.

Piattaforme supportate

È possibile creare un gestore code a più istanze su qualsiasi piattaforma nonz/OS dalla versione 7.0.1.

La riconnessione client automatica è supportata per i client MQI dalla versione 7.0.1 in poi.

Crea un gestore code a più istanze

Creare un gestore code a più istanze, creare il gestore code su un server e configurare IBM WebSphere MQ su un altro server. I gestori code a più istanze hanno condiviso dati e log del gestore code.

La maggior parte delle attività coinvolte nella creazione di un gestore code a più istanze è l'attività di impostazione dei file di log e dei dati del gestore code condivisi. È necessario creare directory condivise sulla memoria di rete e rendere le directory disponibili per altri server utilizzando le condivisioni di rete.

Queste attività devono essere eseguite da un utente con autorità amministrativa, ad esempio *root* su sistemi UNIX and Linux . Le operazioni da eseguire vengono riportate di seguito.

1. Creare le condivisioni per i file di dati e di log.
2. Creare il gestore code su un server.
3. Eseguire il comando **dspmqinf** sul primo server per raccogliere i dati di configurazione del gestore code e copiarli negli appunti.
4. Eseguire il comando **addmqinf** con i dati copiati per creare la configurazione del gestore code sul secondo server.

crtmqm non viene eseguito per creare nuovamente il gestore code sul secondo server.

Controllo accesso file

È necessario fare attenzione che l'utente e il gruppo `mqm` su tutti gli altri server abbiano l'autorizzazione per accedere alle condivisioni.

Su UNIX and Linux, è necessario rendere uguali `uid` e `gid` di `mqm` su tutti i sistemi. Potrebbe essere necessario modificare `/etc/passwd` su ciascun sistema per impostare un `uid` e `gid` comune per `mqm`, quindi riavviare il sistema.

In Microsoft Windows, è necessario che l'ID utente che esegue i processi del gestore code disponga dell'autorizzazione di controllo completo per le directory contenenti i file di log e i dati del gestore code. È possibile configurare l'autorizzazione in due modi:

1. Creare un gestore code con un gruppo globale come principal di sicurezza alternativo. Autorizzare il gruppo globale ad avere il controllo completo delle directory contenenti i dati del gestore code e i file di log; consultare “Proteggere i dati del gestore code condiviso e le directory di log e i file su Windows” a pagina 376. Rendere l'ID utente che sta eseguendo il gestore code un membro del gruppo globale. Non è possibile rendere un utente locale membro di un gruppo globale, pertanto i processi del gestore code devono essere eseguiti con un ID utente del dominio. L'ID utente dominio deve essere un membro del gruppo locale `mqm`. L'attività, “Crea un gestore code a più istanze su server o workstation di dominio” a pagina 352, illustra come impostare un gestore code a più istanze utilizzando i file protetti in questo modo.
2. Creare un gestore code sul controller di dominio, in modo che il gruppo `mqm` locale abbia un ambito dominio, "dominio locale". Proteggere la condivisione file con il dominio locale `mqmed` eseguire i processi del gestore code su tutte le istanze di un gestore code nello stesso gruppo `mqm` locale del dominio. L'attività, “Crea un gestore code a più istanze sui controller di dominio” a pagina 366, illustra come impostare un gestore code a più istanze utilizzando i file protetti in questo modo.

Informazioni sulla configurazione

Configurare tutte le istanze del gestore code necessarie modificando le informazioni di configurazione del gestore code IBM WebSphere MQ per ciascun server. Ogni server deve avere la stessa versione di IBM WebSphere MQ installata a un livello di fix compatibile. I comandi, **dspmqinf** e **addmqinf** , consentono di configurare le istanze aggiuntive del gestore code. In alternativa, è possibile modificare direttamente i file `mqs.ini` e `qm.ini` . Gli argomenti “Crea un gestore code a più istanze su Linux” a pagina 388, “Crea un gestore code a più istanze su server o workstation di dominio” a pagina 352e “Crea un gestore code a più istanze sui controller di dominio” a pagina 366 sono esempi che mostrano come configurare un gestore code a più istanze.

Su Windows, sistemi UNIX and Linux , è possibile condividere un singolo file `mqs.ini` posizionandolo nella condivisione di rete e impostando la variabile di ambiente **AMQ_MQS_INI_LOCATION** in modo che punti ad esso.

Limitazioni

1. Configurare più istanze dello stesso gestore code solo su server con lo stesso sistema operativo, architettura ed endianness. Ad esempio, entrambe le macchine devono essere a 32 bit o a 64 bit.

2. Tutte le installazioni IBM WebSphere MQ devono essere al livello di rilascio 7.0.1 o superiore.
3. Generalmente, le installazioni attive e in standby vengono mantenute allo stesso livello di manutenzione. Consultare le istruzioni di manutenzione per ogni aggiornamento per verificare se è necessario aggiornare tutte le installazioni insieme.

   Tenere presente che i livelli di manutenzione per i gestori code attivi e passivi devono essere identici.
4. Condividere i dati e i log del gestore code solo tra gestori code configurati con lo stesso meccanismo di controllo accessi, gruppo e utente IBM WebSphere MQ .
5. Su sistemi UNIX and Linux , configurare il filesystem condiviso sull'archiviazione in rete con un montaggio `hard`, interrompibile, anziché un montaggio `soft` . Un montaggio hard interruptible forza il blocco del gestore code fino a quando non viene interrotto da una chiamata di sistema. I montaggi soft non garantiscono la coerenza dei dati dopo un malfunzionamento del server.
6. Le directory di dati e di log condivisi non possono essere memorizzate su un file system FAT o NFSv3 . Per i gestori code a più istanze su Windows, la memoria di rete deve essere accessibile dal protocollo CIFS (Common Internet File System) utilizzato dalle reti Windows .

Domini Windows e gestori code a più istanze
Un gestore code a più istanze su Windows richiede la condivisione dei dati e dei log. La condivisione deve essere accessibile a tutte le istanze del gestore code in esecuzione su server o workstation differenti. Configurare i gestori code e condividere come parte di un dominio Windows . Il gestore code può essere eseguito su una stazione di lavoro o su un server di dominio o sul controller di dominio.

Prima di configurare un gestore code a più istanze, leggere “Proteggere i file e le directory di log e i dati del gestore code non condivisi su Windows” a pagina 379 e “Proteggere i dati del gestore code condiviso e le directory di log e i file su Windows” a pagina 376 per esaminare come controllare l'accesso ai file di log e ai dati del gestore code. Gli argomenti sono didattici; se si desidera passare direttamente all'impostazione delle directory condivise per un gestore code a più istanze in un dominio Windows , fare riferimento alla sezione “Crea un gestore code a più istanze su server o workstation di dominio” a pagina 352.

Eseguire un gestore code a più istanze su server o workstation di dominio

Da Version 7.1, i gestori code a più istanze vengono eseguiti su una workstation o su un server membro di un dominio. Prima di Version 7.1, i gestori code a più istanze erano eseguiti solo sui controller di dominio; consultare “Eseguire un gestore code a più istanze sui controller di dominio” a pagina 352. Per eseguire un gestore code a più istanze su Windows, è necessario un controller di dominio, un server di file e due stazioni di lavoro o server che eseguono lo stesso gestore code connesso allo stesso dominio.

La modifica che rende possibile l'esecuzione di un gestore code a più istanze su qualsiasi server o stazione di lavoro in un dominio, è che ora è possibile creare un gestore code con un gruppo di sicurezza aggiuntivo. Il gruppo di sicurezza aggiuntivo viene passato nel comando **crtmqm** , nel parametro `-a` . Proteggere le directory che contengono i dati e i log del gestore code con il gruppo. L'ID utente che esegue i processi del gestore code deve essere un membro di questo gruppo. Quando il gestore code accede alle directory, Windows controlla le autorizzazioni di cui l'ID utente dispone per accedere alle directory. Fornendo sia il gruppo che l'ambito di dominio dell'ID utente, l'ID utente che esegue i processi del gestore code ha le credenziali del gruppo globale. Quando il gestore code è in esecuzione su un altro server, l'ID dell'utente che esegue i processi del gestore code può avere le stesse credenziali. L'ID utente non deve essere lo stesso. Deve essere un membro del gruppo di sicurezza alternativo, nonché un membro del gruppo `mqm` locale.

L'attività di creazione di un gestore code a più istanze è la stessa di Version 7.0.1 con una modifica. È necessario aggiungere il nome del gruppo di protezione aggiuntivo ai parametri del comando **crtmqm** . L'attività è descritta in “Crea un gestore code a più istanze su server o workstation di dominio” a pagina 352.

Sono richiesti più passi per configurare il dominio, i server di dominio e le stazioni di lavoro. È necessario comprendere il modo in cui Windows autorizza l'accesso da parte di un gestore code alle relative directory di dati e log. Se non si è certi del modo in cui i processi del gestore code sono autorizzati ad accedere ai file di log e di dati, leggere l'argomento “Proteggere i file e le directory di log e i dati del gestore code non

condivisi su Windows” a pagina 379. L'argomento include due attività che consentono di comprendere i passaggi richiesti. Le attività sono “Lettura e scrittura di dati e file di log autorizzati dal gruppo mqm locale” a pagina 381 e “Lettura e scrittura dei dati e dei file di log autorizzati da un gruppo di sicurezza locale alternativo” a pagina 384. Un altro argomento, “Proteggere i dati del gestore code condiviso e le directory di log e i file su Windows” a pagina 376, spiega come proteggere le directory condivise contenenti i dati del gestore code e i file di log con il gruppo di protezione alternativo. L'argomento include quattro attività, per configurare un dominio Windows , creare una condivisione file, installare IBM WebSphere MQ for Windowse configurare un gestore code per utilizzare la condivisione. Le attività sono le seguenti:

1. “Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ” a pagina 355.
2. “Installazione di IBM WebSphere MQ su un server o su una stazione di lavoro in un dominio Windows” a pagina 358.
3. “Creazione di una directory condivisa per i dati del gestore code e i file di log” a pagina 361.
4. “Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo” a pagina 363.

È quindi possibile eseguire l'attività, “Crea un gestore code a più istanze su server o workstation di dominio” a pagina 352, utilizzando il dominio. Eseguire queste operazioni per esplorare la configurazione di un gestore code a più istanze prima di trasferire le proprie conoscenze a un dominio di produzione.

Eseguire un gestore code a più istanze sui controller di dominio

In Version 7.0.1, i gestori code a più istanze vengono eseguiti solo sui controller di dominio. I dati del gestore code potrebbero essere protetti con il gruppo `mqm` del dominio. Come spiegato nell'argomento “Proteggere i dati del gestore code condiviso e le directory di log e i file su Windows” a pagina 376 , non è possibile condividere le directory protette con il gruppo `mqm` locale su workstation o server. Tuttavia, sui controller di dominio, tutti i gruppi e i principal hanno un ambito di dominio. Se si installa IBM WebSphere MQ for Windows su un controller di dominio, i dati del gestore code e i file di log sono protetti con il gruppo `mqm` del dominio, che può essere condiviso. Attenersi alla procedura riportata nell'attività, “Crea un gestore code a più istanze sui controller di dominio” a pagina 366 per configurare un gestore code a più istanze sui controller di dominio.

Informazioni correlate

Nodi cluster di Windows 2000, Windows Server 2003 e Windows Server 2008 come controller di dominio

Crea un gestore code a più istanze su server o workstation di dominio

Un esempio mostra come impostare un gestore code a più istanze su Windows su una stazione di lavoro o su un server che fa parte di un dominio Windows . Il server non deve essere un controller di dominio. La configurazione dimostra i concetti coinvolti, piuttosto che essere una scala di produzione. L'esempio è basato su Windows Server 2008. La procedura potrebbe differire su altre versioni di Windows Server.

In una configurazione della scala di produzione, potrebbe essere necessario adattare la configurazione a un dominio esistente. Ad esempio, è possibile definire diversi gruppi di domini per autorizzare diverse condivisioni e per raggruppare gli ID utente che eseguono gestori code.

La configurazione di esempio è composta da tre server:

sun
: Un controller di dominio Windows Server 2008. Possiede il dominio *wmq.example.com* che contiene *Sun*, *mars*e *venus*. A scopo illustrativo, viene utilizzato anche come server di file.

mars
: Un Windows Server 2008 utilizzato come primo server IBM WebSphere MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
: Un Windows Server 2008 utilizzato come secondo server IBM WebSphere MQ . Contiene la seconda istanza del gestore code a più istanze denominato *QMGR*.

Sostituire i nomi in corsivo nell'esempio, con nomi di propria scelta.

Prima di iniziare

Su Windows, non è necessario verificare il file system su cui si intende memorizzare i dati del gestore code e i file di log. La procedura di controllo, Verifica del funzionamento del file system condiviso , è applicabile a UNIX and Linux. In Windows, le verifiche hanno sempre esito positivo.

Effettuare le operazioni riportate di seguito. Le attività creano il controller di dominio e il dominio, installano IBM WebSphere MQ for Windows su un server e creano la condivisione file per i file di dati e di log. Se si sta configurando un controller di dominio esistente, potrebbe essere utile provare la procedura su un nuovo server Windows 2008. È possibile adattare la procedura al dominio.

1. “Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ” a pagina 355.
2. “Installazione di IBM WebSphere MQ su un server o su una stazione di lavoro in un dominio Windows” a pagina 358.
3. “Creazione di una directory condivisa per i dati del gestore code e i file di log” a pagina 361.
4. “Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo” a pagina 363.

Informazioni su questa attività

Questa attività fa parte di una sequenza di attività per configurare un controller di dominio e due server nel dominio per eseguire le istanze di un gestore code. In questa attività è possibile configurare un secondo server, *venus*, per eseguire un'altra istanza del gestore code *QMGR*. Seguire i passi in questa attività per creare la seconda istanza del gestore code, *QMGR*, e verificare che funzioni.

Questa attività è separata dalle quattro attività della precedente sezione. Contiene i passi che convertono un gestore code a istanza singola in un gestore code a più istanze. Tutti gli altri passi sono comuni ai gestori code a istanza singola o multipla.

Procedura

1. Configurare un secondo server per eseguire IBM WebSphere MQ for Windows.
   a) Effettuare le operazioni riportate nell'attività “Installazione di IBM WebSphere MQ su un server o su una stazione di lavoro in un dominio Windows” a pagina 358 per creare un secondo server di dominio. In questa sequenza di attività il secondo server è denominato *venus*.

   Suggerimento: Creare la seconda installazione utilizzando gli stessi valori predefiniti di installazione per IBM WebSphere MQ su ognuno dei due server. Se i valori predefiniti sono differenti, potrebbe essere necessario adattare le variabili `Prefisso` e `InstallationName` nella sezione *QMGR* **`QueueManager`** nel IBM WebSphere MQ file di configurazione `mqs.ini`. Le variabili fanno riferimento a percorsi che possono essere diversi per ogni installazione e gestore code su ciascun server. Se i percorsi rimangono gli stessi su ogni server, è più semplice configurare un gestore code a più istanze.
2. Creare una seconda istanza di *QMGR* su *venus*.
   a) Se *QMGR* su *mars* non esiste, eseguire l'attività “Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo” a pagina 363per crearla
   b) Controllare che i parametri `Prefisso` e `InstallationName` siano corretti per *venus*.

      In *mars*, eseguire il comando **`dspmqinf`** :

      ```
      dspmqinf QMGR
      ```

      La risposta del sistema:

      ```
      QueueManager:
         Name=QMGR
         Directory=QMGR
         Prefix=C:\Program Files\IBM\WebSphere MQ
      ```

```
   DataPath=\\sun\wmq\data\QMGR
   InstallationName=Installation1
```

c) Copiare il formato leggibile dalla macchina della stanza **QueueManager** negli appunti.

Su *mars* eseguire nuovamente il comando **dspmqinf** , con il parametro `-o command` .

```
dspmqinf -o command QMGR
```

La risposta del sistema:

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\Program Files\IBM\WebSphere MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

d) In *venus* eseguire il comando **addmqinf** dagli appunti per creare un'istanza del gestore code su *venus*.

Modificare il comando, se necessario, per adattare le differenze nei parametri `Prefisso` o `InstallationName` .

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\Program Files\IBM\WebSphere MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

```
WebSphere MQ configuration information added.
```

3. Avviare il gestore code *QMGR* su *venus*, consentendo le istanze in standby.

a) Verificare che *QMGR* on *mars* sia arrestato.

In *mars*, eseguire il comando **dspmq** :

```
dspmq -m QMGR
```

La risposta del sistema dipende da come è stato arrestato il gestore code; ad esempio:

```
C:\Users\Administrator>dspmq -m QMGR
QMNAME(QMGR) STATUS(Ended immediately)
```

b) Su *venus* eseguire il comando **strmqm** per avviare *QMGR* consentendo gli standby:

```
strmqm -x QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
WebSphere MQ queue manager 'QMGR' started using V7.1.0.0.
```

Risultati

Per verificare gli switch del gestore code a più istanze, effettuare le seguenti operazioni:

1. Su *mars*, eseguire il comando **strmqm** per avviare *QMGR* consentendo standbys:

```
strmqm -x QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
```

```
A standby instance of queue manager 'QMGR' has been started.
The active instance is running elsewhere.
```

2. Su *venus* eseguire il comando **endmqm** :

```
endmqm -r -s -i QMGR
```

La risposta del sistema su *venus*:

```
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ended, permitting switchover to
a standby instance.
```

E su *mars*:

```
dspmq
QMNAME(QMGR) STATUS(Running as standby)
C:\Users\wmquser2>dspmq
QMNAME(QMGR) STATUS(Running as standby)
C:\Users\wmquser2>dspmq
QMNAME(QMGR)  STATUS(Running)
```

Operazioni successive

Per verificare un gestore code a più istanze utilizzando programmi di esempio, consultare “Verificare il gestore code a più istanze su Windows” a pagina 373.

Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ

Questa attività crea il dominio *wmq.example.com* su un controller di dominio Windows 2008 denominato *sun*. Configura il gruppo globale Domain mqm nel dominio, con i diritti corretti e con un utente.

In una configurazione della scala di produzione, potrebbe essere necessario adattare la configurazione a un dominio esistente. Ad esempio, è possibile definire diversi gruppi di domini per autorizzare diverse condivisioni e per raggruppare gli ID utente che eseguono gestori code.

La configurazione di esempio è composta da tre server:

sun
: Un controller di dominio Windows Server 2008. Possiede il dominio *wmq.example.com* che contiene *Sun*, *mars*e *venus*. A scopo illustrativo, viene utilizzato anche come server di file.

mars
: Un Windows Server 2008 utilizzato come primo server IBM WebSphere MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
: Un Windows Server 2008 utilizzato come secondo server IBM WebSphere MQ . Contiene la seconda istanza del gestore code a più istanze denominato *QMGR*.

Sostituire i nomi in corsivo nell'esempio, con nomi di propria scelta.

Prima di iniziare

1. I passi delle attività sono congruenti con un Windows Server 2008 installato ma non configurato con alcun ruolo. Se si sta configurando un controller di dominio esistente, potrebbe essere utile provare la procedura su un nuovo server Windows 2008. È possibile adattare la procedura al dominio.

Informazioni su questa attività

In questa attività, si crea un dominio Active Directory e DNS su un nuovo controller di dominio. È quindi possibile configurarlo per installare IBM WebSphere MQ su altri server e stazioni di lavoro che si uniscono al dominio. Seguire l'attività se non si ha familiarità con l'installazione e la configurazione di Active Directory per creare un dominio Windows . È necessario creare un dominio Windows per creare una configurazione del gestore code a più istanze. L'attività non ha lo scopo di guidare l'utente nel modo migliore per configurare un dominio Windows . Per distribuire gestori code a più istanze in un ambiente di produzione, è necessario consultare la documentazione Windows .

Durante l'attività, effettuare le seguenti operazioni:

1. Installare Active Directory.
2. Aggiunge un dominio.
3. Aggiungere il dominio a DNS.
4. Creare il gruppo globale `Domain mqm` e assegnarle i diritti corretti.
5. Aggiungere un utente e renderlo membro del gruppo globale `Domain mqm`.

Questa attività è una delle attività correlate che illustrano l'accesso ai dati del gestore code e ai file di log. Le attività mostrano come creare un gestore code autorizzato a leggere e scrivere dati e file di log memorizzati in una directory di propria scelta. Accompagnano l'attività, "Domini Windows e gestori code a più istanze" a pagina 351.

Per l'attività, il nome host del controller di dominio è *sun*e i due server IBM WebSphere MQ sono denominati *mars* e *venus*. Il dominio è denominato *wmq.example.com*. È possibile sostituire tutti i nomi in corsivo nell'attività con nomi di propria scelta.

Procedura

1. Accedere al controller di dominio, *sun*, come amministratore locale o `Workgroup` .

   Se il server è già configurato come controller di dominio, è necessario collegarsi come amministratore di dominio.
2. Eseguire la procedura guidata Servizi dominio di Active Directory .

   a) Fare clic su **Avvia** > **Esegui ...** Immettere `dcpromo` e fare clic su **OK**.

   Se i file binari di Active Directory non sono già installati, Windows installa automaticamente i file.
3. Nella prima finestra della procedura guidata, lasciare deselezionata la check box **Utilizza installazione in modalità avanzata** . Fare clic su **Avanti** > **Avanti** e selezionare **Crea un nuovo dominio in un nuovo insieme di strutture** > **Avanti**.
4. Immettere *wmq.example.com* nel campo **FQDN del dominio root dell'insieme di strutture** . Fare clic su **Avanti**.
5. Nella finestra Imposta livello funzionale dell'insieme di strutture, selezionare **Windows Server 2003**o versione successiva dall'elenco di **Livelli funzionali dell'insieme di strutture** > **Avanti**.

   Il livello più vecchio di Windows Server supportato da IBM WebSphere MQ è Windows Server 2003.
6. Opzionale: Nella finestra Imposta livello funzionale dominio, selezionare **Windows Server 2003**o versioni successive dall'elenco di **Livelli funzionali dominio** > **Avanti**.

   Questo passo è richiesto solo se si imposta il livello funzionale dell'insieme di strutture su **Windows Server 2003**.
7. Viene visualizzata la finestra Opzioni controller di dominio aggiuntive, con **Server DNS** selezionato come opzione aggiuntiva. Fare clic su **Avanti** e su **Sì** per cancellare la finestra di avvertenza.

   Suggerimento: Se un server DNS è già installato, questa opzione non viene visualizzata. Se si desidera seguire questa attività in modo preciso, rimuovere tutti i ruoli da questo controller di dominio e riavviare.
8. Lasciare invariate le directory `Database`, `Log Filese` SYSVOL ; fare clic su **Avanti**.

9. Immettere una parola d'ordine nei campi **Password** e **Conferma parola d'ordine** nella finestra Directory Services Restore Mode Administrator Password. Fare clic su **Avanti** > **Avanti**. Selezionare **Riavvia al completamento** nella finestra finale della procedura guidata.
10. Quando il controller di dominio viene riavviato, collegarsi come *wmq*\Adminstrator.

    Il gestore server viene avviato automaticamente.
11. Aprire la cartella *wmq.example.com*\Users
    a) Aprire **Server Manager** > **Ruoli** > **Active Directory Domain Services** > ***wmq.example.com*** > **Utenti**.
12. Fare clic con il tasto destro del mouse su **Utenti** > **Nuovo gruppo** > .
    a) Immettere un nome gruppo nel campo **Nome gruppo**.

       Nota: Il nome gruppo preferito è Domain mqm. Immetterlo esattamente come visualizzato.

       - La chiamata del gruppo Domain mqm modifica il comportamento della procedura guidata "Prepara IBM WebSphere MQ" in una workstation o in un server del dominio. La procedura guidata "Prepara IBM WebSphere MQ" aggiunge automaticamente il gruppo Domain mqm al gruppo locale mqm in ogni nuova installazione di IBM WebSphere MQ nel dominio.
       - È possibile installare workstation o server in un dominio senza alcun gruppo globale Domain mqm . In questo caso, è necessario definire un gruppo con le stesse proprietà del gruppo Domain mqm. È necessario rendere il gruppo o gli utenti membri di esso, dei membri del gruppo mqm locale ovunque IBM WebSphere MQ sia installato in un dominio. È possibile inserire gli utenti di dominio in più gruppi. Creare più gruppi di domini, ciascuno dei quali corrispondente a un insieme di installazioni che si desidera gestire separatamente. Assegnare gli utenti di dominio ai diversi gruppi di domini in base alle installazioni gestite. Aggiungere ciascun gruppo o gruppi di domini al gruppo mqm locale delle diverse installazioni di IBM WebSphere MQ. Solo gli utenti di dominio nei gruppi di domini che sono dei membri di un gruppo mqm locale specifico possono creare, gestire ed eseguire i gestori code per tale installazione.
       - L'utente del dominio che si nomina quando si installa IBM WebSphere MQ su una workstation o su un server in un dominio deve essere un membro del gruppo Domain mqm o di un gruppo alternativo definito con le stesse proprietà del gruppo Domain mqm .

    b) Lasciare selezionato **Globale** come **Ambito del gruppo** o modificarlo in **Universale**. Lasciare selezionato **Sicurezza** come **Tipo di gruppo**. Fare clic su **OK**.
13. Aggiungere i diritti, **Consenti Lettura appartenenza gruppo** e **Consenti Leggi groupMembershipSAM** ai diritti del gruppo globale Domain mqm .
    a) Nella barra delle azioni di Server Manager, fare clic su **Visualizza** > **Funzioni avanzate**
    b) Nella struttura ad albero di navigazione di Server Manager, fare clic su **Utenti**
    c) Nella finestra Utenti, fare clic con il pulsante destro del mouse su **Domain mqm** > **Proprietà**
    d) Fare clic su **Sicurezza** > **Avanzate** > **Aggiungi ...**. Immettere Domain mqm e fare clic su **Controlla nomi** > **OK**.

       Il campo **Nome** è precompilato con la stringa Domain mqm (*domain name*\Domain mqm).
    e) Fare clic su **Proprietà**. Nell'elenco **Applica a**, selezionare **Oggetti utente discendenti** dalla parte inferiore dell'elenco.
    f) Dall'elenco **Autorizzazioni** , selezionare le caselle di spunta **Leggi appartenenza gruppo** e **Leggi groupMembershipSAM Consenti** ; fare clic su **OK** > **Applica** > **OK** > **OK**.
14. Aggiungere due o più utenti al gruppo globale Domain mqm .

    Un utente, *wmquser1* nell'esempio, esegue il servizio IBM IBM WebSphere MQ e l'altro utente, *wmquser2*, viene utilizzato in modo interattivo.
    Un utente di dominio è richiesto per creare un gestore code che utilizza il gruppo di sicurezza alternativo in una configurazione di dominio. Non è sufficiente che l'ID utente sia un amministratore, anche se un amministratore dispone dell'autorizzazione per eseguire il comando **crtmqm** . L'utente del dominio, che potrebbe essere un amministratore, deve appartenere al gruppo mqm locale e al gruppo di protezione alternativo.

Nell'esempio, si rendono membri *wmquser1* e *wmquser2* del gruppo globale `Domain mqm` . La procedura guidata "Prepara IBM WebSphere MQ" configura automaticamente `Domain mqm` come membro del gruppo `mqm` locale in cui viene eseguita la procedura guidata.
È necessario fornire un utente diverso per eseguire il servizio IBM WebSphere MQ IBM per ogni installazione di IBM WebSphere MQ su un singolo computer. È possibile riutilizzare gli stessi utenti su computer differenti.

a) Nella struttura ad albero di navigazione Server Manager, fare clic su **Utenti** > **Nuovo** > **Utente**
b) Nella finestra Nuovo oggetto - Utente, immettere *wmquser1* nel campo **Nome di accesso utente** . Immettere *WebSphere* nel campo **Nome** e *MQ1* nel campo **Cognome** . Fare clic su **Avanti**.
c) Immettere una password nei campi **Password** e **Conferma password** e deselezionare la casella di spunta **L'utente deve modificare la password al successivo accesso** . Fare clic su **Avanti** > **Fine**.
d) Nella finestra Utenti, fare clic con il tasto destro del mouse su ***WebSphere MQ*** > **Aggiungi a un gruppo ...**. Digitare `Domain mqm` e fare clic su **Verifica nomi** > **OK** > **OK**.
e) Ripetere i passi da a a d per aggiungere *WebSphere MQ2* come *wmquser2*.

15. Esecuzione di IBM WebSphere MQ come servizio.

Se è necessario eseguire IBM WebSphere MQ come un servizio, e quindi concedere all'utente del dominio (ottenuto dall'amministratore del dominio) il diritto di eseguire come un servizio, attenersi alla seguente procedura:

a) Fare clic su **Start > Esegui ...**.
Immettere il comando `secpol.msc` e fare clic su **OK**.
b) Aprire **Impostazioni di sicurezza > Politiche locali > Assegnazioni diritti utente**.
Nell'elenco delle politiche, fare clic con il pulsante destro del mouse su **Accedi come servizio > Proprietà**.
c) Fare clic su **Aggiungi utente o gruppo ...**
Immettere il nome dell'utente ottenuto dall'amministratore del dominio e fare clic su **Verifica nomi**
d) Se richiesto da una finestra Sicurezza di Windows , immettere il nome utente e la parola d'ordine di un utente o di un amministratore dell'account con autorizzazione sufficiente e fare clic su **OK> Applica> OK**.
Chiudere la finestra Politica di sicurezza locale.

Nota: Su Windows Vista e Windows Server 2008, UAC (User Account Control) è abilitata per impostazione predefinita.

La funzione UAC limita le azioni che gli utenti possono eseguire su alcune funzioni del sistema operativo, anche se sono dei membri del gruppo di amministratori. È necessario prendere le misure appropriate per risolvere questa limitazione.

Operazioni successive

Procedere con l'attività successiva, “Installazione di IBM WebSphere MQ su un server o su una stazione di lavoro in un dominio Windows” a pagina 358.

Installazione di IBM WebSphere MQ su un server o su una stazione di lavoro in un dominio Windows
In questa attività, è possibile installare e configurare IBM WebSphere MQ su un server o su una workstation nel dominio *wmq.example.com* Windows .

In una configurazione della scala di produzione, potrebbe essere necessario adattare la configurazione a un dominio esistente. Ad esempio, è possibile definire diversi gruppi di domini per autorizzare diverse condivisioni e per raggruppare gli ID utente che eseguono gestori code.

La configurazione di esempio è composta da tre server:

sun
Un controller di dominio Windows Server 2008. Possiede il dominio *wmq.example.com* che contiene *Sun*, *mars*e *venus*. A scopo illustrativo, viene utilizzato anche come server di file.

mars
Un Windows Server 2008 utilizzato come primo server IBM WebSphere MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
Un Windows Server 2008 utilizzato come secondo server IBM WebSphere MQ . Contiene la seconda istanza del gestore code a più istanze denominato *QMGR*.

Sostituire i nomi in corsivo nell'esempio, con nomi di propria scelta.

Prima di iniziare

1. Effettuare le operazioni in "Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ" a pagina 355 per creare un controller di dominio, *sun*, per il dominio *wmq.example.com*. Modificare i nomi in corsivo per adattarli alla propria configurazione.
2. Consultare Requisiti hardware e software su sistemi Windows per altre versioni di Windows su cui è possibile eseguire IBM WebSphere MQ .

Informazioni su questa attività

In questa attività si configura un Windows Server 2008, denominato *mars*, come membro del dominio *wmq.example.com* . Si installa IBM WebSphere MQe si configura l'installazione da eseguire come membro del dominio *wmq.example.com* .

Questa attività è una delle attività correlate che illustrano l'accesso ai dati del gestore code e ai file di log. Le attività mostrano come creare un gestore code autorizzato a leggere e scrivere dati e file di log memorizzati in una directory di propria scelta. Accompagnano l'attività, "Domini Windows e gestori code a più istanze" a pagina 351.

Per l'attività, il nome host del controller di dominio è *sun*e i due server IBM WebSphere MQ sono denominati *mars* e *venus*. Il dominio è denominato *wmq.example.com*. È possibile sostituire tutti i nomi in corsivo nell'attività con nomi di propria scelta.

Procedura

1. Aggiungere il controller di dominio, *sun.wmq.example.com* a *mars* come server DNS.
   a) Su *mars*, collegarsi come *mars*\Administrator e fare clic su **Avvia**.
   b) Fare clic con il pulsante destro del mouse su **Rete** > **Proprietà** > **Gestisci connessioni di rete**.
   c) Fare clic con il tasto destro del mouse sull'adattatore di rete, fare clic su **Proprietà**.

      Il sistema risponde con la finestra Proprietà connessione area locale che elenca le voci utilizzate dalla connessione.
   d) Selezionare **Internet Protocol Versione 4** o **Internet Protocol Versione 6** dall'elenco di voci nella finestra Proprietà connessione area locale. Fare clic su **Proprietà** > **Avanzate ...** e fare clic sul separatore **DNS** .
   e) Sotto gli indirizzi server DNS, fare clic su **Aggiungi ...**.
   f) Immettere l'indirizzo IP del controller di dominio, che è anche il server DNS, e fare clic su **Aggiungi**.
   g) Fare clic su **Aggiungi questi suffissi DNS** > **Aggiungi ...**.
   h) Immettere *wmq.example.com* e fare clic su **Aggiungi**.
   i) Immettere *wmq.example.com* nel campo **Suffisso DNS per questa connessione** .
   j) Seleziona **Register this connection's address in DNS** e **Use this connection's suffix in DNS registration**. Fare clic su **OK** > **OK** > **Chiudi**
   k) Aprire una finestra comandi e immettere il comando **ipconfig /all** per esaminare le impostazioni TCP/IP.
2. Su *mars*, aggiungere il computer al dominio *wmq.example.com* .

a) Fare clic su **Avvia**

b) Fare clic con il tasto destro del mouse su **Computer** > **Proprietà**. Nella divisione Nome computer, dominio e impostazioni gruppo di lavoro, fare clic su **Modifica impostazioni**.

c) Nelle finestre delle proprietà del sistema, fare clic su **Modifica**.

d) Fare clic su Dominio, immettere *wmq.example.com*e fare clic su **OK**.

e) Immettere il **Nome utente** e la **Password** dell'amministratore del controller di dominio, che dispone dell'autorizzazione per consentire al computer di unirsi al dominio e fare clic su **OK**.

f) Fare clic su **OK** > **OK** > **Chiudi** > **Riavvia ora** in risposta al messaggio "Benvenuti nel dominio *wmq.example.com*" .

3. Verificare che il computer sia un membro del dominio *wmq.example.com*

a) Su *sun*, accedere al controller di dominio come *wmq*\Administrator.

b) Aprire **Server Manager** > **Active Directory Domain Services** > ***wmq.example.com*** > **Computer** e controllare che *mars* sia elencato correttamente nella finestra Computer.

4. Installare IBM WebSphere MQ for Windows su *mars*.

Per ulteriori informazioni sull'esecuzione della procedura guidata di installazione di IBM WebSphere MQ for Windows , consultare Installazione del server IBM WebSphere MQ su Windows .

a) Su *mars*, accedere come amministratore locale, *mars*\Administrator.

b) Eseguire il comando **Setup** sul supporto di installazione IBM WebSphere MQ for Windows .

Viene avviata l'applicazione IBM WebSphere MQ Launchpad.

c) Fare clic su **Requisiti software** per verificare che il software prerequisito sia installato.

d) Fare clic su **Configurazione di rete** > **Sì** per configurare un ID utente di dominio.

L'attività, “Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ” a pagina 355, configura un ID utente di dominio per questa serie di attività.

e) Fare clic su **WebSphere MQ Installazione**, selezionare una lingua di installazione e fare clic su Avvia IBM IBM WebSphere MQ Installer.

f) Confermare l'accordo di licenza e fare clic su **Avanti** > **Avanti** > **Installa** per accettare la configurazione predefinita. Attendere il completamento dell'installazione e fare clic su **Fine**.

È possibile modificare il nome dell'installazione, installare componenti differenti, configurare una directory differente per i dati e i log del gestore code o installare in una directory differente. In tal caso, fare clic su **Personalizzato** invece di **Tipico**.

IBM WebSphere MQ è installato e il programma di installazione avvia la procedura guidata "Prepara IBM WebSphere MQ" .

Importante: Non eseguire ancora la procedura guidata.

5. Configurare l'utente che eseguirà il servizio IBM IBM WebSphere MQ con il diritto **Esegui come servizio** .

Scegli se configurare il gruppo mqm locale, il gruppo Domain mqm o l'utente che eseguirà il servizio IBM IBM WebSphere MQ con la destra. Nell'esempio, si dà all'utente il diritto.

a) Fare clic su **Avvia** > **Esegui ...**, immettere il comando **secpol.msc** e fare clic su **OK**.

b) Aprire **Impostazioni di protezione** > **Politiche locali** > **Assegnazione diritti utente**. Nell'elenco delle politiche, fare clic con il tasto destro del mouse su **Accedi come servizio** > **Proprietà**.

c) Fare clic su **Aggiungi utente o gruppo ...** e immettere *wmquser1* e fare clic su **Verifica nomi**

d) Immettere il nome utente e la password di un amministratore di dominio, *wmq*\Administratore fare clic su **OK** > **Applica** > **OK**. Chiudere la finestra Politica di sicurezza locale.

6. Eseguire la procedura guidata "Prepara IBM WebSphere MQ" .

Per ulteriori informazioni sull'esecuzione della procedura guidata "Prepara IBM WebSphere MQ" ; consultare Configurazione di WebSphere MQ con la procedura guidata Prepara WebSphere MQ .

a) Il programma di installazione di IBM IBM WebSphere MQ esegue automaticamente "Prepara IBM WebSphere MQ" .

   Per avviare la procedura guidata manualmente, individuare il collegamento alla cartella "Prepara IBM WebSphere MQ" in **Avvia** > **Tutti i programmi** > **IBM WebSphere MQ** . Selezionare il collegamento che corrisponde all'installazione di IBM WebSphere MQ in una configurazione a più installazioni.

b) Fare clic su **Avanti** e lasciare **Sì** selezionato in risposta alla domanda "Identifica se è presente un controller di dominio Windows 2000 o successivo nella rete".

c) Fare clic su **Sì** > **Avanti** nella prima finestra Configurazione di IBM WebSphere MQ for Windows per gli utenti del dominio Windows .

d) Nella seconda finestra Configurazione di IBM WebSphere MQ for Windows per gli utenti del dominio Windows , immettere *wmq* nel campo **Dominio** . Immettere *wmquser1* nel campo **Nome utente** e la password, se impostata, nel campo **Password** . Fare clic su **Avanti**.

   La procedura guidata configura e avvia IBM IBM WebSphere MQ con *wmquser1*.

e) Nella pagina finale della procedura guidata, selezionare o deselezionare le caselle di spunta richieste e fare clic su **Fine**.

Operazioni successive

1. Eseguire l'attività, “Lettura e scrittura di dati e file di log autorizzati dal gruppo mqm locale” a pagina 381, per verificare che l'installazione e la configurazione stiano funzionando correttamente.
2. Eseguire l'attività, “Creazione di una directory condivisa per i dati del gestore code e i file di log” a pagina 361, per impostare una condivisione file per memorizzare i dati e i file di log di un gestore code a più istanze.

Concetti correlati

Diritti utente necessari per un servizio Windows di WebSphere MQ

Creazione di una directory condivisa per i dati del gestore code e i file di log

Questa attività è una delle attività correlate che illustrano l'accesso ai dati del gestore code e ai file di log. Le attività mostrano come creare un gestore code autorizzato a leggere e scrivere dati e file di log memorizzati in una directory di propria scelta.

In una configurazione della scala di produzione, potrebbe essere necessario adattare la configurazione a un dominio esistente. Ad esempio, è possibile definire diversi gruppi di domini per autorizzare diverse condivisioni e per raggruppare gli ID utente che eseguono gestori code.

La configurazione di esempio è composta da tre server:

sun
Un controller di dominio Windows Server 2008. Possiede il dominio *wmq.example.com* che contiene *Sun*, *mars*e *venus*. A scopo illustrativo, viene utilizzato anche come server di file.

mars
Un Windows Server 2008 utilizzato come primo server IBM WebSphere MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
Un Windows Server 2008 utilizzato come secondo server IBM WebSphere MQ . Contiene la seconda istanza del gestore code a più istanze denominato *QMGR*.

Sostituire i nomi in corsivo nell'esempio, con nomi di propria scelta.

Prima di iniziare

1. Per eseguire questa attivit ... esattamente come documentato, effettuare le operazioni riportate nell'attivit ..., “Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ” a pagina 355, per creare il dominio *sun.wmq.example.com* sul controller di dominio *sun*. Modificare i nomi in corsivo per adattarli alla propria configurazione.

Informazioni su questa attività

Questa attività è una delle attività correlate che illustrano l'accesso ai dati del gestore code e ai file di log. Le attività mostrano come creare un gestore code autorizzato a leggere e scrivere dati e file di log memorizzati in una directory di propria scelta. Accompagnano l'attività, "Domini Windows e gestori code a più istanze" a pagina 351.

Nell'attività, viene creata una condivisione contenente una directory di dati e log e un gruppo globale per autorizzare l'accesso alla condivisione. Passare il nome del gruppo globale che autorizza la condivisione al comando **crtmqm** nel suo parametro -a . Il gruppo globale offre la flessibilità di separare gli utenti di questa condivisione dagli utenti di altre azioni. Se non è necessaria questa flessibilità, autorizzare la condivisione con il gruppo Domain mqm piuttosto che creare un nuovo gruppo globale.

Il gruppo globale utilizzato per la condivisione in questa attività è denominato *wmqha*e la condivisione è denominata *wmq*. Sono definiti sul controller di dominio *sun* nel Windows dominio *wmq.example.com*. La condivisione ha autorizzazioni di controllo complete per il gruppo globale *wmqha*. Sostituire i nomi in corsivo nell'attività con i nomi desiderati.

Ai fini di questa attività, il controller di dominio è lo stesso server del server di file. Nelle applicazioni pratiche, suddividere i servizi di directory e file tra diversi server per prestazioni e disponibilità.

È necessario configurare l'ID utente con cui è in esecuzione il gestore code in modo che sia membro di due gruppi. Deve essere un membro del gruppo mqm locale su un server IBM WebSphere MQ e del gruppo globale *wmqha* .

In questa serie di attività, quando il gestore code è in esecuzione come servizio, viene eseguito con l'ID utente *wmquser1*, quindi *wmquser1* deve essere un membro di *wmqha*. Quando il gestore code viene eseguito in modo interattivo, viene eseguito con l'ID utente *wmquser2*, quindi *wmquser2* deve essere un membro di *wmqha*. Sia *wmquser1* che *wmquser2* sono membri del gruppo globale Domain mqm. Domain mqm è un membro del gruppo mqm locale sui server *mars* e *venus* IBM WebSphere MQ . Quindi, *wmquser1* e *wmquser2* sono membri del gruppo mqm locale su entrambi i serverIBM WebSphere MQ .

Procedura

1. Accedere al controller di dominio, *sun.wmq.example.com* come amministratore del dominio.
2. Creare il gruppo globale *wmqha*.
   a) Aprire **Server Manager** > **Ruoli** > **Active Directory Domain Services** > ***wmq.example.com*** > **Utenti**.
   b) Aprire la cartella *wmq.example.com*\Users
   c) Fare clic con il tasto destro del mouse su **Utenti** > **Nuovo gruppo** > .
   d) Immettere *wmqha* nel campo **Nome gruppo** .
   e) Lasciare **Globale** selezionato come **Ambito gruppo** e **Sicurezza** come **Tipo di gruppo**. Fare clic su **OK**.
3. Aggiungere gli utenti del dominio *wmquser1* e *wmquser2* al gruppo globale, *wmqha*.
   a) Nella struttura ad albero di navigazione Server Manager, fare clic su **Utenti** e fare clic con il tasto destro del mouse su ***wmqha*** > **Proprietà** nell'elenco degli utenti.
   b) Fare clic sulla scheda Membri nella finestra Proprietà di *wmqha* .
   c) Fare clic su **Aggiungi ...**; immettere *wmquser1*; *wmquser2* e fare clic su **Verifica nomi** > **OK** > **Applica** > **OK**.
4. Creare la struttura di directory per contenere i dati del gestore code e i file di log.
   a) Aprire un prompt dei comandi.
   b) Immettere il comando:

```
md c:\wmq\data , c:\wmq\logs
```

5. Autorizzare il gruppo globale *wmqha* ad avere l'autorizzazione di controllo completo per le directory *c:* *wmq* e la condivisione.
   a) In Windows Explorer, fare clic con il pulsante destro del mouse su ***c:* *wmq*** > **Proprietà**.

b) Fare clic sulla scheda **Sicurezza** , quindi su **Avanzate** > **Modifica ...**.

c) Deselezionare la check box per **Includi autorizzazioni ereditabili dal proprietario di questo oggetto**. Fare clic su **Copia** nella finestra Sicurezza di Windows.

d) Selezionare le linee per gli utenti nell'elenco **Voci di autorizzazione** e fare clic su **Rimuovi**. Lasciare le righe per SYSTEM, Administrators e CREATOR OWNER nell'elenco **Voci di autorizzazione**.

e) Fare clic su **Aggiungi ...**, e immettere il nome del gruppo globale *wmqha*. Fare clic su **Verifica nomi** > **OK**.

f) Nella finestra Immissione per wmq , selezionare **Controllo completo** nell'elenco di **Autorizzazioni**.

g) Fare clic su **OK** > **Applica** > **OK** > **OK** > **OK**

h) In Windows Explorer, fare clic con il pulsante destro del mouse su ***c: \wmq*** > **Condividi ...**.

i) Fare clic su **Condivisione avanzata ...** e selezionare la casella di spunta **Condividi questa cartella** . Lasciare il nome condivisione come *wmq*.

j) Fare clic su **Autorizzazioni** > **Aggiungi ...**, e immettere il nome del gruppo globale *wmqha*. Fare clic su **Verifica nomi** > **OK**.

k) Selezionare *wmqha* nell'elenco **Nomi gruppo o utente**. Selezionare la casella di spunta **Controllo completo** nell'elenco **Autorizzazioni per *wmqha***; fare clic su **Applica**.

l) Selezionare *Administrators* nell'elenco **Nomi gruppo o utente**. Selezionare la casella di spunta **Controllo completo** nell'elenco **Autorizzazioni per *Amministratori***; fare clic su **Applica** > **OK** > **OK** > **Chiudi**.

Operazioni successive

Verificare che sia possibile leggere e scrivere file nelle directory condivise da ciascuno dei server IBM WebSphere MQ . Controllare l'ID utente di servizio IBM IBM WebSphere MQ *wmquser1* e l'ID utente interattivo, *wmquser2*.

1. Se si utilizza il desktop remoto, è necessario aggiungere *wmq**wmquser1* e *wmquser2* al gruppo locale Remote Desktop Users su *mars*.
   a. Accedere a *mars* come *wmq*\Administrator
   b. Eseguire il comando **lusrmgr.msc** per aprire la finestra Utenti e gruppi locali.
   c. Fare clic su **Gruppi**. Fare clic con il pulsante destro del mouse su **Utenti desktop remoto** > **Proprietà** > **Aggiungi ...**. Immettere *wmquser1; wmquser2* e fare clic su **Verifica nomi**.
   d. Immettere il nome utente e la password dell'amministratore del dominio, *wmq*\Administratore fare clic su **OK** > **Applica** > **OK**.
   e. Chiudere la finestra Utenti e gruppi locali.
2. Accedere a *mars* come *wmq**wmquser1*.
   a. Aprire una finestra Esplora risorse di Windows e immettere *sun**wmq*.

      Il sistema risponde aprendo la condivisione *wmq* su *sun.wmq.example.com*ed elenca le directory di dati e log.
   b. Controllare le autorizzazioni di *wmquser1* creando un file nella sottodirectory dei dati, aggiungendo del contenuto, leggendolo ed eliminandolo.
3. Accedere a *mars* come *wmq**wmquser2*e ripetere i controlli.
4. Eseguire l'attività successiva, per creare un gestore code per utilizzare i dati condivisi e le directory di log; consultare “Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo” a pagina 363.

Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo
In questa sezione viene illustrato come utilizzare l'indicatore -a nel comando **crtmqm** . L'indicatore -a fornisce al gestore code l'accesso ai relativi file di log e di dati su una condivisione file remota utilizzando il gruppo di sicurezza alternativo.

In una configurazione della scala di produzione, potrebbe essere necessario adattare la configurazione a un dominio esistente. Ad esempio, è possibile definire diversi gruppi di domini per autorizzare diverse condivisioni e per raggruppare gli ID utente che eseguono gestori code.

La configurazione di esempio è composta da tre server:

sun
Un controller di dominio Windows Server 2008. Possiede il dominio *wmq.example.com* che contiene *Sun*, *mars*e *venus*. A scopo illustrativo, viene utilizzato anche come server di file.

mars
Un Windows Server 2008 utilizzato come primo server IBM WebSphere MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
Un Windows Server 2008 utilizzato come secondo server IBM WebSphere MQ . Contiene la seconda istanza del gestore code a più istanze denominato *QMGR*.

Sostituire i nomi in corsivo nell'esempio, con nomi di propria scelta.

Prima di iniziare

Effettuare le operazioni riportate di seguito. Le attività creano il controller di dominio e il dominio, installano IBM WebSphere MQ for Windows su un server e creano la condivisione file per i file di dati e di log. Se si sta configurando un controller di dominio esistente, potrebbe essere utile provare la procedura su un nuovo server Windows 2008. È possibile adattare la procedura al dominio.

1. “Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ” a pagina 355.
2. “Installazione di IBM WebSphere MQ su un server o su una stazione di lavoro in un dominio Windows” a pagina 358.
3. “Creazione di una directory condivisa per i dati del gestore code e i file di log” a pagina 361.

Informazioni su questa attività

Questa attività è una delle attività correlate che illustrano l'accesso ai dati del gestore code e ai file di log. Le attività mostrano come creare un gestore code autorizzato a leggere e scrivere dati e file di log memorizzati in una directory di propria scelta. Accompagnano l'attività, “Domini Windows e gestori code a più istanze” a pagina 351.

In questa attività, si crea un gestore code che memorizza i dati e i log in una directory remota su un file server. Ai fini di questo esempio, il server di file è lo stesso server del controller di dominio. La directory contenente le cartelle di dati e di log è condivisa con l'autorizzazione di controllo completo fornita al gruppo globale wmqha.

Procedura

1. Accedere al server di dominio, *mars*, come amministratore locale, *mars*\Administrator.
2. Apri una finestra di comando.
3. Riavviare il servizio IBM IBM WebSphere MQ .

   È necessario riavviare il servizio in modo che l'ID utente con cui viene eseguito acquisisca le ulteriori credenziali di sicurezza configurate per esso.

   Immettere i comandi:

   ```
   endmqsvc
   strmqsvc
   ```

   Le risposte del sistema:

   ```
   5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
   The MQ service for installation 'Installation1' ended successfully.
   ```

```
E:
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
The MQ service for installation 'Installation1' started successfully.
```

4. Creare il gestore code.

```
crtmqm -a wmq\wmqha -sax -u SYSTEM.DEAD.LETTER.QUEUE -md \\sun\wmq\data -ld \\sun\wmq\logs
QMGR
```

È necessario specificare il dominio, *wmq*, del gruppo di protezione alternativo *wmqha* specificando il nome dominio completo del gruppo globale *"wmq\wmqha"*.

È necessario specificare il nome UNC (Universal Naming Convention) della condivisione *\\sun\wmq*e non utilizzare un riferimento unità mappato.

La risposta del sistema:

```
WebSphere MQ queue manager created.
Directory '\\sun\wmq\data\QMGR' created.
The queue manager is associated with installation '1'
Creating or replacing default objects for queue manager 'QMGR'
Default objects statistics : 74 created. 0 replaced.
Completing setup.
Setup completed.
```

Operazioni successive

Verificare il gestore code inserendo e ricevendo un messaggio in una coda.

1. Avviare il gestore code.

```
strmqm QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' starting.
The queue manager is associated with installation '1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
WebSphere MQ queue manager 'QMGR' started using V7.1.0.0.
```

2. Creare una coda di test.

```
echo define qlocal(QTEST) | runmqsc QMGR
```

La risposta del sistema:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QMGR.


     1 : define qlocal(QTEST)
AMQ8006: WebSphere MQ queue created.
One MQSC command read.
No commands have a syntax error.
All valid MQSC commands were processed.
```

3. Inserire un messaggio di verifica utilizzando il programma di esempio **amqsput**.

```
echo 'A test message' | amqsput QTEST QMGR
```

La risposta del sistema:

```
Sample AMQSPUT0 start
target queue is QTEST
Sample AMQSPUT0 end
```

4. Richiamare il messaggio di test utilizzando il programma di esempio **amqsget**.

   ```
   amqsget QTEST QMGR
   ```

   La risposta del sistema:

   ```
   Sample AMQSGET0 start
   message <A test message>
   Wait 15 seconds ...
   no more messages
   Sample AMQSGET0 end
   ```

5. Chiudere il gestore code.

   ```
   endmqm -i QMGR
   ```

   La risposta del sistema:

   ```
   WebSphere MQ queue manager 'QMGR' ending.
   WebSphere MQ queue manager 'QMGR' ended.
   ```

6. Eliminare il gestore code.

   ```
   dltmqm QMGR
   ```

   La risposta del sistema:

   ```
   WebSphere MQ queue manager 'QMGR' deleted.
   ```

7. Eliminare le directory create.

   Suggerimento: Aggiungere l'opzione /Q ai comandi per evitare che il comando richieda di eliminare ogni file o directory.

   ```
   del /F /S C:\wmq\*.*
   rmdir /S C:\wmq
   ```

Crea un gestore code a più istanze sui controller di dominio
Un esempio mostra come configurare un gestore code a più istanze su Windows sui controller di dominio. La configurazione dimostra i concetti coinvolti, piuttosto che essere una scala di produzione. L'esempio si basa su Windows Server 2008. La procedura potrebbe differire su altre versioni di Windows Server.

La configurazione utilizza il concetto di mini - dominio o "domainlet"; consultare Nodi cluster di Windows 2000, Windows Server 2003 e Windows Server 2008 come controller di dominio. Per aggiungere gestori code a più istanze a un dominio esistente, consultare “Crea un gestore code a più istanze su server o workstation di dominio” a pagina 352.

La configurazione di esempio è composta da tre server:

sun
: Un server Windows Server 2008 utilizzato come primo controller di dominio. Definisce il dominio *wmq.example.com* che contiene *sun*, *earth*e *mars*. Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

earth
: Un server Windows Server 2008 utilizzato come secondo controller di dominio IBM WebSphere MQ . Contiene la seconda istanza del gestore code a più istanze denominato *QMGR*.

mars
: Un Windows Server 2008 utilizzato come server di file.

Sostituire i nomi in corsivo nell'esempio, con nomi di propria scelta.

Prima di iniziare

1. Su Windows, non è necessario verificare il file system su cui si intende memorizzare i dati del gestore code e i file di log. La procedura di controllo, Verifica del funzionamento del file system condiviso , è applicabile a UNIX and Linux. In Windows, le verifiche hanno sempre esito positivo.
2. Eseguire le operazioni in “Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ” a pagina 355 per creare il primo controller di dominio.
3. Eseguire le operazioni in “Aggiunta di un secondo controller di dominio al dominio wmq.example.com” a pagina 369 per aggiungere un secondo controller di dominio, installare IBM WebSphere MQ for Windows su entrambi i controller di dominio e verificare le installazioni.
4. Effettuare le operazioni riportate in “Installazione di IBM WebSphere MQ sui controller di dominio nel dominio wmq.example.com” a pagina 371 per installare IBM WebSphere MQ sui due controller di dominio.

Informazioni su questa attività

Su un file server nello stesso dominio, creare una condivisione per le directory di dati e di log del gestore code. Successivamente, creare la prima istanza di un gestore code a più istanze che utilizzi la condivisione file su uno dei controller di dominio. Creare l'altra istanza sull'altro controller di dominio e infine verificare la configurazione. È possibile creare la condivisione file su un controller di dominio.

Nell'esempio, *sun* è la prima unità di controllo del dominio, *earth* la seconda e *mars* è il server di file.

Procedura

1. Creare le directory che devono contenere i file di log e i dati del gestore code.
   a) Su *mars*, immettere il comando:

   ```
   md c:\wmq\data , c:\wmq\logs
   ```

2. Condividere le directory che devono contenere i file di log e i dati del gestore code.

   È necessario consentire l'accesso di controllo completo al gruppo locale del dominio mqme all'ID utente utilizzato per creare il gestore code. Nell'esempio, gli ID utente membri di Domain Administrators hanno l'autorità per creare i gestori code.

   La condivisione file deve essere su un server che si trovi nello stesso dominio dei controller di dominio. Nell'esempio, il server *mars* si trova nello stesso dominio dei controller di dominio.

   a) In Windows Explorer, fare clic con il pulsante destro del mouse su ***c: \wmq*** > **Proprietà**.
   b) Fare clic sulla scheda **Sicurezza** , quindi su **Avanzate** > **Modifica ...**.
   c) Deselezionare la check box per **Includi autorizzazioni ereditabili dal proprietario di questo oggetto**. Fare clic su **Copia** nella finestra Sicurezza di Windows.
   d) Selezionare le linee per gli utenti nell'elenco **Voci di autorizzazione** e fare clic su **Rimuovi**. Lasciare le righe per SYSTEM, Administrators e CREATOR OWNER nell'elenco **Voci di autorizzazione**.
   e) Fare clic su **Aggiungi ...**, e immettere il nome del gruppo locale del dominio *mqm*. Fare clic su **Verifica nomi**
   f) In risposta a una finestra di sicurezza di Windows, immettere il nome e la password di Domain Administrator e fare clic su **OK** > **OK**.
   g) Nella finestra Immissione per wmq , selezionare **Controllo completo** nell'elenco di **Autorizzazioni**.
   h) Fare clic su **OK** > **Applica** > **OK** > **OK** > **OK**
   i) Ripetere i passi e per h per aggiungere Domain Administrators.
   j) In Windows Explorer, fare clic con il pulsante destro del mouse su ***c: \wmq*** > **Condividi ...**.
   k) Fare clic su **Condivisione avanzata ...** e selezionare la casella di spunta **Condividi questa cartella** . Lasciare il nome condivisione come *wmq*.

l) Fare clic su **Autorizzazioni** > **Aggiungi ...**, e immettere il nome del gruppo locale del dominio *mqm*; `Domain Administrators`. Fare clic su **Verifica nomi**.

m) In risposta a una finestra di sicurezza di Windows, immettere il nome e la password di `Domain Administrator` e fare clic su **OK** > **OK**.

3. Creare il gestore code *QMGR* sul primo controller di dominio, *sun*.

```
crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE -md \\mars\wmq\data -ld \\mars\wmq\logs  QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager created.
Directory '\\mars\wmq\data\QMGR' created.
The queue manager is associated with installation 'Installation1'.
Creating or replacing default objects for queue manager 'QMGR'.
Default objects statistics : 74 created. 0 replaced. 0 failed.
Completing setup.
Setup completed.
```

4. Avviare il gestore code su *sun*, consentendo un'istanza in standby.

```
strmqm -x QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
WebSphere MQ queue manager 'QMGR' started using V7.1.0.0.
```

5. Creare una seconda istanza di *QMGR* su *earth*.

a) Controllare che i parametri `Prefisso` e `InstallationName` siano corretti per *earth*.

In *sun*, eseguire il comando **dspmqinf** :

```
dspmqinf QMGR
```

La risposta del sistema:

```
QueueManager:
   Name=QMGR
   Directory=QMGR
   Prefix=C:\Program Files\IBM\WebSphere MQ
   DataPath=\\mars\wmq\data\QMGR
   InstallationName=Installation1
```

b) Copiare il formato leggibile dalla macchina della stanza **QueueManager** negli appunti.

Su *sun* eseguire nuovamente il comando **dspmqinf** , con il parametro `-o command` .

```
dspmqinf -o command QMGR
```

La risposta del sistema:

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\Program Files\IBM\WebSphere MQ"
-v DataPath=\\mars\wmq\data\QMGR
```

c) In *earth* eseguire il comando **addmqinf** dagli appunti per creare un'istanza del gestore code su *earth*.

Modificare il comando, se necessario, per adattare le differenze nei parametri `Prefisso` o `InstallationName` .

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\Program Files\IBM\WebSphere MQ"
-v DataPath=\\mars\wmq\data\QMGR
```

```
WebSphere MQ configuration information added.
```

6. Avviare l'istanza in standby del gestore code in *earth*.

```
strmqm -x QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
A standby instance of queue manager 'QMGR' has been started. The active
instance is running elsewhere.
```

Risultati

Verificare che il gestore code passi da *sun* a *earth*:

1. Su *sun*, eseguire il seguente comando:

```
endmqm -i -r -s QMGR
```

La risposta del sistema su *sun*:

```
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ended, permitting switchover to
a standby instance.
```

2. Su *earth* immettere ripetutamente il comando:

```
dspmq
```

Le risposte del sistema:

```
QMNAME(QMGR) STATUS(Running as standby)
QMNAME(QMGR) STATUS(Running as standby)
QMNAME(QMGR) STATUS(Running)
```

Operazioni successive

Per verificare un gestore code a più istanze utilizzando programmi di esempio, consultare “Verificare il gestore code a più istanze su Windows” a pagina 373.

Attività correlate

“Aggiunta di un secondo controller di dominio al dominio wmq.example.com” a pagina 369

“Installazione di IBM WebSphere MQ sui controller di dominio nel dominio wmq.example.com” a pagina 371

Informazioni correlate

Nodi cluster di Windows 2000, Windows Server 2003 e Windows Server 2008 come controller di dominio

Aggiunta di un secondo controller di dominio al dominio wmq.example.com

Aggiungere un secondo controller di dominio al dominio *wmq.example.com* per creare un dominio Windows in cui eseguire gestori code a più istanze su controller di dominio e server di file.

La configurazione di esempio è composta da tre server:

sun
Un server Windows Server 2008 utilizzato come primo controller di dominio. Definisce il dominio *wmq.example.com* che contiene *sun*, *earth*e *mars*. Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

earth
Un server Windows Server 2008 utilizzato come secondo controller di dominio IBM WebSphere MQ . Contiene la seconda istanza del gestore code a più istanze denominato *QMGR*.

mars
Un Windows Server 2008 utilizzato come server di file.

Sostituire i nomi in corsivo nell'esempio, con nomi di propria scelta.

Prima di iniziare

1. Effettuare le operazioni in "Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ" a pagina 355 per creare un controller di dominio, *sun*, per il dominio *wmq.example.com*. Modificare i nomi in corsivo per adattarli alla propria configurazione.
2. Installare Windows Server 2008 su un server nel gruppo di lavoro predefinito, WORKGROUP. Per l'esempio, il server è denominato *earth*.

Informazioni su questa attività

In questa attività si configura un Windows Server 2008, denominato *earth*, come secondo controller di dominio nel dominio *wmq.example.com* .

Questa attività è una delle attività correlate che illustrano l'accesso ai dati del gestore code e ai file di log. Le attività mostrano come creare un gestore code autorizzato a leggere e scrivere dati e file di log memorizzati in una directory di propria scelta. Accompagnano l'attività, "Domini Windows e gestori code a più istanze" a pagina 351.

Procedura

1. Aggiungere il controller di dominio, *sun.wmq.example.com* a *earth* come server DNS.
   a) Su *earth*, collegarsi come *earth*\Administrator e fare clic su **Avvia**.
   b) Fare clic con il pulsante destro del mouse su **Rete** > **Proprietà** > **Gestisci connessioni di rete**.
   c) Fare clic con il tasto destro del mouse sull'adattatore di rete, fare clic su **Proprietà**.

      Il sistema risponde con la finestra Proprietà connessione area locale che elenca le voci utilizzate dalla connessione.
   d) Selezionare **Internet Protocol Versione 4** o **Internet Protocol Versione 6** dall'elenco di voci nella finestra Proprietà connessione area locale. Fare clic su **Proprietà** > **Avanzate ...** e fare clic sul separatore **DNS** .
   e) Sotto gli indirizzi server DNS, fare clic su **Aggiungi ...**.
   f) Immettere l'indirizzo IP del controller di dominio, che è anche il server DNS, e fare clic su **Aggiungi**.
   g) Fare clic su **Aggiungi questi suffissi DNS** > **Aggiungi ...**.
   h) Immettere *wmq.example.com* e fare clic su **Aggiungi**.
   i) Immettere *wmq.example.com* nel campo **Suffisso DNS per questa connessione** .
   j) Seleziona **Register this connection's address in DNS** e **Use this connection's suffix in DNS registration**. Fare clic su **OK** > **OK** > **Chiudi**
   k) Aprire una finestra comandi e immettere il comando **ipconfig /all** per esaminare le impostazioni TCP/IP.
2. Accedere al controller di dominio, *sun*, come amministratore locale o Workgroup .

Se il server è già configurato come controller di dominio, è necessario collegarsi come amministratore di dominio.

3. Eseguire la procedura guidata Servizi dominio di Active Directory .
   a) Fare clic su **Avvia** > **Esegui ...** Immettere `dcpromo` e fare clic su **OK**.

   Se i file binari di Active Directory non sono già installati, Windows installa automaticamente i file.
4. Configurare *earth* come secondo controller di dominio nel dominio *wmq.example.com* .
   a) Nella prima finestra della procedura guidata, lasciare deselezionata la check box **Utilizza installazione in modalità avanzata** . Fare clic su **Avanti** > **Avanti** e fare clic su **Crea Aggiungi un controller di dominio a un dominio esistente** > **Avanti**.
   b) Immettere *wmq* in **Immettere il nome di qualsiasi dominio in questa struttura ...** . Si fa clic sul pulsante di opzione **Credenziali alternative** , quindi su **Imposta ...**. Immettere il nome e la password dell'amministratore del dominio e fare clic su **OK** > **Avanti** > **Avanti** > **Avanti**.
   c) Nella finestra Opzioni aggiuntive controller di dominio, accettare le opzioni **Server DNS** e **Catalogo globale** , che sono selezionate; fare clic su **Avanti** > **Avanti**.
   d) In Directory Services Restore Mode Administrator Password, immettere **Password** e **Conferma password** e fare clic su **Avanti** > **Avanti**.
   e) Quando viene richiesto **Credenziali di rete**, immettere la password dell'amministratore del dominio. Selezionare **Riavvia al completamento** nella finestra finale della procedura guidata.
   f) Dopo un po' di tempo, potrebbe aprirsi una finestra con un errore **DCPromo** relativo alla delega DNS; fare clic su **OK**. Il server viene riavviato.

Risultati

Una volta riavviato *earth* , accedere come amministratore del dominio. Verificare che il dominio `wmq.example.com` sia stato replicato in *earth*.

Operazioni successive

Continuare con l'installazione di IBM WebSphere MQ; consultare “Installazione di IBM WebSphere MQ sui controller di dominio nel dominio wmq.example.com” a pagina 371.

Attività correlate

“Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ” a pagina 355

Installazione di IBM WebSphere MQ sui controller di dominio nel dominio wmq.example.com
Installare e configurare le installazioni di IBM WebSphere MQ su entrambi i controller di dominio nel dominio *wmq.example.com* .
Inserire qui una breve descrizione; utilizzata per il primo paragrafo e la sintesi.

La configurazione di esempio è composta da tre server:

sun
Un server Windows Server 2008 utilizzato come primo controller di dominio. Definisce il dominio *wmq.example.com* che contiene *sun*, *earth*e *mars*. Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

earth
Un server Windows Server 2008 utilizzato come secondo controller di dominio IBM WebSphere MQ . Contiene la seconda istanza del gestore code a più istanze denominato *QMGR*.

mars
Un Windows Server 2008 utilizzato come server di file.

Sostituire i nomi in corsivo nell'esempio, con nomi di propria scelta.

Prima di iniziare

1. Effettuare le operazioni in “Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ” a pagina 355 per creare un controller di dominio, *sun*, per il dominio *wmq.example.com*. Modificare i nomi in corsivo per adattarli alla propria configurazione.
2. Effettuare le operazioni riportate in “Aggiunta di un secondo controller di dominio al dominio wmq.example.com” a pagina 369 per creare un secondo controller di dominio, *earth*, per il dominio *wmq.example.com*. Modificare i nomi in corsivo per adattarli alla propria configurazione.
3. Consultare Requisiti hardware e software sui Windows sistemi per altre versioni di Windows su cui è possibile eseguire IBM WebSphere MQ .

Informazioni su questa attività

Installare e configurare le installazioni di IBM WebSphere MQ su entrambi i controller di dominio nel dominio *wmq.example.com* .

Procedura

1. Installare IBM WebSphere MQ su *sun* e *earth*.

   Per ulteriori informazioni sull'esecuzione della procedura guidata di installazione di IBM WebSphere MQ for Windows , consultare Installazione del server IBM WebSphere MQ su Windows .

   a) Su *sun* e *earth*, accedere come amministratore del dominio, *wmq*\Administrator.

   b) Eseguire il comando **Setup** sul supporto di installazione IBM WebSphere MQ for Windows .

      Viene avviata l'applicazione IBM WebSphere MQ Launchpad.

   c) Fare clic su **Requisiti software** per verificare che il software prerequisito sia installato.

   d) Fare clic su **Configurazione di rete** > **No**.

      È possibile configurare o meno un ID utente di dominio per questa installazione. L'ID utente creato è un ID utente locale del dominio.

   e) Fare clic su **WebSphere MQ Installazione**, selezionare una lingua di installazione e fare clic su Avvia IBM IBM WebSphere MQ Installer.

   f) Confermare l'accordo di licenza e fare clic su **Avanti** > **Avanti** > **Installa** per accettare la configurazione predefinita. Attendere il completamento dell'installazione e fare clic su **Fine**.

      Se si desidera modificare il nome dell'installazione, installare componenti differenti, configurare una directory differente per i dati e i log del gestore code oppure eseguire l'installazione in una directory diversa, fare clic su **Personalizzato** anziché su **Tipico**.

      IBM WebSphere MQ è installato e il programma di installazione avvia la procedura guidata "Prepara IBM WebSphere MQ" .

   L'installazione di IBM WebSphere MQ for Windows configura un gruppo locale di dominio `mqme` un gruppo di dominio `Domain mqm`. Rende `Domain mqm` un membro di `mqm`. I controller di dominio successivi nello stesso dominio condividono i gruppo `mqm` e `Domain mqm` .
2. Su *earth* e *sun*, eseguire la procedura guidata "Prepara IBM WebSphere MQ" .

   Per ulteriori informazioni sull'esecuzione della procedura guidata "Prepara IBM WebSphere MQ" , consultare Configurazione di WebSphere MQ con la procedura guidata Prepara WebSphere MQ .

   a) Il programma di installazione IBM WebSphere MQ esegue automaticamente "Prepara IBM WebSphere MQ" .

      Per avviare la procedura guidata manualmente, individuare il collegamento alla cartella "Prepara IBM WebSphere MQ" in **Avvia** > **Tutti i programmi** > **IBM WebSphere MQ** . Selezionare il collegamento che corrisponde all'installazione di IBM WebSphere MQ in una configurazione a più installazioni.

b) Fare clic su **Avanti** e lasciare **No** selezionato in risposta alla domanda "Identifica se nella rete è presente un controller di dominio Windows 2000 o successivo"[1].

c) Nella pagina finale della procedura guidata, selezionare o deselezionare le caselle di spunta richieste e fare clic su **Fine**.

La procedura guidata "Prepara IBM WebSphere MQ" consente di creare un utente locale di dominio `MUSR_MQADMIN` sul primo controller di dominio e un altro utente locale di dominio `MUSR_MQADMIN1` sul secondo controller di dominio. La procedura guidata crea il servizio IBM IBM WebSphere MQ su ciascun controller, con `MUSR_MQADMIN` o `MUSR_MQADMIN1` come utente che accede al servizio.

3. Definire un utente che dispone dell'autorizzazione per creare un gestore code.

   L'utente deve avere il diritto di accedere localmente e deve essere membro del gruppo `mqm` locale del dominio. Sui controller di dominio, gli utenti di dominio non hanno il diritto di accedere localmente, ma gli amministratori sì. Per impostazione predefinita, nessun utente ha entrambi questi attributi. In questa attività, aggiungere amministratori di dominio al gruppo `mqm` locale del dominio.

   a) Aprire **Server Manager** > **Ruoli** > **Active Directory Domain Services** > ***wmq.example.com*** > **Utenti**.

   b) Fare clic con il tasto destro del mouse su **Admin dominio** > **Aggiungi a un gruppo ...** e digitare `mqm`; fare clic su **Verifica nomi** > **OK** > **OK**

Risultati

1. Verificare che "Prepara IBM WebSphere MQ" abbia creato l'utente del dominio, `MUSR_MQADMIN`:

   a. Aprire **Server Manager** > **Ruoli** > **Active Directory Domain Services** > ***wmq.example.com*** > **Utenti**.

   b. Fare clic con il tasto destro del mouse su **MUSR_MQADMIN** > **Proprietà ...** > **Membro di**e vedere che è un membro di `Domain users` e `mqm`.

2. Verificare che `MUSR_MQADMIN` abbia il diritto di essere eseguito come servizio:

   a. Fare clic suFare clic su **Avvia** > **Esegui ...**, immettere il comando **`secpol.msc`** e fare clic su **OK**.

   b. Aprire **Impostazioni di protezione** > **Politiche locali** > **Assegnazione diritti utente**. Nell'elenco delle politiche, fare clic con il tasto destro del mouse su **Accedi come servizio** > **Proprietà**e vedi `MUSR_MQADMIN` è elencato come avente il diritto di accedere come un servizio. Fare clic su **OK**.

Operazioni successive

1. Eseguire l'attività, “Lettura e scrittura di dati e file di log autorizzati dal gruppo mqm locale” a pagina 381, per verificare che l'installazione e la configurazione stiano funzionando correttamente.
2. Tornare all'attività, “Crea un gestore code a più istanze sui controller di dominio” a pagina 366, per completare l'attività di configurazione di un gestore code a più istanze sui controller di dominio.

Concetti correlati

Diritti utente necessari per un servizio Windows di WebSphere MQ

Verificare il gestore code a più istanze su Windows

Utilizzare i programmi di esempio **amqsghac**, **amqsphac** e **amqsmhac** per verificare la configurazione di un gestore code a più istanze. Questo argomento fornisce una configurazione di esempio per verificare la configurazione di un gestore code a più istanze su Windows Server 2003.

I programmi di esempio ad alta disponibilità utilizzano la riconnessione client automatica. Quando il gestore code connesso ha esito negativo, il client tenta di riconnettersi a un gestore code nello stesso gruppo di gestori code. La descrizione degli esempi, Programmi di esempio ad alta disponibilità, illustra la riconnessione del client utilizzando un gestore code a istanza singola per semplicità. È possibile utilizzare gli stessi esempi con i gestori code a più istanze per verificare una configurazione del gestore code a più istanze.

[1] È possibile configurare l'installazione per il dominio. Poiché tutti gli utenti e i gruppi su un controller di dominio hanno un ambito di dominio, non fa alcuna differenza. È più semplice installare IBM WebSphere MQ come se non fosse nel dominio.

Questo esempio usa la configurazione a più istanze descritta in “Crea un gestore code a più istanze sui controller di dominio” a pagina 366. Utilizzare la configurazione per verificare che il gestore code a più istanze passi all'istanza in standby. Arrestare il gestore code con il comando **endmqm** e utilizzare l'opzione `-s`, switchover,. I programmi client si riconnettono alla nuova istanza del gestore code e continuano a lavorare con la nuova istanza dopo un leggero ritardo.

Il client è installato in un'immagine VMware da 400 MB su cui è in esecuzione Windows XP Service Pack 2. Per motivi di sicurezza, è connesso sulla stessa rete solo host VMware dei server di dominio che eseguono il gestore code a più istanze. Condivide la cartella `/MQHA` , che contiene la tabella di connessione client, per semplificare la configurazione.

Verifica del failover mediante WebSphere MQ Explorer

Prima di utilizzare le applicazioni di esempio per verificare il failover, eseguire WebSphere MQ Explorer su ciascun server. Aggiungere entrambe le istanze del gestore code a ciascun explorer utilizzando la procedura guidata **Aggiungi gestore code remoto> Connetti direttamente a gestore code a più istanze** . Verificare che entrambe le istanze siano in esecuzione, consentendo lo standby. Chiudere la finestra eseguendo l'immagine VMware con l'istanza attiva, spegnendo virtualmente il server o arrestando l'istanza attiva, consentendo la commutazione dell'istanza in standby e la riconnessione dei client.

Nota: Se si spegne il server, assicurarsi che non sia quello che ospita la cartella `MQHA` !

Nota: L'opzione **Consenti commutazione a un'istanza in standby** potrebbe non essere disponibile nella finestra di dialogo **Arresta gestore code** . L'opzione è mancante perché il gestore code è in esecuzione come gestore code a istanza singola. È necessario che sia stato avviato senza l'opzione **Consenti un'istanza standby** . Se la tua richiesta di arrestare il gestore code viene rifiutata, guarda la finestra **Details** , probabilmente non c'è alcuna istanza in standby in esecuzione.

Verifica del failover utilizzando i programmi di esempio

Scegliere un server per eseguire l'istanza attiva

È possibile che sia stato scelto uno dei server per ospitare la directory o il file system `MQHA` . Se si prevede di verificare il failover chiudendo la finestra VMware che esegue il server attivo, assicurarsi che non sia quello che ospita `MQHA`!

Sul server che esegue l'istanza del gestore code attivo

1. Modificare *ipaddr1* e *ipaddr2* e salvare i seguenti comandi in `N:\hasample.tst.`

```
DEFINE QLOCAL(SOURCE) REPLACE
DEFINE QLOCAL(TARGET) REPLACE
DEFINE CHANNEL(CHANNEL1) CHLTYPE(SVRCONN)   TRPTYPE(TCP) +
       MCAUSER(' ') REPLACE
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN)  TRPTYPE(TCP) +
       CONNAME('ipaddr1(1414),ipaddr2(1414)') QMNAME(QM1) REPLACE
START  CHANNEL(CHANNEL1)
DEFINE LISTENER(LISTENER.TCP) TRPTYPE(TCP) CONTROL(QMGR)
DISPLAY LISTENER(LISTENER.TCP) CONTROL
DISPLAY LSSTATUS(LISTENER.TCP) STATUS
```

   Nota: Lasciando vuoto il parametro **MCAUSER** , l'ID utente client viene inviato al server. L'ID utente client deve avere le autorizzazioni corrette sui server. Un'alternativa è quella di impostare il parametro **MCAUSER** nel canale SVRCONN sull'ID utente configurato sul server.

2. Aprire un prompt dei comandi con il percorso `N:\` ed eseguire il comando:

```
runmqsc -m QM1 < hasample.tst
```

3. Verificare che il listener sia in esecuzione e che disponga del controllo del gestore code, ispezionando l'output del comando **runmqsc** .

```
 LISTENER(LISTENER.TCP)CONTROL(QMGR)
 LISTENER(LISTENER.TCP)STATUS(RUNNING)
```

   Oppure, utilizzando WebSphere MQ Explorer che il listener TCPIP è in esecuzione e dispone di `Control = Queue Manager`.

Sul client

1. Associare la directory condivisa `C:\MQHA` sul server a `N:\` sul client.
2. Aprire un prompt dei comandi con il percorso `N:\` . Impostare la variabile di ambiente `MQCHLLIB` in modo che punti alla tabella di definizione del canale client (CCDT) sul server:

   ```
   SET MQCHLLIB=N:\data\QM1\@ipcc
   ```

3. Al prompt dei comandi immettere i seguenti comandi:

   ```
   start amqsghac TARGET QM1
   start amqsmhac -s SOURCE -t TARGET -m QM1
   start amqsphac SOURCE QM1
   ```

   Nota: In caso di problemi, avviare le applicazioni da un prompt dei comandi in modo che il codice di errore venga stampato sulla console oppure consultare AMQERR01.LOG nella cartella `N:\data\QM1\errors` .

Sul server che esegue l'istanza del gestore code attivo

1. Le alternative sono:
   - Chiudere la finestra che esegue l'immagine VMware con l'istanza del server attiva.
   - Utilizzando Esplora risorse di WebSphere MQ , arrestare l'istanza del gestore code attivo, consentendo il passaggio all'istanza in standby e istruendo i client ricollegabili a riconnettersi.
2. I tre client alla fine rilevano che la connessione è interrotta e quindi si ricollegano. In questa configurazione, se si chiude la finestra del server, sono necessari circa sette minuti perché tutte e tre le connessioni vengano ristabilite. Alcune connessioni vengono ristabilite ben prima di altre.

Risultati

```
N:\>amqsphac SOURCE QM1
Sample AMQSPHAC start
target queue is SOURCE
message <Message 1>
message <Message 2>
message <Message 3>
message <Message 4>
message <Message 5>
17:05:25 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:52 : EVENT : Connection Reconnected
message <Message 6>
message <Message 7>
message <Message 8>
message <Message 9>
```

```
N:\>amqsmhac -s SOURCE -t TARGET -m QM1
Sample AMQSMHA0 start

17:05:25 : EVENT : Connection Reconnecting (Delay: 97ms)
17:05:48 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:53 : EVENT : Connection Reconnected
```

```
N:\>amqsghac TARGET QM1
Sample AMQSGHAC start
message <Message 1>
message <Message 2>
message <Message 3>
message <Message 4>
message <Message 5>
17:05:25 : EVENT : Connection Reconnecting (Delay: 156ms)
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:52 : EVENT : Connection Reconnected
message <Message 6>
message <Message 7>
message <Message 8>
message <Message 9>
```

Proteggere i dati del gestore code condiviso e le directory di log e i file su Windows
Questo argomento descrive come proteggere un'ubicazione condivisa per i dati del gestore code e i file di log utilizzando un gruppo di sicurezza alternativo globale. È possibile condividere l'ubicazione tra diverse istanze di un gestore code in esecuzione su server differenti.

Generalmente, non si imposta un'ubicazione condivisa per i dati del gestore code e i file di log. Quando si installa IBM WebSphere MQ for Windows, il programma di installazione crea una directory home di propria scelta per tutti i gestori code creati su tale server. Protegge le directory con il gruppo `mqm` locale e configura un ID utente per il servizio IBM IBM WebSphere MQ per accedere alle directory.

Quando si protegge una cartella condivisa con un gruppo di sicurezza, un utente a cui è consentito accedere alla cartella deve disporre delle credenziali del gruppo. Si supponga che una cartella su un server di file remoto sia protetta con il gruppo `mqm` locale su un server denominato *`mars`*. Rendere l'utente che esegue i processi del gestore code un membro del gruppo `mqm` locale su *`mars`*. L'utente dispone di credenziali che corrispondono a quelle della cartella sul file server remoto. Utilizzando queste credenziali, il gestore code è in grado di accedere ai propri dati e file di log nella cartella. L'utente che esegue i processi del gestore code su un server differente è membro di un gruppo `mqm` locale diverso che non dispone di credenziali corrispondenti. Quando il gestore code viene eseguito su un altro server su *`mars`*, non può accedere ai dati e ai file di log che ha creato quando è stato eseguito su *`mars`* . Anche se si rende l'utente un utente di dominio, ha credenziali diverse, perché deve acquisire le credenziali dal gruppo `mqm` locale su *`mars`*e non può farlo da un server diverso.

Fornire al gestore code un gruppo di sicurezza alternativo globale risolve il problema; consultare Figura 64 a pagina 377 . Proteggere una cartella remota con un gruppo globale. Passare il nome del gruppo globale al gestore code quando lo si crea su *`mars`*. Inoltrare il nome del gruppo globale come gruppo di protezione alternativo utilizzando il parametro `-a[r]` sul comando **`crtmqm`** . Se si trasferisce il gestore code per l'esecuzione su un server differente, il nome del gruppo di protezione viene trasferito con esso. Il nome viene trasferito nella stanza **AccessMode** nel file `qm.ini` come `SecurityGroup`; ad esempio:

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

La stanza **AccessMode** in `qm.ini` include anche `RemoveMQMAccess`; ad esempio:

```
AccessMode:
   RemoveMQMAccess=<true\false>
```

Se questo attributo viene specificato con il valore `true`ed è stato fornito anche un gruppo di accesso, al gruppo mqm locale non viene concesso l'accesso ai file di dati del gestore code.

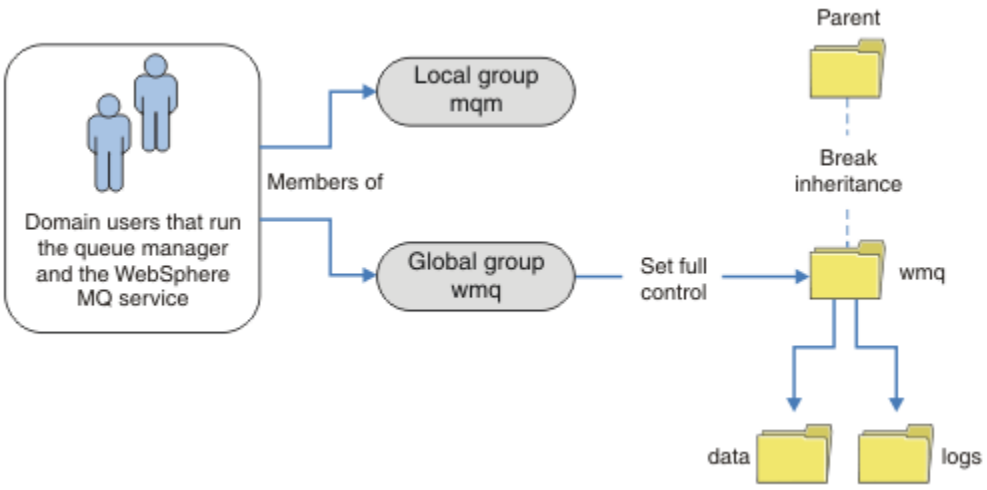


Figura 64. Protezione dei dati e dei log del gestore code mediante un gruppo di sicurezza globale alternativo (1)

Per l'ID utente con cui devono essere eseguiti i processi del gestore code per avere le credenziali corrispondenti del gruppo di sicurezza globale, l'ID utente deve avere anche un ambito globale. Non è possibile rendere un gruppo locale o un principal un membro di un gruppo globale. In Figura 64 a pagina 377 , gli utenti che eseguono i processi del gestore code vengono visualizzati come utenti del dominio.

Se si distribuiscono molti server IBM WebSphere MQ , il raggruppamento di utenti in Figura 64 a pagina 377 non è conveniente. È necessario ripetere il processo di aggiunta di utenti ai gruppi locali per ogni server IBM WebSphere MQ . Creare invece un gruppo globale `Domain mqm` sul controller di dominio e rendere gli utenti che eseguono i membri IBM WebSphere MQ del gruppo `Domain mqm` ; consultare Figura 65 a pagina 378 . Quando si installa IBM WebSphere MQ come installazione di dominio, la procedura guidata "Prepara IBM WebSphere MQ" rende automaticamente il gruppo `Domain mqm` membro del gruppo `mqm` locale. Gli stessi utenti si trovano in entrambi i gruppi globali `Domain mqm` e `wmq`.

Suggerimento: Gli stessi utenti possono eseguire IBM WebSphere MQ su server differenti, ma su un singolo server è necessario disporre di utenti differenti per eseguire IBM WebSphere MQ come servizio ed eseguire in modo interattivo. È inoltre necessario disporre di utenti differenti per ogni installazione su un server. Di solito, quindi, `Domain mqm` contiene un numero di utenti.

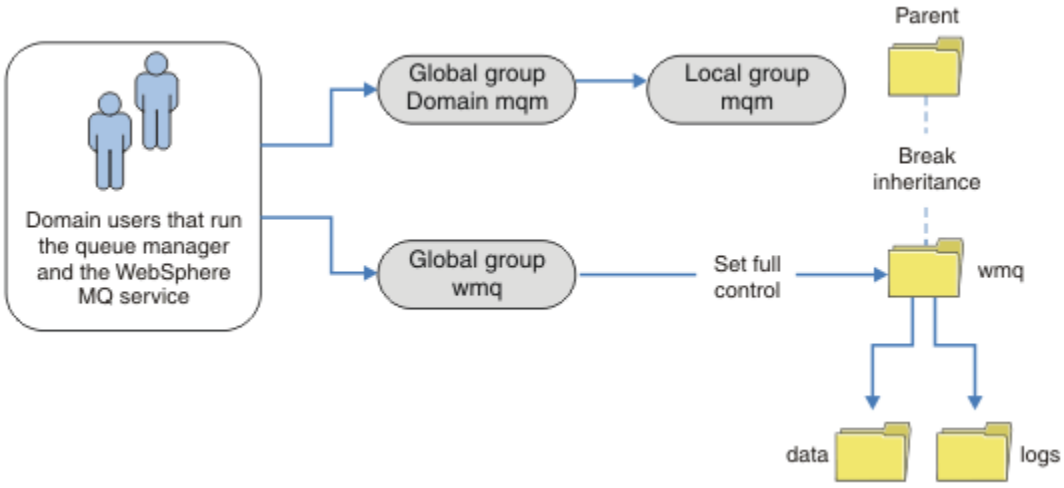


Figura 65. Protezione dei dati e dei log del gestore code utilizzando un gruppo di sicurezza globale alternativo (2)

L'organizzazione in Figura 65 a pagina 378 è inutilmente complicata così com' è. L'accordo ha due gruppi globali con membri identici. È possibile semplificare l'organizzazione e definire solo un gruppo globale; consultare Figura 66 a pagina 378.

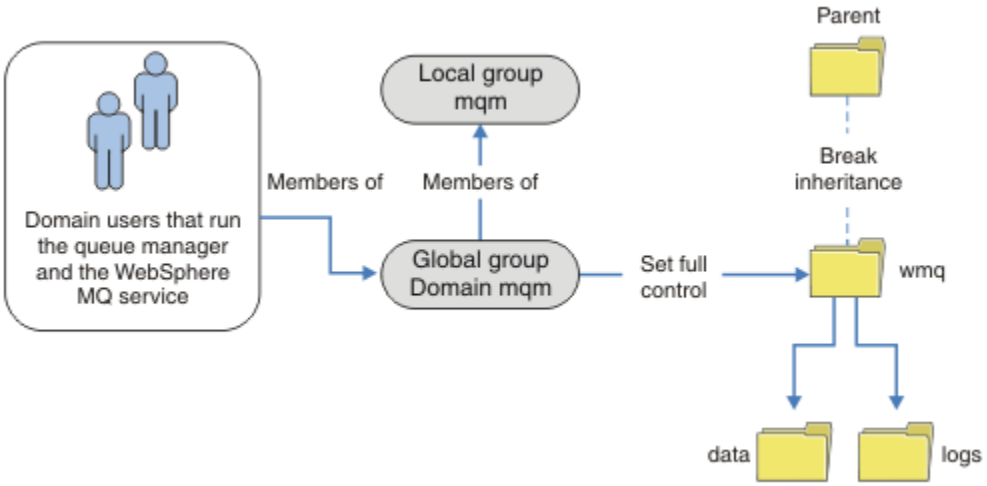


Figura 66. Protezione dei log e dei dati del gestore code utilizzando un gruppo di sicurezza globale alternativo (3)

In alternativa, potrebbe essere necessario un livello più elevato di controllo degli accessi, con diversi gestori code limitati ad accedere a cartelle differenti; consultare Figura 67 a pagina 379. In Figura 67 a pagina 379, sono definiti due gruppi di utenti del dominio, in gruppi globali separati per proteggere i diversi file di dati e di log del gestore code. Vengono visualizzati due diversi gruppi `mqm` locali, che devono trovarsi su server IBM WebSphere MQ diversi. In questo esempio, i gestori code sono suddivisi in due insiemi, con utenti differenti assegnati ai due insiemi. I due set potrebbero essere gestori code di test e di produzione. I gruppi di sicurezza alternativi sono denominati `wmq1` e `wmq2` . È necessario aggiungere manualmente i gruppi globali `wmq1` e `wmq2` ai gestori code corretti in base al fatto che si trovino nel dipartimento di test o di produzione. La configurazione non può trarre vantaggio dal fatto che l'installazione di IBM WebSphere MQ propaga `Domain mqm` al gruppo `mqm` locale come in Figura 66 a pagina 378, poiché esistono due gruppi di utenti.

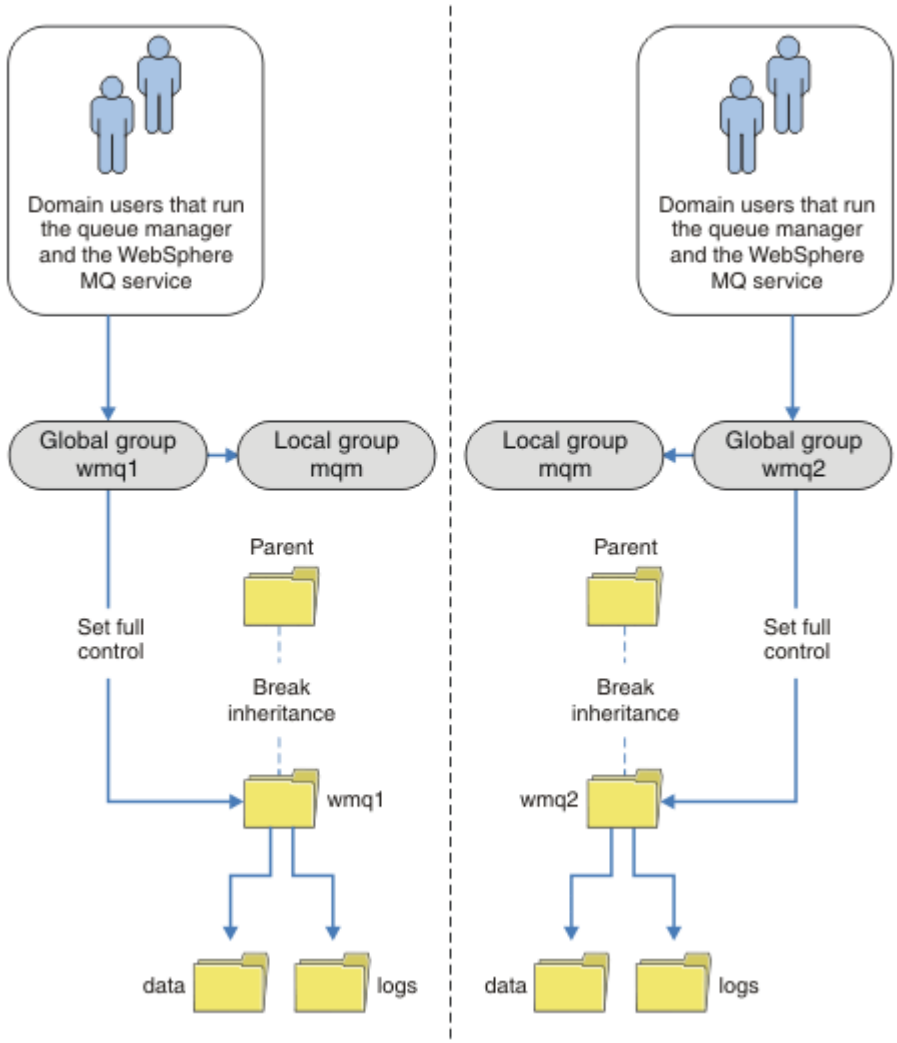


Figura 67. Protezione dei dati e dei log del gestore code utilizzando un principal di sicurezza globale alternativo (4)

Un modo alternativo per partizionare due dipartimenti sarebbe quello di posizionarli in due domini Windows. In tal caso, è possibile tornare a utilizzare il modello più semplice mostrato in Figura 66 a pagina 378.

Proteggere i file e le directory di log e i dati del gestore code non condivisi su Windows
Questo argomento descrive come proteggere un'ubicazione alternativa per i dati del gestore code e i file di log, sia utilizzando il gruppo `mqm` locale che un gruppo di protezione alternativo.

In genere non si imposta un'ubicazione alternativa per i dati del gestore code e i file di log. Quando si installa IBM WebSphere MQ for Windows, il programma di installazione crea una directory home a scelta per tutti i gestori code creati. Protegge le directory con il gruppo `mqm` locale e configura un ID utente per il servizio IBM IBM WebSphere MQ per accedere alle directory.

Due esempi dimostrano come configurare il controllo accessi per IBM WebSphere MQ. Gli esempi mostrano come creare un gestore code con i relativi dati e log nelle directory che non si trovano nei percorsi di dati e log creati dall'installazione. Nel primo esempio, “Lettura e scrittura di dati e file di log autorizzati dal gruppo mqm locale” a pagina 381, si consente l'accesso alle directory di coda e log autorizzando il gruppo `mqm` locale. Il secondo esempio, “Lettura e scrittura dei dati e dei file di log autorizzati da un gruppo di sicurezza locale alternativo” a pagina 384, differisce in quanto l'accesso alle indirizzari è autorizzato da un gruppo di protezione alternativo. Quando si accede alle directory da un gestore code in esecuzione su un solo server, la protezione dei dati e dei file di log con il gruppo di

sicurezza alternativo consente di proteggere diversi gestori code con diversi gruppi o principal locali. Quando si accede alle directory da un gestore code in esecuzione su server differenti, ad esempio con un gestore code a più istanze, la protezione dei file di dati e di log con il gruppo di protezione alternativo è l'unica scelta; consultare “Proteggere i dati del gestore code condiviso e le directory di log e i file su Windows” a pagina 376.

La configurazione delle permessi di sicurezza dei dati del gestore code e dei file di log non è un'attività comune su Windows. Quando si installa IBM WebSphere MQ for Windows, è possibile specificare le directory per i dati e i log del gestore code oppure accettare le directory predefinite. Il programma di installazione protegge automaticamente queste directory con il gruppo `mqm` locale, fornendo l'autorizzazione di controllo completo. Il processo di installazione verifica che l'ID utente che esegue i gestori code sia un membro del gruppo `mqm` locale. È possibile modificare le altre autorizzazioni di accesso sulle directory per soddisfare le proprie esigenze di accesso.

Se si sposta la directory dei file di dati e di log in nuove ubicazioni, è necessario configurare la sicurezza delle nuove ubicazioni. È possibile modificare l'ubicazione delle directory se si esegue il back up di un gestore code e lo si ripristina su un altro computer o se si modifica il gestore code in un gestore code a più istanze. È possibile scegliere tra due modi per proteggere i dati del gestore code e le directory di log nella nuova posizione. È possibile proteggere le directory limitando l'accesso al gruppo `mqm` locale oppure è possibile limitare l'accesso a qualsiasi gruppo di sicurezza di propria scelta.

È necessario il minor numero di passi per proteggere le directory utilizzando il gruppo `mqm` locale. Impostare le autorizzazioni sulle directory di dati e log per consentire il controllo completo del gruppo `mqm` locale. Un approccio tipico consiste nel copiare la serie di autorizzazioni esistenti, rimuovendo l'ereditarietà dal parent. È quindi possibile rimuovere o limitare le autorizzazioni di altri principal.

Se si esegue il gestore code con un ID utente diverso per il servizio impostato dalla procedura guidata Prepara IBM WebSphere MQ , tale ID utente deve essere membro del gruppo `mqm` locale. L'attività, “Lettura e scrittura di dati e file di log autorizzati dal gruppo mqm locale” a pagina 381, consente di eseguire le fasi.

È anche possibile proteggere i dati e i file di log del gestore code utilizzando un gruppo di protezione alternativo. Il processo di protezione dei dati del gestore code e dei file di log con il gruppo di sicurezza alternativo prevede una serie di fasi che fanno riferimento a Figura 68 a pagina 380. Il gruppo locale, `wmq`, è un esempio di un gruppo di protezione alternativo.

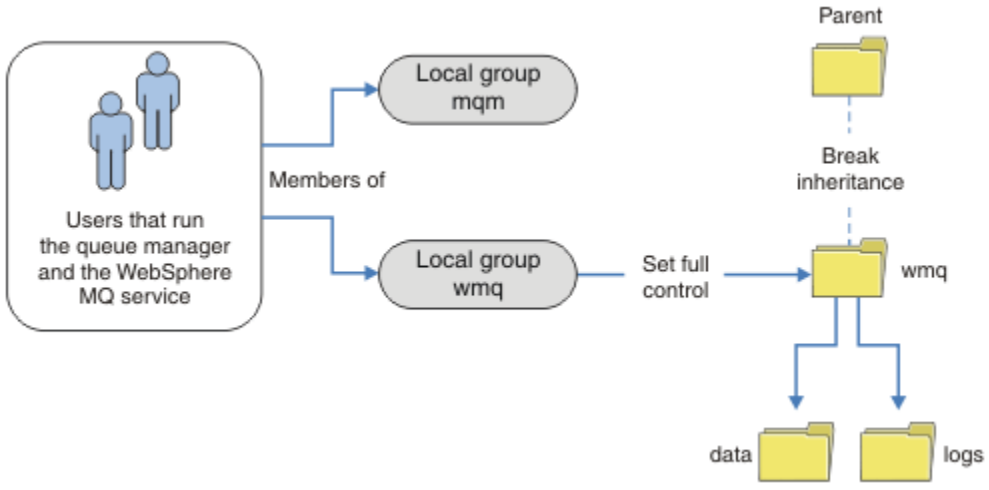


Figura 68. Protezione dei dati e dei log del gestore code utilizzando un gruppo di protezione locale alternativo, `wmq`

1. Creare directory separate per i dati e i log del gestore code, una directory comune o una directory principale comune.

2. Copiare la serie esistente di autorizzazioni ereditate per le directory o la directory principale e modificarle in base alle proprie esigenze.
3. Proteggere le directory che devono contenere il gestore code e i log fornendo al gruppo alternativo, `wmq`, l'autorizzazione di controllo completo per le directory.
4. Fornire a tutti gli ID utente che eseguono i processi del gestore code le credenziali del principal o del gruppo di sicurezza alternativo:
   a. Se si definisce un utente come principal di sicurezza alternativo, l'utente deve essere lo stesso utente con cui verrà eseguito il gestore code. L'utente deve essere un membro del gruppo `mqm` locale.
   b. Se si definisce un gruppo locale come gruppo di sicurezza alternativo, aggiungere l'utente sotto il quale verrà eseguito il gestore code al gruppo alternativo. L'utente deve anche essere membro del gruppo `mqm` locale.
   c. Se si definisce un gruppo globale come gruppo di sicurezza alternativo, consultare "Proteggere i dati del gestore code condiviso e le directory di log e i file su Windows" a pagina 376.
5. Creare il gestore code specificando il gruppo di sicurezza alternativo o il principal nel comando **`crtmqm`** , con il parametro `-a` .

Lettura e scrittura di dati e file di log autorizzati dal gruppo mqm locale
L'attività illustra come creare un gestore code con i relativi dati e file di log memorizzati in qualsiasi directory di propria scelta. L'accesso ai file è protetto dal gruppo `mqm` locale. La directory non è condivisa.

Prima di iniziare

1. Installare IBM WebSphere MQ for Windows come installazione primaria.
2. Eseguire la procedura guidata "Prepara IBM WebSphere MQ" . Per questa attività, configurare l'installazione in modo che venga eseguita con un ID utente locale o con un ID utente di dominio. Alla fine, per completare tutte le attività in "Domini Windows e gestori code a più istanze" a pagina 351, l'installazione deve essere configurata per un dominio.
3. Accedere con autorità di amministratore per eseguire la prima parte dell'attività.

Informazioni su questa attività

Questa attività è una delle attività correlate che illustrano l'accesso ai dati del gestore code e ai file di log. Le attività mostrano come creare un gestore code autorizzato a leggere e scrivere dati e file di log memorizzati in una directory di propria scelta. Accompagnano l'attività, "Domini Windows e gestori code a più istanze" a pagina 351.

In Windows, è possibile creare i percorsi di dati e log predefiniti per un IBM WebSphere MQ for Windows in qualsiasi directory di propria scelta. La procedura guidata di installazione e configurazione fornisce automaticamente al gruppo `mqm` locale, e all'ID utente che sta eseguendo i processi del gestore code, l'accesso alle directory. Se si crea un gestore code specificando directory differenti per i dati del gestore code e i file di log, è necessario configurare l'autorizzazione di controllo completo per le directory.

In questo esempio, si fornisce al gestore code il controllo completo sui relativi file di dati e di log fornendo al gruppo `mqm` locale l'autorizzazione alla directory *`c:\wmq`*.

Il comando **`crtmqm`** crea un gestore code che viene avviato automaticamente quando la workstation viene avviata utilizzando il servizio IBM IBM WebSphere MQ .

L'attività è illustrativa; utilizza valori specifici che è possibile modificare. I valori che è possibile modificare sono in corsivo. Alla fine dell'attivit ..., seguire le istruzioni per rimuovere tutte le modifiche apportate.

Procedura

1. Aprire un prompt dei comandi.
2. Immettere il comando:

```
md c:\wmq\data , c:\wmq\logs
```

3. Impostare le autorizzazioni sulle directory per consentire l'accesso in lettura e scrittura del gruppo mqm locale.

   ```
   cacls c:\wmq /T /E /G mqm:F
   ```

   La risposta del sistema:

   ```
   processed dir: c:\wmq
   processed dir: c:\wmq\data
   processed dir: c:\wmq\logs
   ```

4. Opzionale: Passare a un ID utente che è un membro del gruppo mqm locale.

   È possibile continuare come amministratore, ma per una configurazione di produzione realistica, continuare con un ID utente con diritti più limitati. L'ID utente deve essere almeno un membro del gruppo mqm locale.
   Se l'installazione di IBM WebSphere MQ è configurata come parte di un dominio, rendere l'ID utente un membro del gruppo Domain mqm . La procedura guidata "Prepara IBM WebSphere MQ" rende il gruppo globale Domain mqm un membro del gruppo mqm locale, quindi non è necessario rendere l'ID utente direttamente un membro del gruppo mqm locale.

5. Creare il gestore code.

   ```
   crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE -md c:\wmq\data -ld c:\wmq\logs  QMGR
   ```

   La risposta del sistema:

   ```
   WebSphere MQ queue manager created.
   Directory 'c:\wmq\data\QMGR' created.
   The queue manager is associated with installation '1'
   Creating or replacing default objects for queue manager 'QMGR'
   Default objects statistics : 74 created. 0 replaced.
   Completing setup.
   Setup completed.
   ```

6. Verificare che le directory create dal gestore code si trovino nella directory *c:\wmq* .

   ```
   dir c:\wmq /D /B /S
   ```

7. Verificare che i file dispongano dell'autorizzazione di lettura e scrittura o di controllo completo per il gruppo mqm locale.

   ```
   cacls c:\wmq\*.*
   ```

Operazioni successive

Verificare il gestore code inserendo e ricevendo un messaggio in una coda.

1. Avviare il gestore code.

   ```
   strmqm QMGR
   ```

   La risposta del sistema:

   ```
   WebSphere MQ queue manager 'QMGR' starting.
   The queue manager is associated with installation '1'.
   5 log records accessed on queue manager 'QMGR' during the log
   replay phase.
   Log replay for queue manager 'QMGR' complete.
   Transaction manager state recovered for queue manager 'QMGR'.
   WebSphere MQ queue manager 'QMGR' started using V7.1.0.0.
   ```

2. Creare una coda di test.

```
echo define qlocal(QTEST) | runmqsc QMGR
```

   La risposta del sistema:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QMGR.


     1 : define qlocal(QTEST)
AMQ8006: WebSphere MQ queue created.
One MQSC command read.
No commands have a syntax error.
All valid MQSC commands were processed.
```

3. Inserire un messaggio di verifica utilizzando il programma di esempio **amqsput**.

```
echo 'A test message' | amqsput QTEST QMGR
```

   La risposta del sistema:

```
Sample AMQSPUT0 start
target queue is QTEST
Sample AMQSPUT0 end
```

4. Richiamare il messaggio di test utilizzando il programma di esempio **amqsget**.

```
amqsget QTEST QMGR
```

   La risposta del sistema:

```
Sample AMQSGET0 start
message <A test message>
Wait 15 seconds ...
no more messages
Sample AMQSGET0 end
```

5. Chiudere il gestore code.

```
endmqm -i QMGR
```

   La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ended.
```

6. Eliminare il gestore code.

```
dltmqm QMGR
```

   La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' deleted.
```

7. Eliminare le directory create.

   Suggerimento: Aggiungere l'opzione /Q ai comandi per evitare che il comando richieda di eliminare ogni file o directory.

```
del /F /S C:\wmq\*.*
rmdir /S C:\wmq
```

Concetti correlati

“Domini Windows e gestori code a più istanze” a pagina 351

Un gestore code a più istanze su Windows richiede la condivisione dei dati e dei log. La condivisione deve essere accessibile a tutte le istanze del gestore code in esecuzione su server o workstation differenti. Configurare i gestori code e condividere come parte di un dominio Windows . Il gestore code può essere eseguito su una stazione di lavoro o su un server di dominio o sul controller di dominio.

Attività correlate

“Lettura e scrittura dei dati e dei file di log autorizzati da un gruppo di sicurezza locale alternativo” a pagina 384
In questa sezione viene illustrato come utilizzare l'indicatore -a nel comando **crtmqm** . L'indicatore fornisce al gestore code un gruppo di protezione locale alternativo per fornire l'accesso ai file di log e di dati.

“Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo” a pagina 363

“Crea un gestore code a più istanze su server o workstation di dominio” a pagina 352

Lettura e scrittura dei dati e dei file di log autorizzati da un gruppo di sicurezza locale alternativo
In questa sezione viene illustrato come utilizzare l'indicatore -a nel comando **crtmqm** . L'indicatore fornisce al gestore code un gruppo di protezione locale alternativo per fornire l'accesso ai file di log e di dati.

Prima di iniziare

1. Installare IBM WebSphere MQ for Windows come installazione primaria.
2. Eseguire la procedura guidata "Prepara IBM WebSphere MQ" . Per questa attività, configurare l'installazione in modo che venga eseguita con un ID utente locale o con un ID utente di dominio. Alla fine, per completare tutte le attività in “Domini Windows e gestori code a più istanze” a pagina 351, l'installazione deve essere configurata per un dominio.
3. Accedere con autorità di amministratore per eseguire la prima parte dell'attività.

Informazioni su questa attività

Questa attività è una delle attività correlate che illustrano l'accesso ai dati del gestore code e ai file di log. Le attività mostrano come creare un gestore code autorizzato a leggere e scrivere dati e file di log memorizzati in una directory di propria scelta. Accompagnano l'attività, “Domini Windows e gestori code a più istanze” a pagina 351.

In Windows, è possibile creare i percorsi di dati e log predefiniti per un IBM WebSphere MQ for Windows in qualsiasi directory di propria scelta. La procedura guidata di installazione e configurazione fornisce automaticamente al gruppo `mqm` locale, e all'ID utente che sta eseguendo i processi del gestore code, l'accesso alle directory. Se si crea un gestore code specificando directory differenti per i dati del gestore code e i file di log, è necessario configurare l'autorizzazione di controllo completo per le directory.

In questo esempio, si fornisce al gestore code un gruppo locale di protezione alternativo che dispone dell'autorizzazione di controllo completo per le directory. Il gruppo di sicurezza alternativo fornisce al gestore code l'autorizzazione a gestire i file nella directory. Lo scopo principale del gruppo di sicurezza alternativo è di autorizzare un gruppo globale di sicurezza alternativo. Utilizzare un gruppo globale di sicurezza alternativo per configurare un gestore code a più istanze. In questo esempio, configurare un gruppo locale per familiarizzare con l'utilizzo di un gruppo di protezione alternativo senza installare IBM WebSphere MQ in un dominio. È insolito configurare un gruppo locale come gruppo di sicurezza alternativo.

Il comando **crtmqm** crea un gestore code che viene avviato automaticamente quando la workstation viene avviata utilizzando il servizio IBM IBM WebSphere MQ .

L'attività è illustrativa; utilizza valori specifici che è possibile modificare. I valori che è possibile modificare sono in corsivo. Alla fine dell'attivit ..., seguire le istruzioni per rimuovere tutte le modifiche apportate.

Procedura

1. Configurare un gruppo di sicurezza alternativo.

   Il gruppo di sicurezza alternativo è generalmente un gruppo di domini. Nell'esempio, si crea un gestore code che utilizza un gruppo di sicurezza alternativo locale. Con un gruppo di sicurezza alternativo locale, è possibile eseguire l'attivit ... con un'installazione di IBM WebSphere MQ che non fa parte di un dominio.

   a) Eseguire il comando **lusrmgr.msc** per aprire la finestra Utenti e gruppi locali.

   b) Fare clic con il tasto destro del mouse su **Gruppi** > **Nuovo gruppo ...**

   c) Nel campo **Nome gruppo** , immettere *altmqm* e fare clic su **Crea** > **Chiudi**.

   d) Identificare l'ID utente che esegue il servizio IBM IBM WebSphere MQ .

      i) Fare clic su **Avvia** > **Esegui ...**, immettere `services.msc` e fare clic su **OK**.

      ii) Fare clic sul servizio IBM IBM WebSphere MQ nell'elenco di servizi e fare clic sulla scheda Accesso.

      iii) Ricordare l'ID utente e chiudere Esplora servizi.

   e) Aggiungere l'ID utente che esegue il servizio IBM IBM WebSphere MQ al gruppo *altmqm* . Aggiungere inoltre l'ID utente con cui si accede per creare un gestore code ed eseguirlo in modo interattivo.

      Windows controlla l'autorizzazione del gestore code per accedere alle directory di dati e log controllando l'autorizzazione dell'ID utente che sta eseguendo i processi del gestore code. L'ID utente deve essere un membro, direttamente o indirettamente tramite un gruppo globale, del gruppo *altmqm* che ha autorizzato le directory.
      Se IBM WebSphere MQ è stato installato come parte di un dominio e verranno eseguite le attività in “Crea un gestore code a più istanze su server o workstation di dominio” a pagina 352, gli ID utente del dominio creati in “Creazione di un dominio Active Directory e DNS per IBM WebSphere MQ” a pagina 355 sono *wmquser1* e *wmquser2*.
      Se il gestore code non è stato installato come parte di un dominio, l'ID utente locale predefinito che esegue il servizio IBM IBM WebSphere MQ è `MUSR_MQADMIN`. Se si intende eseguire le attività senza l'autorizzazione di amministratore, creare un utente che sia un membro del gruppo `mqm` locale.
      Seguire questi passi per aggiungere *wmquser1* e *wmquser2* a *altmqm*. Se la configurazione è diversa, sostituire i nomi per gli ID utente e il gruppo.

      i) Nell'elenco dei gruppi, fare clic con il tasto destro del mouse su **altmqm** > **Proprietà** > **Aggiungi ...**.

      ii) Nella finestra Seleziona utenti, computer o gruppi, immettere *wmquser1; wmquser2* e fare clic su **Controlla nomi**.

      iii) Immettere il nome e la parola d'ordine di un amministratore di dominio nella finestra Sicurezza di Windows, quindi fare clic su **OK** > **OK** > **Applica** > **OK**.

2. Aprire un prompt dei comandi.

3. Riavviare il servizio IBM IBM WebSphere MQ .

   È necessario riavviare il servizio in modo che l'ID utente con cui viene eseguito acquisisca le ulteriori credenziali di sicurezza configurate per esso.

   Immettere i comandi:

   ```
   endmqsvc
   strmqsvc
   ```

   Le risposte del sistema:

   ```
   5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
   The MQ service for installation 'Installation1' ended successfully.
   E:
   ```

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
The MQ service for installation 'Installation1' started successfully.
```

4. Immettere il comando:

```
md c:\wmq\data , c:\wmq\logs
```

5. Impostare le autorizzazioni sulle directory per consentire all'utente locale *user* l'accesso in lettura e scrittura.

```
cacls c:\wmq /T /E /G altmqm:F
```

La risposta del sistema:

```
processed dir: c:\wmq
processed dir: c:\wmq\data
processed dir: c:\wmq\logs
```

6. Opzionale: Passare a un ID utente che è un membro del gruppo mqm locale.

È possibile continuare come amministratore, ma per una configurazione di produzione realistica, continuare con un ID utente con diritti più limitati. L'ID utente deve essere almeno un membro del gruppo mqm locale.
Se l'installazione di IBM WebSphere MQ è configurata come parte di un dominio, rendere l'ID utente un membro del gruppo Domain mqm . La procedura guidata "Prepara IBM WebSphere MQ" rende il gruppo globale Domain mqm un membro del gruppo mqm locale, quindi non è necessario rendere l'ID utente direttamente un membro del gruppo mqm locale.

7. Creare il gestore code.

```
crtmqm -a altmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE -md c:\wmq\data -ld c:\wmq\logs  QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager created.
Directory 'c:\wmq1\data\QMGR' created.
The queue manager is associated with installation '1'
Creating or replacing default objects for queue manager 'QMGR'
Default objects statistics : 74 created. 0 replaced.
Completing setup.
Setup completed.
```

8. Verificare che le directory create dal gestore code si trovino nella directory *c:\wmq* .

```
dir c:\wmq /D /B /S
```

9. Verificare che i file dispongano dell'autorizzazione di lettura e scrittura o di controllo completo per il gruppo mqm locale.

```
cacls c:\wmq\*.*
```

Operazioni successive

Verificare il gestore code inserendo e ricevendo un messaggio in una coda.

1. Avviare il gestore code.

```
strmqm QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' starting.
The queue manager is associated with installation '1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
```

```
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
WebSphere MQ queue manager 'QMGR' started using V7.1.0.0.
```

2. Creare una coda di test.

```
echo define qlocal(QTEST) | runmqsc QMGR
```

La risposta del sistema:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024. ALL RIGHTS RESERVED.
Starting MQSC for queue manager QMGR.


     1 : define qlocal(QTEST)
AMQ8006: WebSphere MQ queue created.
One MQSC command read.
No commands have a syntax error.
All valid MQSC commands were processed.
```

3. Inserire un messaggio di verifica utilizzando il programma di esempio **amqsput**.

```
echo 'A test message' | amqsput QTEST QMGR
```

La risposta del sistema:

```
Sample AMQSPUT0 start
target queue is QTEST
Sample AMQSPUT0 end
```

4. Richiamare il messaggio di test utilizzando il programma di esempio **amqsget**.

```
amqsget QTEST QMGR
```

La risposta del sistema:

```
Sample AMQSGET0 start
message <A test message>
Wait 15 seconds ...
no more messages
Sample AMQSGET0 end
```

5. Chiudere il gestore code.

```
endmqm -i QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' ending.
WebSphere MQ queue manager 'QMGR' ended.
```

6. Eliminare il gestore code.

```
dltmqm QMGR
```

La risposta del sistema:

```
WebSphere MQ queue manager 'QMGR' deleted.
```

7. Eliminare le directory create.

Suggerimento: Aggiungere l'opzione /Q ai comandi per evitare che il comando richieda di eliminare ogni file o directory.

```
del /F /S C:\wmq\*.*
rmdir /S C:\wmq
```

Crea un gestore code a più istanze su Linux
Un esempio mostra come configurare un gestore code a più istanze su Linux. L'impostazione è piccola per illustrare i concetti coinvolti. L'esempio si basa su Linux Red Hat Enterprise 5. I passi differiscono su altre piattaforme UNIX .

L'esempio è impostato su un computer notebook a 2 GHz con 3 GB di RAM su cui è in esecuzione Windows XP Service Pack 2. Due macchine virtuali VMware , Server1 e Server2, eseguono Linux Red Hat Enterprise 5 in immagini da 640 MB. Server1 ospita il file system di rete (NFS), i log del gestore code e un'istanza HA. Non è consuetudine per il server NFS ospitare anche una delle istanze del gestore code; questo per semplificare l'esempio. Server2 monta i log del gestore code del Server1con un'istanza in standby. Un client WebSphere MQ MQI viene installato su un'immagine VMware aggiuntiva di 400 MB che esegue Windows XP Service Pack 2 ed esegue le applicazioni di esempio ad alta disponibilità. Tutte le macchine virtuali sono configurate come parte di una rete solo host VMware per ragioni di sicurezza.

Nota: È necessario inserire solo i dati del gestore code su un server NFS . Su NFS, utilizzare le seguenti tre opzioni con il comando mount per rendere il sistema sicuro:

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.

Esempio

Tabella 30. Configurazione illustrativa del gestore code a più istanze su Linux

Server1	**Server2**
Accedere come *root*	
Seguire le istruzioni riportate in Installazione di IBM WebSphere MQ per installare WebSphere MQ, creare l'utente e il gruppo mqm, se non esistono, e definire `/var/mqm`. Controllare cosa vengono visualizzati `uid` e `gid` in `/etc/passwd` sulla prima macchina per mqm; ad esempio, `mqm:x:501:100:MQ User:/var/mqm:/bin/bash` Associare `uid` e `gid` per mqm in `/etc/passwd` sulla seconda macchina per assicurarsi che questi valori siano identici. Riavviare questa macchina se è necessario modificare i valori.	
Completare l'attività Verifica del funzionamento del file system condiviso per verificare che il file system supporti gestori code a più istanze.	
Creare le directory di log e di dati in una cartella comune, `/MQHA`, da condividere. Ad esempio: 1. **mkdir** */MQHA* 2. **mkdir** */MQHA/logs* 3. **mkdir** */MQHA/qmgrs*	Creare la cartella, `/MQHA`, per montare il file system condiviso. Mantenere lo stesso percorso di Server1; ad esempio: 1. **mkdir** */MQHA*

Tabella 30. Configurazione illustrativa del gestore code a più istanze su Linux (Continua)

Server1	Server2
Assicurarsi che le directory MQHA siano di proprietà dell'utente e del gruppo mqm e che le autorizzazioni di accesso siano impostate su rwx per utente e gruppo; ad esempio, **ls -al** visualizza, drwxrwxr-x mqm mqm 4096 Nov 27 14:38 MQDATA 1. **chown -R** mqm:mqm */MQHA* 2. **chmod -R** ug+rwx */MQHA*	
Creare il gestore code: **crtmqm -ld** */MQHA/logs* **-md** */MQHA/qmgrs* *QM1*	
Aggiungi[2]Da /MQHA *(rw,sync,no_wdelay,fsid=0) a /etc/exports	
Avviare il daemon NFS : */etc/init.d/***nfs** start	Montare il file system esportato /MQHA: **mount -t** nfs4 **-o** hard,intr *Server1:/ /MQHA*
Copiare i dettagli di configurazione del gestore code da Server1: : **dspmqinf -o** command QM1 e copiare il risultato negli appunti: addmqinf -s QueueManager -v Name=QM1 -v Directory=QM1 -v Prefix=/var/mqm -v DataPath=/MQHA/qmgrs/QM1	Incollare il comando di configurazione del gestore code in Server2: **addmqinf -s** QueueManager **-v** Name=QM1 **-v** Directory=QM1 **-v** Prefix=/var/mqm **-v** DataPath=/MQHA/qmgrs/QM1
Avviare le istanze del gestore code, in entrambi gli ordini, con il parametro **x** : **strmqm -x** QM1 Il comando utilizzato per avviare le istanze del gestore code deve essere immesso dalla stessa installazione IBM WebSphere MQ del comando **addmqinf** . Per avviare e arrestare il gestore code da una installazione diversa, è necessario prima impostare l'installazione associata al gestore code utilizzando il comando **setmqm** . Per ulteriori informazioni, vedere setmqm.	

Verifica del gestore code a più istanze su Linux

Utilizzare i programmi di esempio **amqsghac**, **amqsphac** e **amqsmhac** per verificare la configurazione di un gestore code a più istanze. Questo argomento fornisce una configurazione di esempio per verificare una configurazione del gestore code a più istanze su Linux Red Hat Enterprise 5.

I programmi di esempio ad alta disponibilità utilizzano la riconnessione client automatica. Quando il gestore code connesso ha esito negativo, il client tenta di riconnettersi a un gestore code nello stesso gruppo di gestori code. La descrizione degli esempi, Programmi di esempio ad alta disponibilità, illustra la riconnessione del client utilizzando un gestore code a istanza singola per semplicità. È possibile utilizzare gli stessi esempi con i gestori code a più istanze per verificare una configurazione del gestore code a più istanze.

L'esempio utilizza la configurazione a più istanze descritta in “Crea un gestore code a più istanze su Linux” a pagina 388. Utilizzare la configurazione per verificare che il gestore code a più istanze passi all'istanza

[2] '*' consente a tutte le macchine che possono raggiungere questo montaggio /MQHA per la lettura/scrittura. Limitare l'accesso su una macchina di produzione.

in standby. Arrestare il gestore code con il comando **endmqm** e utilizzare l'opzione -s, switchover,. I programmi client si riconnettono alla nuova istanza del gestore code e continuano a lavorare con la nuova istanza dopo un leggero ritardo.

Nell'esempio, il client è in esecuzione su un sistema Windows XP Service Pack 2. Il sistema ospita due server VMware Linux che eseguono il gestore code a più istanze.

Verifica del failover mediante WebSphere MQ Explorer

Prima di utilizzare le applicazioni di esempio per verificare il failover, eseguire WebSphere MQ Explorer su ciascun server. Aggiungere entrambe le istanze del gestore code a ciascun explorer utilizzando la procedura guidata **Aggiungi gestore code remoto> Connetti direttamente a gestore code a più istanze** . Verificare che entrambe le istanze siano in esecuzione, consentendo lo standby. Chiudere la finestra che esegue l'immagine VMware con l'istanza attiva, spegnendo virtualmente il server o arrestando l'istanza attiva, consentendo il passaggio all'istanza standby.

Nota: Se si spegne il server, assicurarsi che non sia quello che ospita /MQHA!

Nota: L'opzione **Consenti commutazione a un'istanza in standby** potrebbe non essere disponibile nella finestra di dialogo **Arresta gestore code** . L'opzione è mancante perché il gestore code è in esecuzione come gestore code a istanza singola. È necessario che sia stato avviato senza l'opzione **Consenti un'istanza standby** . Se la richiesta di arresto del gestore code viene rifiutata, consultare la finestra **Dettagli** , probabilmente perché non è in esecuzione alcuna istanza in standby.

Verifica del failover utilizzando i programmi di esempio

Scegliere un server da utilizzare per eseguire l'istanza attiva

È possibile che sia stato scelto uno dei server per ospitare la directory o il file system MQHA . Se si prevede di verificare il failover chiudendo la finestra VMware che esegue il server attivo, assicurarsi che non sia quello che ospita MQHA!

Sul server che esegue l'istanza del gestore code attivo

Nota: L'esecuzione del canale SVRCONN con MCAUSER impostato su mqm, è una comodità per ridurre il numero di fasi di configurazione nell'esempio. Se viene scelto un altro ID utente e il proprio sistema è impostato in modo diverso da quello utilizzato nell'esempio, è possibile che si verifichino problemi di autorizzazione di accesso. Non utilizzare mqm come MCAUSER su un sistema esposto; è probabile che comprometta notevolmente la sicurezza.

1. Modificare *ipaddr1* e *ipaddr2* e salvare i seguenti comandi in /MQHA/hasamples.tst.

```
DEFINE  QLOCAL(SOURCE) REPLACE
DEFINE  QLOCAL(TARGET) REPLACE
DEFINE  CHANNEL(CHANNEL1) CHLTYPE(SVRCONN)   TRPTYPE(TCP) +
        MCAUSER('mqm') REPLACE
DEFINE  CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN)  TRPTYPE(TCP) +
        CONNAME('ipaddr1(1414),ipaddr2
(1414)') QMNAME(QM1) REPLACE
START   CHANNEL(CHANNEL1)
DEFINE  LISTENER(LISTENER.TCP) TRPTYPE(TCP) CONTROL(QMGR)
DISPLAY LISTENER(LISTENER.TCP) CONTROL
START   LISTENER(LISTENER.TCP)
DISPLAY LSSTATUS(LISTENER.TCP) STATUS
```

2. Aprire una finestra di terminale con il percorso /MQHA ed eseguire il comando:

```
runmqsc -m QM1 < hasamples.tst
```

3. Verificare che il listener sia in esecuzione e che disponga del controllo del gestore code, ispezionando l'output del comando **runmqsc** .

```
 LISTENER(LISTENER.TCP)CONTROL(QMGR)
 LISTENER(LISTENER.TCP)STATUS(RUNNING)
```

   Oppure, utilizzando WebSphere MQ Explorer che il listener TCPIP è in esecuzione e dispone di Control = Queue Manager.

Sul client

1. Copiare la tabella di connessione client AMQCLCHL.TAB da `/MQHA/qmgrs/QM1.000/@ipcc` sul server a `C:\` sul client.
2. Aprire un prompt dei comandi con il percorso `C:\` e impostare la variabile di ambiente `MQCHLLIB` in modo che punti alla tabella di definizione del canale client (CCDT)

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

3. Al prompt dei comandi immettere i seguenti comandi:

```
start amqsghac TARGET QM1
start amqsmhac -s SOURCE -t TARGET -m QM1
start amqsphac SOURCE QM1
```

Sul server che esegue l'istanza del gestore code attivo

1. Le alternative sono:
   - Chiudere la finestra che esegue l'immagine VMware con l'istanza del server attiva.
   - Utilizzando Esplora risorse di WebSphere MQ , arrestare l'istanza del gestore code attivo, consentendo il passaggio all'istanza in standby e istruendo i client ricollegabili a riconnettersi.
2. I tre client alla fine rilevano che la connessione è interrotta e quindi si ricollegano. In questa configurazione, se si chiude la finestra del server, sono necessari circa sette minuti perché tutte e tre le connessioni vengano ristabilite. Alcune connessioni vengono ristabilite ben prima di altre.

Risultati

```
N:\>amqsphac SOURCE QM1
Sample AMQSPHAC start
target queue is SOURCE
message <Message 1>
message <Message 2>
message <Message 3>
message <Message 4>
message <Message 5>
17:05:25 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:52 : EVENT : Connection Reconnected
message <Message 6>
message <Message 7>
message <Message 8>
message <Message 9>
```

```
N:\>amqsmhac -s SOURCE -t TARGET -m QM1
Sample AMQSMHA0 start

17:05:25 : EVENT : Connection Reconnecting (Delay: 97ms)
17:05:48 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:53 : EVENT : Connection Reconnected
```

```
N:\>amqsghac TARGET QM1
Sample AMQSGHAC start
message <Message 1>
message <Message 2>
message <Message 3>
message <Message 4>
message <Message 5>
17:05:25 : EVENT : Connection Reconnecting (Delay: 156ms)
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:52 : EVENT : Connection Reconnected
message <Message 6>
message <Message 7>
message <Message 8>
message <Message 9>
```

Eliminazione di un gestore code a più istanze

Per eliminare completamente un gestore code a più istanze, è necessario utilizzare il comando **dltmqm** per eliminare il gestore code e quindi rimuovere le istanze da altri server utilizzando i comandi **rmvmqinf** o **dltmqm** .

Eseguire il comando **dltmqm** per eliminare un gestore code con istanze definite su altri server, su qualsiasi server in cui è definito tale gestore code. Non è necessario eseguire il comando **dltmqm** sullo stesso server su cui è stato creato. Quindi, eseguire il comando **rmvmqinf** o **dltmqm** su tutti gli altri server che hanno una definizione del gestore code.

È possibile eliminare un gestore code solo quando è arrestato. Nel momento in cui si elimina, non ci sono istanze in esecuzione e il gestore code, in senso stretto, non è né un gestore code a istanza singola né un gestore code a più istanze; è semplicemente un gestore code che ha i dati del gestore code e i log su una condivisione remota. Quando si elimina un gestore code, i relativi log e dati del gestore code vengono eliminati e la stanza del gestore code viene rimossa dal file `mqs.ini` sul server su cui è stato immesso il comando **dltmqm** . È necessario disporre dell'accesso alla condivisione di rete contenente i dati e i log del gestore code quando si elimina il gestore code.

Su altri server in cui sono state precedentemente create istanze del gestore code, sono presenti anche voci nei file `mqs.ini` su tali server. È necessario visitare ciascun server e rimuovere la sezione del gestore code eseguendo il comando **rmvmqinf** *Nome stanza gestore code*.

Su sistemi UNIX and Linux , se è stato inserito un file `mqs.ini` comune nella memoria di rete e si fa riferimento ad esso da tutti i server impostando la variabile di ambiente `AMQ_MQS_INI_LOCATION` su ciascun server, è necessario eliminare il gestore code da uno solo dei relativi server poiché esiste un solo file `mqs.ini` da aggiornare.

Esempio

Primo server

```
dltmqm QM1
```

Altri server in cui sono definite le istanze

```
rmvmqinf QM1o
dltmqm QM1
```

Avvio e arresto di un gestore code a più istanze

Avvio e arresto di un gestore code configurato come una singola istanza o un gestore code a più istanze.

Una volta definito un gestore code a più istanze su una coppia di server, è possibile eseguire il gestore code su entrambi i server, come gestore code a istanza singola o come gestore code a più istanze.

Per eseguire un gestore code a più istanze, avviare il gestore code su uno dei server utilizzando il comando **strmqm** `-x` *QM1* ; l'opzione `-x` consente il failover dell'istanza. Diventa l'istanza *attiva* . Avviare l'istanza di standby sull'altro server utilizzando lo stesso comando **strmqm** `-x` *QM1* ; l'opzione `-x` consente l'avvio dell'istanza come standby.

Il gestore code è ora in esecuzione con un'istanza attiva che sta elaborando tutte le richieste e un'istanza in standby che è pronta a subentrare se l'istanza attiva ha esito negativo. All'istanza attiva viene concesso l'accesso esclusivo ai log e ai dati del gestore code. Lo standby attende che venga concesso l'accesso esclusivo ai log e ai dati del gestore code. Quando lo standby ha accesso esclusivo, diventa l'istanza attiva.

È anche possibile passare manualmente il controllo all'istanza standby immettendo il comando **endmqm** `-s` sull'istanza attiva. Il comando **endmqm** `-s` arresta l'istanza attiva senza arrestare lo standby. Il blocco di accesso esclusivo sui log e sui dati del gestore code viene rilasciato e lo standby assume il controllo.

È anche possibile avviare e arrestare un gestore code configurato con più istanze su server diversi come gestore code a istanza singola. Se si avvia il gestore code senza utilizzare l'opzione `-x` nel comando **strmqm** , alle istanze del gestore code configurato su altre macchine viene impedito l'avvio come istanze in standby. Se si tenta di avviare un'altra istanza, si riceve la risposta che l'istanza del gestore code non può essere eseguita come standby.

Se si arresta l'istanza attiva di un gestore code a più istanze utilizzando il comando **endmqm** senza l'opzione -s , le istanze attive e in standby si arrestano entrambe. Se si arresta l'istanza in standby utilizzando il comando **endmqm** con l'opzione -x , smette di essere in standby e l'istanza attiva continua l'esecuzione. Non è possibile emettere **endmqm** senza l'opzione -x sullo standby.

Solo due istanze del gestore code possono essere eseguite contemporaneamente; una è l'istanza attiva e l'altra è un'istanza in standby. Se si avviano due istanze contemporaneamente, WebSphere MQ non ha alcun controllo su quale istanza diventa l'istanza attiva; è determinata dal file system di rete. La prima istanza che acquisisce l'accesso esclusivo ai dati del gestore code diventa l'istanza attiva.

Nota: Prima di riavviare un gestore code non riuscito, è necessario disconnettere le applicazioni da tale istanza del gestore code. In caso contrario, il gestore code potrebbe non essere riavviato correttamente.

File system condiviso

Un gestore code a più istanze utilizza un file system di rete per gestire le istanze del gestore code.

Un gestore code a più istanze automatizza il failover utilizzando una combinazione di blocchi del filesystem e log e dati del gestore code condivisi. Solo una istanza di un gestore code può avere accesso esclusivo ai log e ai dati del gestore code condivisi. Quando ottiene l'accesso, diventa l'istanza attiva. L'altra istanza che non riesce a ottenere l'accesso esclusivo attende come istanza in standby fino a quando i dati e i log del gestore code diventano disponibili.

Il file system di rete è responsabile del rilascio dei blocchi che detiene per l'istanza del gestore code attiva. Se l'istanza attiva ha esito negativo in qualche modo, il file system di rete rilascia i blocchi che sta detenendo per l'istanza attiva. Non appena il blocco esclusivo viene rilasciato, un gestore code in attesa del blocco tenta di acquisirlo. Se ha esito positivo, diventa l'istanza attiva e ha accesso esclusivo ai dati del gestore code e ai log sul file system condiviso. Continua quindi ad iniziare.

L'argomento correlato, Supporto file system di pianificazione descrive come impostare e verificare che il proprio file system supporti i gestori code a più istanze.

Un gestore code a più istanze non protegge l'utente da un errore nel filesystem. Esistono diversi modi per proteggere i tuoi dati.

- Investi in storage affidabile, come RAID (redundant disk array), e includili in un file system di rete con resilienza di rete.
- Eseguire il backup dei log lineari WebSphere MQ su un supporto alternativo e, se il supporto di log principale ha esito negativo, eseguire il ripristino utilizzando i log sul supporto alternativo. È possibile utilizzare un gestore code di backup per gestire questo processo.

Più istanze del gestore code

Un gestore code a più istanze è resiliente perché utilizza un'istanza del gestore code in standby per ripristinare la disponibilità del gestore code dopo l'errore.

La replica delle istanze del gestore code è un modo molto efficiente per aumentare la disponibilità dei processi del gestore code. Utilizzando un modello di disponibilità semplice, puramente illustrativo: se l'affidabilità di un'istanza di un gestore code è del 99% (in un anno, il tempo di inattività cumulativo è di 3.65 giorni), l'aggiunta di un'altra istanza del gestore code aumenta la disponibilità a 99.99% (in un anno, il tempo di inattività cumulativo di circa un'ora).

Si tratta di un modello troppo semplice per fornire stime numeriche pratiche della disponibilità. Per modellare realisticamente la disponibilità, è necessario raccogliere statistiche per il tempo medio tra i guasti (MTBF) e il tempo medio di riparazione (MTTR), e la distribuzione di probabilità del tempo tra i guasti e i tempi di riparazione.

Il termine, gestore code a più istanze, fa riferimento alla combinazione di istanze attive e in standby del gestore code che condividono i dati e i log del gestore code. I gestori code a più istanze proteggono l'utente dall'errore dei processi del gestore code, in quanto un'istanza del gestore code è attiva su un server e un'altra istanza del gestore code è in standby su un altro server, pronta a subentrare automaticamente in caso di errore dell'istanza attiva.

Failover o commutazione

Un'istanza del gestore code in standby subentra all'istanza attiva su richiesta (commutazione) o quando l'istanza attiva ha esito negativo (failover).

- Lo *switchover* si verifica quando un'istanza in standby viene avviata in seguito al comando **endmqm** `-s` emesso per l'istanza del gestore code attivo. È possibile specificare i **endmqm** parametri `-c`, `-i` o `-p` per controllare l'arresto improvviso del gestore code.

  Nota: La commutazione ha luogo solo se un'istanza del gestore code in standby è già stata avviata. Il comando **endmqm** `-s` rilascia il blocco del gestore code attivo e consente la commutazione: non avvia un'istanza del gestore code in standby.
- Il *failover* si verifica quando il blocco dei dati del gestore code trattenuti dall'istanza attiva viene rilasciato perché l'istanza sembrava arrestarsi in modo imprevisto (ovvero, senza l'emissione di un comando **endmqm**).

Quando l'istanza in standby assume il controllo come istanza attiva, scrive un messaggio nel log degli errori del gestore code.

I client ricollegabili vengono riconnessi automaticamente quando un gestore code ha esito negativo o si commuta. Non è necessario includere l'indicatore `-r` nel comando **endmqm** per richiedere la riconnessione client. La riconnessione automatica del client non è supportata dalle classi WebSphere MQ per Java.

Se si rileva che non è possibile riavviare un'istanza non riuscita, anche se si è verificato un failover e l'istanza in standby è diventata attiva, verificare che le applicazioni connesse localmente all'istanza non riuscita non si siano disconnesse dall'istanza non riuscita. Le applicazioni connesse localmente terminano o si disconnettono da un'istanza del gestore code non riuscita per garantire che l'istanza non riuscita possa essere riavviata. Tutte le applicazioni connesse localmente che utilizzano i bind condivisi (che è l'impostazione predefinita) che mantengono una connessione a un'istanza non riuscita agiscono per impedire il riavvio dell'istanza. Se non è possibile terminare le applicazioni connesse localmente o assicurarsi che si disconnettano quando l'istanza del gestore code locale ha esito negativo, considerare l'utilizzo di bind isolati. Le applicazioni connesse localmente che utilizzano collegamenti isolati non impediscono il riavvio dell'istanza del gestore code locale, anche se non si disconnettono.

Riconnessione canale e client

La riconnessione del canale e del client è una parte essenziale del ripristino dell'elaborazione dei messaggi dopo che un'istanza del gestore code in standby è diventata attiva.

Le istanze del gestore code a più istanze sono installate su server con indirizzi di rete diversi. È necessario configurare i canali e client IBM WebSphere MQ con le informazioni di connessione per tutte le istanze del gestore code. Quando subentra uno standby, i client e i canali vengono riconnessi automaticamente all'istanza del gestore code appena attiva al nuovo indirizzo di rete. La riconnessione automatica del client non è supportata dalle classi WebSphere MQ per Java.

Il design è diverso da come funzionano gli ambienti ad alta disponibilità come HA - CMP. HA - CMP fornisce un indirizzo IP virtuale per il cluster e trasferisce l'indirizzo al server attivo. WebSphere MQ la riconnessione non modifica o reindirizza gli indirizzi IP. Funziona riconnettendosi utilizzando gli indirizzi di rete definiti nelle definizioni di canale e nelle connessioni client. In qualità di amministratore, è necessario definire gli indirizzi di rete nelle definizioni di canale e nelle connessioni client a tutte le istanze di qualsiasi gestore code a più istanze. Il modo migliore per configurare gli indirizzi di rete per un gestore code a più istanze dipende dalla connessione:

Canali gestore code

L'attributo `CONNAME` dei canali è un elenco separato da virgole di nomi di connessione; ad esempio `CONNAME('127.0.0.1(1234), 192.0.2.0(4321)')`. Le connessioni vengono tentate nell'ordine specificato nell'elenco delle connessioni finché non viene stabilita una connessione con esito positivo. Se nessuna connessione ha esito positivo, il canale tenta di riconnettersi.

Canali cluster

Di norma, non è richiesta alcuna configurazione aggiuntiva per far funzionare i gestori code a più istanze in un cluster.

Se un gestore code si connette a un gestore code del repository, il repository rileva l'indirizzo di rete del gestore code. Fa riferimento al CONNAME del canale CLUSRCVR nel gestore code. Su TCPIP, il gestore code imposta automaticamente il CONNAME se lo si omette o lo si configura su spazi vuoti. Quando un'istanza in standby prende il controllo, il relativo indirizzo IP sostituisce l'indirizzo IP della precedente istanza attiva come CONNAME.

Se necessario, è possibile configurare manualmente CONNAME con l'elenco di indirizzi di rete delle istanze del gestore code.

Connessioni client
Le connessioni client possono utilizzare elenchi di connessioni o gruppi di gestori code per selezionare connessioni alternative. Per ulteriori informazioni sulla riconnessione del client a un gestore code a più istanze, consultare “Riconnessione automatica del client” a pagina 315. I client devono essere compilati per essere eseguiti con le librerie client WebSphere MQ Versione 7.0.1 o superiore. Devono essere connessi almeno a una versione 7.0.1 del gestore code.

Quando si verifica il failover, la riconnessione richiede del tempo. Il gestore code in standby deve completare l'avvio. I client connessi al gestore code non riuscito devono rilevare l'errore di connessione e avviare una nuova connessione client. Se una nuova connessione client seleziona il gestore code in standby che è diventato nuovamente attivo, il client viene riconnesso allo stesso gestore code.

Se il client è nel mezzo di una chiamata MQI durante la riconnessione, deve tollerare un'attesa estesa prima del completamento della chiamata.

Se l'errore si verifica durante un trasferimento batch su un canale di messaggi, il batch viene sottoposto a rollback e riavviato.

La commutazione è più veloce del failover e impiega solo il tempo necessario per arrestare un'istanza del gestore code e avviarne un'altra. Per un gestore code con solo pochi record di log da ripetere, la commutazione potrebbe richiedere l'ordine di pochi secondi. Per stimare il tempo impiegato dal failover, è necessario aggiungere il tempo impiegato per rilevare l'errore. Nel migliore dei casi, il rilevamento richiede l'ordine di 10 secondi e potrebbe richiedere diversi minuti, a seconda della rete e del sistema di file.

Ripristino applicazione
Il ripristino dell'applicazione è la continuazione automatizzata dell'elaborazione dell'applicazione dopo il failover. Il ripristino dell'applicazione dopo il failover richiede un'attenta progettazione. Alcune applicazioni devono essere a conoscenza del failover.

L'obiettivo del ripristino dell'applicazione è che l'applicazione continui l'elaborazione con un breve ritardo. Prima di continuare con la nuova elaborazione, l'applicazione deve eseguire il backout e inoltrare nuovamente l'unità di lavoro che stava elaborando durante l'errore.

Un problema per il ripristino dell'applicazione è la perdita del contesto condiviso tra il client MQI WebSphere MQ e il gestore code e memorizzato nel gestore code. Il client WebSphere MQ MQI ripristina la maggior parte del contesto, ma alcune parti del contesto non possono essere ripristinate in modo affidabile. Le seguenti sezioni descrivono alcune proprietà del recupero dell'applicazione e come influiscono sul recupero delle applicazioni connesse a un gestore code a più istanze.

Messaggistica transazionale

Dal punto di vista del recapito dei messaggi, il failover non modifica le proprietà persistenti della messaggistica WebSphere MQ . Se i messaggi sono persistenti e correttamente gestiti all'interno delle unità di lavoro, i messaggi non vengono persi durante un failover.

Dal punto di vista dell'elaborazione delle transazioni, le transazioni vengono sottoposte a backout o a commit dopo il failover.

Viene eseguito il rollback delle transazioni non sottoposte a commit. Dopo il failover, un'applicazione riconnettibile riceve un codice di errore MQRC_BACKED_OUT per indicare che la transazione ha avuto esito negativo e deve eseguire il rollback della transazione emettendo MQBACK. È quindi necessario riavviare nuovamente la transazione.

Le transazioni sottoposte a commit sono transazioni che hanno raggiunto la seconda fase di un commit a due fasi o transazioni a fase singola (solo messaggio) che hanno iniziato MQCMIT .

Se il gestore code è il coordinatore della transazione e MQCMIT ha iniziato la seconda fase del suo commit a due fasi prima dell'errore, la transazione viene completata correttamente. Il completamento è sotto controllo del gestore code e continua quando il gestore code è di nuovo in esecuzione. In un'applicazione ricollegabile, la chiamata MQCMIT viene completata normalmente.

In un commit a fase singola, che implica solo messaggi, una transazione che ha avviato l'elaborazione del commit viene completata normalmente sotto il controllo del gestore code una volta che è di nuovo in esecuzione. In un'applicazione ricollegabile, il MQCMIT viene completato normalmente.

I client ricollegabili possono utilizzare transazioni a fase singola sotto il controllo del gestore code come coordinatore delle transazioni. Il client transazionale esteso non supporta la riconnessione. Se la riconnessione viene richiesta quando il client transazionale si connette, la connessione ha esito positivo, ma senza la possibilità di riconnessione. La connessione si comporta come se non fosse ricollegabile.

Riavvio o ripresa dell'applicazione

Il failover interrompe un'applicazione. Dopo un errore, un'applicazione può essere riavviata dall'inizio oppure può riprendere l'elaborazione dopo l'interruzione. Quest' ultimo è chiamato *riconnessione client automatica*. La riconnessione automatica del client non è supportata dalle classi WebSphere MQ per Java.

Con un'applicazione client WebSphere MQ , è possibile impostare un'opzione di connessione per riconnettere automaticamente il client. Le opzioni sono MQCNO_RECONNECT o MQCNO_RECONNECT_Q_MGR . Se non è impostata alcuna opzione, il client non tenta di riconnettersi automaticamente e l'errore del gestore code restituisce MQRC_CONNECTION_BROKEN al client. È possibile progettare il client in modo che tenti di avviare una nuova connessione emettendo una nuova chiamata MQCONN o MQCONNX .

I programmi server devono essere riavviati; non possono essere riconnessi automaticamente dal gestore code nel momento in cui sono stati elaborati quando il gestore code o il server hanno avuto esito negativo. WebSphere I programmi server MQ non vengono generalmente riavviati sull'istanza del gestore code in standby quando si verifica un malfunzionamento di un'istanza del gestore code a più istanze.

È possibile automatizzare un programma server WebSphere MQ per riavviare il server standby in due modi:

1. Impacchettare l'applicazione server come servizio gestore code. Viene riavviato al riavvio del gestore code in standby.
2. Scrivere la propria logica di failover, attivata ad esempio dal messaggio di log di failover scritto da un'istanza del gestore code in standby quando viene avviata. L'istanza dell'applicazione deve quindi richiamare MQCONN o MQCONNX dopo l'avvio, per creare una connessione al gestore code.

Rilevamento del failover

Alcune applicazioni devono essere a conoscenza del failover, altre no. Si considerino questi due esempi.

1. Un'applicazione di messaggistica che riceve o riceve messaggi su un canale di messaggistica normalmente non richiede che il gestore code all'altra estremità del canale sia in esecuzione: è improbabile che ne venga influenzata se il gestore code all'altra estremità del canale viene riavviato su un'istanza in standby.
2. Un'applicazione client MQI WebSphere MQ elabora l'input di messaggi persistenti da una coda e inserisce le risposte di messaggi persistenti in un'altra coda come parte di una singola unità di lavoro: se gestisce un codice di errore MQRC_BACKED_OUT da MQPUT, MQGET o MQCMIT all'interno del punto di sincronizzazione emettendo MQBACK e riavviando l'unità di lavoro, non viene perso alcun messaggio. Inoltre, l'applicazione non deve eseguire alcuna elaborazione speciale per gestire un errore di connessione.

Si supponga, tuttavia, nel secondo esempio, che l'applicazione stia esplorando la coda per selezionare il messaggio da elaborare utilizzando l'opzione MQGET , MQGMO_MSG_UNDER_CURSOR. La riconnessione

reimposta il cursore di esplorazione e la chiamata MQGET non restituisce il messaggio corretto. In questo esempio, l'applicazione deve essere consapevole che si è verificato un failover. Inoltre, prima di emettere un altro MQGET per il messaggio sotto il cursore, l'applicazione deve ripristinare il cursore di ricerca.

La perdita del cursore di esplorazione è un esempio di come il contesto dell'applicazione cambia dopo la riconnessione. Altri casi sono documentati in "Ripristino di un client riconnesso automaticamente" a pagina 397.

Sono disponibili tre modelli di progettazione alternativi per le applicazioni client WebSphere MQ MQI in seguito al failover. Solo uno di essi non deve rilevare il failover.

Nessuna riconnessione

In questo modello, l'applicazione arresta tutta l'elaborazione sulla connessione corrente quando la connessione è interrotta. Per continuare l'elaborazione dell'applicazione, è necessario stabilire una nuova connessione con il gestore code. L'applicazione è interamente responsabile del trasferimento di tutte le informazioni di stato necessarie per continuare l'elaborazione sulla nuova connessione. Le applicazioni client esistenti che si riconnettono a un gestore code dopo aver perso la connessione vengono scritte in questo modo.

Il client riceve un codice motivo, ad esempio MQRC_CONNECTION_BROKEN o MQRC_Q_MGR_NOT_AVAILABLE dalla successiva chiamata MQI dopo la perdita della connessione. L'applicazione deve eliminare tutte le informazioni sullo stato di WebSphere MQ , come gli handle delle code, ed emettere una nuova chiamata MQCONN o MQCONNX per stabilire una nuova connessione, quindi riaprire gli oggetti WebSphere MQ che deve elaborare.

Il comportamento MQI predefinito prevede che l'handle di connessione del gestore code diventi inutilizzabile dopo la perdita di una connessione con il gestore code. Il valore predefinito è equivalente all'impostazione dell'opzione MQCNO_RECONNECT_DISABLED su MQCONNX per impedire la riconnessione dell'applicazione dopo il failover.

Tolleranza failover

Scrivere l'applicazione in modo che non sia influenzata dal failover. A volte un'attenta gestione degli errori è sufficiente per gestire il failover.

Riconnessione consapevole

Registrare un gestore eventi MQCBT_EVENT_HANDLER con il gestore code. Il gestore eventi viene inviato con MQRC_RECONNECTING quando il client inizia a tentare di riconnettersi con il server e MQRC_RECONNECTED dopo una riconnessione eseguita correttamente. È quindi possibile eseguire una routine per ristabilire uno stato prevedibile in modo che l'applicazione del client possa continuare l'elaborazione.

Ripristino di un client riconnesso automaticamente

Il failover è un evento imprevisto e perché un client riconnesso automaticamente funzioni come progettato, le conseguenze della riconnessione devono essere prevedibili.

Un elemento importante per trasformare un errore imprevisto in un ripristino prevedibile e affidabile è l'utilizzo delle transazioni.

Nella sezione precedente, un esempio, "2" a pagina 396, è stato fornito di un client MQI WebSphere MQ che utilizza una transazione locale per coordinare MQGET e MQPUT. Il client emette una chiamata MQCMIT o MQBACK in risposta a un errore MQRC_BACKED_OUT e quindi inoltra nuovamente la transazione di cui è stato eseguito il backout. L'errore del gestore code causa il backout della transazione e il comportamento dell'applicazione client garantisce che non vengano perse transazioni e messaggi.

Non tutto lo stato del programma viene gestito come parte di una transazione e quindi le conseguenze della riconnessione diventano più difficili da comprendere. È necessario sapere in che modo la riconnessione modifica lo stato di un WebSphere MQ client MQI per progettare l'applicazione client in modo da sopravvivere al failover del gestore code.

Potresti decidere di progettare la tua applicazione senza alcun codice di failover speciale, gestendo gli errori di riconnessione con la stessa logica degli altri errori. In alternativa, è possibile scegliere di riconoscere che la riconnessione richiede un'elaborazione di errori speciali e registrare un gestore

eventi con WebSphere MQ per eseguire una routine per gestire il failover. La routine potrebbe gestire l'elaborazione della riconnessione stessa oppure impostare un indicatore per indicare al thread del programma principale che quando riprende l'elaborazione è necessario eseguire l'elaborazione del recupero.

L'ambiente client WebSphere MQ MQI è consapevole del failover stesso e ripristina il maggior numero di contesti possibile, dopo la riconnessione, memorizzando alcune informazioni sullo stato nel client ed emettendo ulteriori chiamate MQI per conto dell'applicazione client per ripristinare lo stato WebSphere MQ . Ad esempio, gli handle per gli oggetti che erano aperti nel punto di errore vengono ripristinati e le code dinamiche temporanee vengono aperte con lo stesso nome. Ma ci sono cambiamenti che sono inevitabili e hai bisogno del tuo design per affrontare questi cambiamenti. Le modifiche possono essere suddivise in cinque tipi:

1. Gli errori nuovi o precedentemente non diagnosticati vengono restituiti dalle chiamate MQI fino a quando non viene ripristinato un nuovo stato di contesto coerente dal programma di applicazione.

   Un esempio di ricezione di un nuovo errore è il codice di ritorno MQRC_CONTEXT_NOT_AVAILABLE quando si tenta di passare il contesto dopo aver salvato il contesto prima della riconnessione. Il contesto non può essere ripristinato dopo la riconnessione perché il contesto di sicurezza non viene passato a un programma client non autorizzato. Per fare ciò, un programma di applicazione dannoso potrebbe ottenere il contesto di sicurezza.

   In genere, le applicazioni gestiscono gli errori comuni e prevedibili in modo accurato e relegano gli errori non comuni in un gestore di errori generico. Il gestore degli errori potrebbe disconnettersi da WebSphere MQ e riconnettersi di nuovo oppure arrestare del tutto il programma. Per migliorare la continuità potrebbe essere necessario affrontare alcuni errori in modo diverso.
2. I messaggi non persistenti potrebbero andare persi.
3. Viene eseguito il rollback delle transazioni.
4. Le chiamate MQGET o MQPUT utilizzate al di fuori di un punto di sincronizzazione potrebbero essere interrotte con la possibile perdita di un messaggio.
5. Errori di temporizzazione indotti, a causa di un'attesa prolungata in una chiamata MQI.

Alcuni dettagli sul contesto perso sono riportati nella seguente sezione.

- I messaggi non persistenti vengono eliminati, a meno che non vengano inseriti in una coda con l'opzione NPMCLASS (HIGH) e l'errore del gestore code non abbia interrotto l'opzione di memorizzazione dei messaggi non persistenti all'arresto.
- Una sottoscrizione non durevole viene persa quando una connessione viene interrotta. Alla riconnessione, viene ristabilito. Considerare l'utilizzo di una sottoscrizione durevole.
- L'intervallo get - wait viene ricalcolato; se il limite viene superato, restituisce MQRC_NO_MSG_AVAILABLE. Allo stesso modo, la scadenza della sottoscrizione viene ricalcolata per fornire la stessa scadenza globale.
- La posizione del cursore di ricerca in una coda viene persa; in genere viene ristabilita prima del primo messaggio.
  - MQGET chiamate che specificano MQGMO_BROWSE_MSG_UNDER_CURSOR o MQGMO_MSG_UNDER_CURSOR, non riuscite con codice motivo MQRC_NO_MSG_AVAILABLE.
  - I messaggi bloccati per la ricerca sono sbloccati.
  - I messaggi contrassegnati con l'ambito dell'handle non sono contrassegnati e possono essere ricercati di nuovo.
  - Nella maggior parte dei casi, i messaggi contrassegnati da ricerca cooperativa non vengono contrassegnati.
- Il contesto di sicurezza è andato perduto. I tentativi di utilizzare il contesto del messaggio salvato, come l'inserimento di un messaggio con MQPMO_PASS_ALL_CONTEXT , non riescono con MQRC_CONTEXT_NOT_AVAILABLE.
- I token del messaggio vengono persi. MQGET utilizzando un token del messaggio restituisce il codice motivo MQRC_NO_MSG_AVAILABLE .

Nota: *MsgId* e *CorrelId*, poiché fanno parte del messaggio, vengono conservati con il messaggio durante il failover e quindi MQGET utilizzando MsgId o CorrelId funzionano come previsto.

- I messaggi inseriti su una coda nel punto di sincronizzazione in una transazione non sottoposta a commit non sono più disponibili.
- L'elaborazione dei messaggi in un ordine logico o in un gruppo di messaggi, risulta in un codice di ritorno MQRC_RECONNECT_INCOMPATIBLE dopo la riconnessione.
- Una chiamata MQI potrebbe restituire MQRC_RECONNECT_FAILED piuttosto che il più generale MQRC_CONNECTION_BROKEN che i client generalmente ricevono oggi.
- La riconnessione durante una chiamata MQPUT all'esterno del punto di sincronizzazione restituisce MQRC_CALL_INTERRUPTED se il client MQI WebSphere MQ non sa se il messaggio è stato recapitato correttamente al gestore code. La riconnessione durante MQCMIT funziona in modo simile.
- MQRC_CALL_INTERRUPTED viene restituito - dopo una riconnessione eseguita correttamente - se il client WebSphere MQ MQI non ha ricevuto alcuna risposta dal gestore code per indicare l'esito positivo o negativo di
  - la consegna di un messaggio persistente utilizzando una chiamata MQPUT fuori dal punto di sincronizzazione.
  - la consegna di un messaggio persistente o di un messaggio con persistenza predefinita utilizzando una chiamata MQPUT1 fuori dal punto di sincronizzazione.
  - il commit di una transazione utilizzando una chiamata MQCMIT. La risposta viene restituita solo dopo una riconnessione riuscita.
- I canali vengono riavviati come nuove istanze (potrebbero anche essere canali differenti) e quindi non viene conservato alcuno stato di uscita del canale.
- Le code dinamiche temporanee vengono ripristinate come parte del processo di recupero dei client ricollegabili che avevano code dinamiche temporanee aperte. Non viene ripristinato alcun messaggio su una coda dinamica temporanea, ma le applicazioni che avevano la coda aperta o che avevano ricordato il nome della coda, sono in grado di continuare l'elaborazione.

  Esiste la possibilità che se la coda viene utilizzata da un'applicazione diversa da quella che l'ha creata, potrebbe non essere ripristinata abbastanza rapidamente da essere presente al successivo riferimento. Ad esempio, se un client crea una coda dinamica temporanea come coda di risposta e un messaggio di risposta deve essere inserito sulla coda da un canale, la coda potrebbe non essere recuperata in tempo. In questo caso, il canale generalmente posiziona il messaggio di risposta sulla coda di messaggi non recapitabili.

  Se un'applicazione client ricollegabile apre una coda dinamica temporanea per nome (perché un'altra applicazione l'ha già creata), quando si verifica la riconnessione, il client WebSphere MQ MQI non è in grado di ricreare la coda dinamica temporanea perché non dispone del modello da cui crearla. In MQI, solo un'applicazione può aprire la coda dinamica temporanea per modello. Altre applicazioni che desiderano utilizzare la coda dinamica temporanea devono utilizzare MQPUT1o i bind del server oppure essere in grado di provare nuovamente la riconnessione se non riesce.

  Solo i messaggi non persistenti possono essere inseriti in una coda dinamica temporanea e questi messaggi vengono persi durante il failover; questa perdita si verifica per i messaggi inseriti in una coda dinamica temporanea utilizzando MQPUT1 durante la riconnessione. Se il failover si verifica durante MQPUT1, il messaggio potrebbe non essere inserito, anche se MQPUT1 ha esito positivo. Una soluzione temporanea a questo problema consiste nell'utilizzare code dinamiche permanenti. Qualsiasi applicazione di bind del server può aprire la coda dinamica temporanea in base al nome perché non è ricollegabile.

Data recovery e alta disponibilità

Le soluzioni di alta disponibilità che utilizzano gestori code a più istanze devono includere un meccanismo per il ripristino dei dati dopo un errore di memoria.

Un gestore code a più istanze aumenta la disponibilità dei processi del gestore code, ma non la disponibilità di altri componenti, come ad esempio il file system, che il gestore code utilizza per memorizzare messaggi e altre informazioni.

Un modo per rendere i dati altamente disponibili è quello di utilizzare l'archiviazione dati resiliente in rete. È possibile creare una propria soluzione utilizzando un file system collegato in rete e un archivio dati resiliente oppure è possibile acquistare una soluzione integrata. Se si desidera combinare la resilienza con il ripristino di emergenza, è disponibile la replica del disco asincrona, che consente la replica del disco su decine o centinaia di chilometri.

È possibile configurare il modo in cui le diverse directory WebSphere MQ vengono associate al supporto di memorizzazione, per utilizzare al meglio il supporto. Per i gestori code *a più istanze* esiste una distinzione importante tra due tipi di file e directory WebSphere MQ .

Directory che devono essere condivise tra le istanze di un gestore code.
Le informazioni che devono essere condivise tra diverse istanze di un gestore code si trovano in due directory: le directory `qmgrs` e `logs` . Le directory devono trovarsi su un file system di rete condiviso. Si consiglia di utilizzare un supporto di archiviazione che fornisce alta disponibilità continua e prestazioni eccellenti perché i dati cambiano costantemente quando i messaggi vengono creati ed eliminati.

Le directory e i file che non *hanno* da condividere tra le istanze di un gestore code.
Alcune altre directory non devono essere condivise tra diverse istanze di un gestore code e vengono ripristinate rapidamente mediante mezzi diversi dall'utilizzo di un file system sottoposto a mirroring.

- WebSphere MQ e la directory degli strumenti. Sostituire reinstallando o eseguendo il backup e il ripristino da un archivio di file di cui è stato eseguito il backup.
- Informazioni di configurazione modificate per l'installazione nel suo insieme. Le informazioni di configurazione sono gestite da WebSphere MQ, ad esempio il file `mqs.ini` su sistemi Windows, UNIX and Linux o parte della propria gestione della configurazione, ad esempio gli script di configurazione **MQSC** . Eseguire il backup e il ripristino utilizzando un archivio file.
- Output a livello di installazione come tracce, log degli errori e file FFDC. I file sono memorizzati nelle sottodirectory `errors` e `trace` nella directory di dati predefinita. La directory dei dati predefinita sui sistemi UNIX and Linux è `/var/mqm` . In Windows , la directory dei dati predefinita è la directory di installazione di `WebSphere MQ` .

È anche possibile utilizzare un gestore code di backup per eseguire backup di supporti regolari di un gestore code a più istanze utilizzando la registrazione lineare. Un gestore code di backup non fornisce un ripristino rapido come da un file system sottoposto a mirroring e non recupera le modifiche dall'ultimo backup. Il meccanismo del gestore code di backup è più appropriato per l'utilizzo in scenari di ripristino di emergenza offsite rispetto al ripristino di un gestore code dopo un malfunzionamento della memoria localizzata.

Combinazione di soluzioni IBM WebSphere MQ Availability
Le applicazioni stanno utilizzando altre funzionalità IBM WebSphere MQ per migliorare la disponibilità. I gestori code a più istanze completano altre capacità di alta disponibilità.

IBM WebSphere MQ I cluster aumentano la disponibilità della coda
È possibile aumentare la disponibilità della coda creando più definizioni di una coda cluster; fino a un massimo di una coda su ciascun gestore nel cluster.

Si supponga che un membro del cluster abbia esito negativo e quindi venga inviato un nuovo messaggio a una coda cluster. A meno che il messaggio *non abbia* per passare al gestore code non riuscito, il messaggio viene inviato a un'altro gestore code in esecuzione nel cluster che ha una definizione della coda.

Anche se i cluster aumentano notevolmente la disponibilità, ci sono due scenari di errore correlati che provocano il ritardo dei messaggi. La creazione di un cluster con gestori code a più istanze riduce la probabilità che un messaggio venga ritardato.

Messaggi marooned
Se un gestore code nel cluster ha esito negativo, nessun altro messaggio che può essere instradato ad altri gestori code nel cluster viene instradato al gestore code non riuscito. I messaggi che sono già stati inviati vengono cancellati fino al riavvio del gestore code in errore.

Affinità

Affinità è il termine utilizzato per descrivere le informazioni condivise tra due calcoli altrimenti separati. Ad esempio, esiste un'affinità tra un'applicazione che invia un messaggio di richiesta a un server e la stessa applicazione che prevede di elaborare la risposta. Un altro esempio potrebbe essere una sequenza di messaggi, l'elaborazione di ogni messaggio in base ai messaggi precedenti.

Se si inviano messaggi alle code cluster, è necessario considerare le affinità. È necessario inviare messaggi successivi allo stesso gestore code oppure ogni messaggio può essere inviato a qualsiasi membro del cluster?

Se è necessario inviare messaggi allo stesso gestore code nel cluster e questo ha esito negativo, i messaggi attendono nella coda di trasmissione del mittente fino a quando il gestore code del cluster non è di nuovo in esecuzione.

Se il cluster è configurato con gestori code a più istanze, il ritardo nell'attesa del riavvio del gestore code non riuscito è limitato all'ordine di un minuto o più mentre lo standby prende il sopravvento. Quando lo standby è in esecuzione, i messaggi di cui è stato eseguito il marooned riprendono l'elaborazione, i canali per l'istanza del gestore code appena attivata vengono avviati e i messaggi che erano in attesa nelle code di trasmissione iniziano a fluire.

Un modo possibile per configurare un cluster per superare i messaggi ritardati da un gestore code non riuscito consiste nel distribuire due diversi gestori code a ciascun server nel cluster e fare in modo che uno sia attivo e uno sia l'istanza in standby dei diversi gestori code. Questa è una configurazione di standby attivo e aumenta la disponibilità del cluster.

Oltre a beneficiare di una gestione ridotta e di una maggiore scalabilità, i cluster continuano a fornire ulteriori elementi di disponibilità per integrare i gestori code a più istanze. I cluster proteggono da altri tipi di errori che influiscono sia sulle istanze attive che su quelle in standby di un gestore code.

Servizio ininterrotto
Un cluster fornisce un servizio ininterrotto. I nuovi messaggi ricevuti dal cluster vengono inviati ai gestori code attivi per l'elaborazione. Non fare affidamento su un gestore code a più istanze per fornire un servizio ininterrotto perché il gestore code in standby impiega del tempo per rilevare l'errore e completarne l'avvio, per riconnettere i canali e per inoltrare nuovamente i batch di messaggi non riusciti.

Interruzione localizzata
Esistono limitazioni pratiche alla distanza tra i server attivi, standby e file system, poiché devono interagire a velocità di millisecondi per fornire prestazioni accettabili.

I gestori code con cluster richiedono velocità di interazione dell'ordine di molti secondi e possono essere geograficamente distribuiti ovunque nel mondo.

Errore operativo
Utilizzando due meccanismi diversi per aumentare la disponibilità, si riducono le probabilità che un errore operativo, come un errore umano, comprometta i propri sforzi di disponibilità.

I gruppi di condivisione della coda aumentano la disponibilità di elaborazione dei messaggi

I gruppi di condivisione code, forniti solo su z/OS, consentono a un gruppo di gestori code di condividere una coda. Se un gestore code ha esito negativo, gli altri gestori code continuano a elaborare tutti i messaggi sulla coda. I gestori code a più istanze non sono supportati su z/OS e integrano i gruppi di condivisione code solo come parte di un'architettura di messaggistica più ampia.

I client WebSphere MQ aumentano la disponibilità delle applicazioni

I programmi client WebSphere MQ MQI possono connettersi a diversi gestori code in un gruppo di gestori code in base alla disponibilità del gestore code, al peso della connessione e alle affinità. Eseguendo un'applicazione su una macchina differente rispetto a quella su cui è in esecuzione il gestore code, è possibile migliorare la disponibilità generale di una soluzione purché esista un modo per riconnettere l'applicazione se l'istanza del gestore code a cui è connessa non riesce.

I gruppi di gestori code vengono utilizzati per incrementare la disponibilità del client separando un client da un gestore code arrestato e bilanciando il carico delle connessioni client in un gruppo di gestori code, piuttosto che come un sprayer IP. L'applicazione client non deve avere alcuna affinità con il gestore code in errore, ad esempio una dipendenza da una particolare coda, oppure non può riprendere l'elaborazione.

La riconnessione automatica del client e i gestori code a più istanze aumentano la disponibilità del client risolvendo alcuni problemi di affinità. La riconnessione automatica del client non è supportata dalle classi WebSphere MQ per Java.

È possibile impostare l'opzione `MQCNO` `MQCNO_RECONNECT_Q_MGR`per forzare un client a riconnettersi allo stesso gestore code:

1. Se il gestore code a istanza singola precedentemente connesso non è in esecuzione, la connessione viene ritentata fino a quando il gestore code non è nuovamente in esecuzione.
2. Se il gestore code è configurato come gestore code a più istanze, il client si riconnette all'istanza attiva.

Ricollegandosi automaticamente allo stesso gestore code, vengono ripristinate molte delle informazioni di stato che il gestore code deteneva per conto del client, ad esempio le code che aveva aperto e l'argomento a cui aveva effettuato la sottoscrizione. Se il client ha aperto una coda di risposta dinamica per ricevere una risposta a una richiesta, viene ripristinata anche la connessione alla coda di risposta.

Verifica che i messaggi non vadano persi (registrazione)

WebSphere MQ registra tutte le informazioni necessarie per il recupero da un malfunzionamento del gestore code.

WebSphere MQ registra tutte le modifiche significative ai dati controllati dal gestore code in un log di recupero.

Ciò include la creazione e l'eliminazione di oggetti, aggiornamenti di messaggi persistenti, stati delle transazioni, modifiche agli attributi degli oggetti e attività del canale. Il file di log contiene le informazioni necessarie per ripristinare tutti gli aggiornamenti alle code di messaggi mediante:

- Conservazione dei record delle modifiche del gestore code
- Conservazione dei record degli aggiornamenti della coda per l'utilizzo da parte del processo di riavvio
- Abilitazione al ripristino dei dati dopo un errore hardware o software

Tuttavia, WebSphere MQ si basa anche sul sistema disco che ospita i relativi file. Se il sistema disco è esso stesso inaffidabile, le informazioni, incluse le informazioni di log, possono ancora essere perse.

Aspetto dei log

I log sono costituiti da file primari e secondari e un file di controllo. Si definisce il numero e la dimensione dei file di log e la posizione in cui vengono memorizzati nel file system.

Un log WebSphere MQ è costituito da due componenti:

1. Uno o più file di dati di log.
2. Un file di controllo log

Un file di dati di log è noto anche come estensione di log.

Esistono diversi file di log che contengono i dati registrati. È possibile definire il numero e la dimensione (come spiegato in “Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code” a pagina 422) oppure utilizzare il valore predefinito di sistema di tre file.

In WebSphere MQ per Windows, ognuno dei tre file assume il valore predefinito di 1 MB. In WebSphere MQ per sistemi UNIX and Linux , ognuno dei tre file assume il valore predefinito di 4 MB.

Quando si crea un gestore code, il numero di file di log definito è il numero di file di log *primari* assegnati. Se non si specifica un numero, viene utilizzato il valore predefinito.

In WebSphere MQ per Windows, se non è stato modificato il percorso di log, i file di log vengono creati nella directory:

```
C:\Program Files\IBM\WebSphere MQ\log\<QMgrName>
```

Nei sistemi WebSphere MQ per UNIX and Linux , se non è stato modificato il percorso di log, i file di log vengono creati nella directory:

```
/var/mqm/log/<QMgrName>
```

WebSphere MQ inizia con questi file di log primari, ma se lo spazio di log primario non è sufficiente, assegna i file di log *secondari* . Lo fa dinamicamente e li rimuove quando la richiesta di spazio di log si riduce. Per impostazione predefinita, è possibile assegnare fino a due file di log secondari. È possibile modificare questa allocazione predefinita, come descritto in "Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code" a pagina 422.

Il file di controllo log

Il file di controllo log contiene le informazioni necessarie per controllare l'utilizzo dei file di log, come la loro dimensione e ubicazione e il nome del successivo file disponibile.

Il file di controllo log è solo per uso interno del gestore code.

Il gestore code conserva i dati di controllo associati con lo stato del log di ripristino nel file di controllo log e non è necessario modificare il contenuto del file di controllo log.

Nota: Assicurarsi che i log creati quando si avvia un gestore code siano abbastanza grandi da contenere la dimensione e il volume dei messaggi che verranno gestiti dalle applicazioni. Sarà probabilmente necessario modificare i numeri di log predefiniti e le dimensioni per soddisfare le esigenze. Per ulteriori informazioni, vedere "Calcolo della dimensione del log" a pagina 407.

Tipi di registrazione

In WebSphere MQ, il numero di file richiesti per la registrazione dipende dalla dimensione del file, dal numero di messaggi ricevuti e dalla lunghezza dei messaggi. Esistono due modi per conservare i record delle attività dei gestori code: registrazione circolare e registrazione lineare.

registrazione circolare

Utilizzare la registrazione circolare se si desidera solo riavviare il ripristino, utilizzando il log per eseguire il rollback delle transazioni che erano in corso quando il sistema è stato arrestato.

La registrazione circolare mantiene tutti i dati di riavvio in un anello di file di log. La registrazione completa il primo file dell'anello e quindi passa al successivo e così via, fino a quando tutti i file sono completi. Successivamente, torna al primo file dell'anello e ricomincia. Questo processo va avanti finché il prodotto è in uso e comporta il vantaggio che non si rimane mai senza file di log durante l'esecuzione.

WebSphere MQ conserva le voci di log richieste per riavviare il gestore code senza perdita di dati fino a quando non sono più necessarie per garantire il ripristino dei dati del gestore code. Il meccanismo per rilasciare i file di log per il riutilizzo è descritto in "Utilizzo del punto di controllo per garantire il ripristino completo" a pagina 404.

registrazione lineare

Utilizzare la registrazione lineare se si desidera riavviare il ripristino e il ripristino del supporto (ricreando i dati persi o danneggiati riproducendo il contenuto del log). La registrazione lineare gestisce i dati del log in una sequenza continua di file. Lo spazio non viene riutilizzato, pertanto è possibile recuperare in qualsiasi momento qualsiasi record registrato in qualsiasi estensione log non eliminata.

Poiché lo spazio su disco è limitato, potrebbe essere necessario pensare a qualche forma di archiviazione. Si tratta di un'attività di gestione per gestire lo spazio su disco per il log, riutilizzando o estendendo lo spazio esistente come necessario.

Il numero di file di log utilizzati con la registrazione lineare può essere molto elevato, a seconda del flusso di messaggi e della durata del gestore code. Tuttavia, esistono diversi file che si dice siano *attivi*. I file attivi contengono le voci di log richieste per riavviare il gestore code. Collettivamente, i file di log attivi sono noti come *log attivi*. Il numero di file di log attivi è generalmente inferiore al numero di file di log primari come definito nei file di configurazione. (Consultare "Calcolo della dimensione del log" a pagina 407 per informazioni sulla definizione del numero.)

L'evento chiave che controlla se un file di log è definito attivo o meno è un *punto di controllo*. Un punto di controllo WebSphere MQ è un punto di coerenza tra il log di recupero e i file oggetto. Un punto di controllo determina la serie di file di log necessari per eseguire il ripristino del riavvio. I file di log non attivi non sono richiesti per il ripristino del riavvio e sono definiti inattivi. In alcuni casi, i file di log inattivi sono richiesti per il ripristino del supporto. (Consultare "Utilizzo del punto di controllo per garantire il ripristino completo" a pagina 404 per ulteriori informazioni sul checkpoint.)

I file di log inattivi possono essere archiviati perché non sono richiesti per il ripristino del riavvio. I file di log inattivi che non sono richiesti per il ripristino del supporto possono essere considerati come file di log superflui. È possibile eliminare i file di log superflui se non sono più di interesse per l'operazione. Fare riferimento a "Gestione dei log" a pagina 409 per ulteriori informazioni sulla disposizione dei file di log.

Se un nuovo punto di controllo viene registrato nel secondo file di log primario o in un file successivo, il primo file può diventare inattivo e un nuovo file primario viene formattato e aggiunto alla fine del pool primario, ripristinando il numero di file primari disponibili per la registrazione. In questo modo, il pool di file di log principale può essere visualizzato come una serie corrente di file in un elenco di file di log sempre esteso. Ancora una volta, è un'attività amministrativa gestire i file inattivi in base ai requisiti dell'operazione.

Sebbene i file di log secondari siano definiti per la registrazione lineare, non vengono utilizzati nelle normali operazioni. Se si verifica una situazione quando, probabilmente a causa di transazioni di lunga durata, non è possibile liberare un file dal pool attivo perché potrebbe essere ancora richiesto per un riavvio, i file secondari vengono formattati e aggiunti al pool di file di log attivo.

Se si utilizza il numero di file secondari disponibili, le richieste per la maggior parte delle operazioni che richiedono l'attività di log verranno rifiutate con un codice di ritorno MQRC_RESOURCE_PROBLEM restituito all'applicazione.

Entrambi i tipi di registrazione possono far fronte a una perdita di alimentazione imprevista, supponendo che non vi siano errori hardware.

Utilizzo del punto di controllo per garantire il ripristino completo

I checkpoint sincronizzano i file di log e i dati del gestore code e contrassegnano un punto di congruenza da cui è possibile eliminare i record di log. Il checkpoint frequente rende il recupero più rapido.

Gli aggiornamenti permanenti alle code messaggi si verificano in due fasi. Innanzitutto, i record che rappresentano l'aggiornamento vengono scritti nel log, quindi il file di coda viene aggiornato. I file di log possono quindi diventare più aggiornati rispetto ai file della coda. Per garantire che l'elaborazione del riavvio inizi da un punto congruente, WebSphere MQ utilizza i punti di controllo. Un punto di controllo è un momento in cui il record descritto nel log è uguale al record nella coda. Il punto di controllo è costituito dalla serie di record di log necessari per riavviare il gestore code; ad esempio, lo stato di tutte le transazioni (unità di lavoro) attive al momento del punto di controllo.

WebSphere MQ genera automaticamente i checkpoint.Vengono utilizzati quando il gestore code viene avviato, all'arresto, quando lo spazio di registrazione è insufficiente e dopo ogni 10.000 operazioni registrate.

Man mano che le code gestiscono ulteriori messaggi, il record del punto di controllo diventa incongruente con lo stato corrente delle code.

Quando WebSphere MQ viene riavviato, trova l'ultimo record del punto di controllo nel log. Queste informazioni vengono conservate nel file del punto di controllo aggiornato alla fine di ogni punto di controllo. Il record del punto di controllo rappresenta il punto di coerenza più recente tra il log e i dati. Tutte le operazioni che hanno avuto luogo dopo il checkpoint vengono rieseguite in avanti. Questa è nota come fase di ripetizione. La fase di ripetizione riporta le code allo stato logico in cui si trovavano prima dell'errore o della chiusura del sistema. Durante la fase di ripetizione, viene creato un elenco delle transazioni che erano in corso quando si è verificato l'errore di sistema o la chiusura. I messaggi AMQ7229 e AMQ7230 vengono emessi per indicare l'avanzamento della fase di riproduzione.

Per conoscere le operazioni di cui eseguire il backout o il commit, WebSphere MQ accede a ciascun record di log attivo associato a una transazione incompleta. Questa è nota come fase di recupero. I messaggi AMQ7231, AMQ7232 e AMQ7234 vengono emessi per indicare l'avanzamento della fase di ripristino.

Una volta eseguito l'accesso a tutti i record di log necessari durante la fase di recupero, ciascuna transazione attiva viene a sua volta risolta e ciascuna operazione associata alla transazione verrà sottoposta a backout o a commit. Questa è nota come la fase di risoluzione. Il messaggio AMQ7233 viene emesso per indicare l'avanzamento della fase di risoluzione.

WebSphere MQ mantiene i puntatori interni alla testa e alla coda del log. Sposta il puntatore di testa al punto di controllo più recente congruente con il ripristino dei dati del messaggio.

I punti di controllo vengono utilizzati per rendere più efficiente il recupero e per controllare il riutilizzo dei file di log primari e secondari.

In Figura 69 a pagina 406, tutti i record prima dell'ultimo punto di controllo, Checkpoint 2, non sono più necessari per WebSphere MQ. Le code possono essere recuperate dalle informazioni del punto di controllo e da eventuali voci di log successive. Per la registrazione circolare, è possibile riutilizzare tutti i file liberati prima del punto di controllo. Per un log lineare, non è più necessario accedere ai file di log liberati per le normali operazioni e diventare inattivi. Nell'esempio, il puntatore di testa della coda viene spostato in modo da puntare all'ultimo punto di controllo, Checkpoint 2, che diventa la nuova testa della coda, Head 2. Il file di log 1 può ora essere riutilizzato.

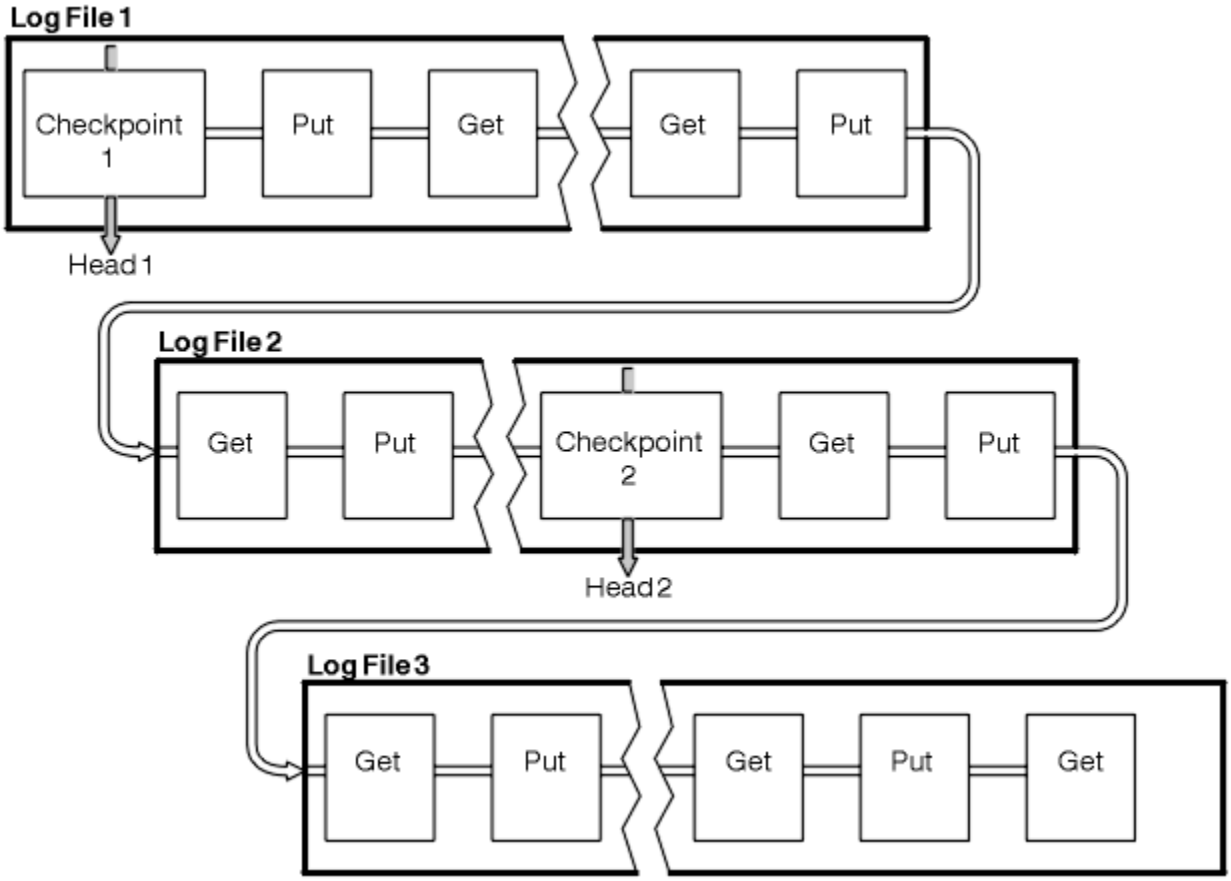


Figura 69. Checkpoint

Checkpoint con transazioni di lunga durata

Come una transazione di lunga durata influisce sul riutilizzo dei file di log.

Figura 70 a pagina 407 mostra in che modo una transazione di lunga durata influisce sul riutilizzo dei file di log. Nell'esempio, una transazione di lunga durata ha creato una voce nel log, mostrata come LR 1, dopo il primo checkpoint visualizzato. La transazione non viene completata (al punto LR 2) fino a dopo il terzo punto di controllo. Tutte le informazioni di log da LR 1 in poi vengono conservate per consentire il ripristino di tale transazione, se necessario, fino al completamento.

Una volta completata la transazione di lunga durata, in LR 2, la parte principale del log viene spostata in Checkpoint 3, l'ultimo checkpoint registrato. I file che contengono i record di log prima del punto di controllo 3, intestazione 2, non sono più necessari. Se si utilizza la registrazione circolare, lo spazio può essere riutilizzato.

Se i file di log primari sono completamente pieni prima del completamento della transazione di lunga durata, i file di log secondari vengono utilizzati per evitare che i log si riempiano.

Quando l'intestazione del log viene spostata e si utilizza la registrazione circolare, i file di log primari potrebbero diventare idonei per il riutilizzo e il programma di registrazione, dopo aver riempito il file corrente, riutilizza il primo file primario disponibile. Se si utilizza la registrazione lineare, l'intestazione del log viene ancora spostata verso il basso nel pool attivo e il primo file diventa inattivo. Un nuovo file primario viene formattato e aggiunto alla fine del lotto in modo da essere pronto per future attività di registrazione.

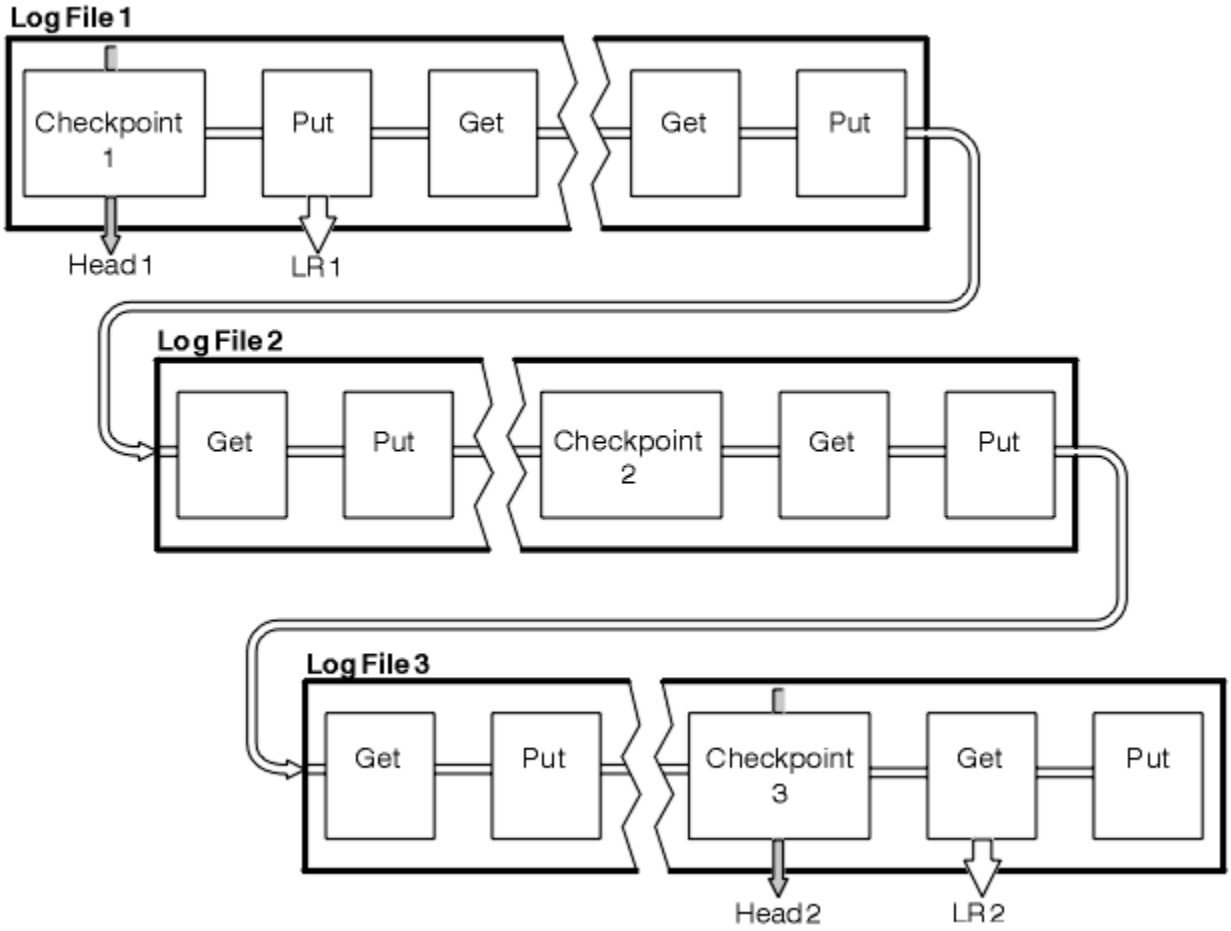


Figura 70. Checkpoint con una transazione di lunga durata

Calcolo della dimensione del log

Stima della dimensione del log necessaria per un gestore code.

Dopo aver deciso se il gestore code utilizza la registrazione circolare o lineare, è necessario valutare la dimensione del log di cui il gestore code ha bisogno. La dimensione del log è determinata dai seguenti parametri di configurazione del log:

LogFilePages
La dimensione di ciascun file di log primario e secondario in unità di pagine 4K

LogPrimaryFiles
Il numero di file di log primari preassegnati

LogSecondaryFiles
Il numero di file di log secondari che è possibile creare per l'utilizzo quando i file di log primari sono pieni

Tabella 31 a pagina 408 mostra la quantità di dati che il gestore code registra per varie operazioni. La maggior parte delle operazioni del gestore code richiede una quantità minima di spazio di log.Tuttavia, quando un messaggio persistente viene inserito in una coda, **tutti** i dati del messaggio devono essere scritti nel log per rendere possibile il ripristino del messaggio. La dimensione del log dipende, generalmente, dal numero e dalla dimensione dei messaggi persistenti che il gestore code deve gestire.

Tabella 31. Dimensioni delle voci di log (tutti i valori sono approssimativi)

Operazione	**Dimensione**
Inserisci messaggio persistente	750 byte + lunghezza messaggio Se il messaggio è grande, viene diviso in segmenti di 261844 byte, ogni segmento aggiunge altri 300 byte.
Acquisisci messaggio	260 byte
Punto di sincronizzazione, commit	750 byte
Punto di sincronizzazione, rollback	1000 byte + 12 byte per ogni get o put di cui eseguire il rollback
Crea oggetto	1500 byte
Elimina oggetto	300 byte
Modifica attributi	1024 byte
Registra immagine supporto	800 byte + immagine L'immagine è divisa in segmenti di 260 000 byte, ogni segmento aggiunge altri 300 byte.
Punto di controllo	750 byte + 200 byte per ogni unità di lavoro attiva + 380 byte per ogni canale mittente del cluster, se si utilizzano più code di trasmissione del cluster per gestore code. Ulteriori dati potrebbero essere registrati per eventuali inserimenti o richiami non sottoposti a commit che vengono memorizzati nel buffer per motivi di prestazioni. Se si dispone di canali mittenti del cluster, ad ogni checkpoint vengono scritti ulteriori 380 byte nel log per canale mittente del cluster.

Nota:

1. È possibile modificare il numero di file di log primari e secondari ogni volta che il gestore code viene avviato.
2. Non è possibile modificare la dimensione del file di log; è necessario determinarlo **prima** di creare il gestore code.
3. Il numero di file di log primari e la dimensione del log determinano la quantità di spazio di log preassegnato quando viene creato il gestore code.
4. Il numero totale di file di log primari e secondari non può essere superiore a 511 su sistemi UNIX and Linux o a 255 su Windows, che in presenza di transazioni di lunga durata, limita la quantità massima di spazio di log disponibile per il gestore code per il riavvio del ripristino. La quantità di spazio di log di cui il gestore code potrebbe aver bisogno per il ripristino del supporto non condivide questo limite.
5. Quando viene utilizzata la registrazione *circolare* , il gestore code riutilizza spazio di log primario. Ciò significa che il log del gestore code può essere inferiore alla quantità di dati stimata che il gestore code deve registrare. Il gestore code assegnerà, fino a un limite, un file di log secondario quando un file di log diventa pieno e il successivo file di log primario nella sequenza non è disponibile.
6. I file di log primari vengono resi disponibili per il riutilizzo durante un checkpoint. Il gestore code prende in considerazione sia lo spazio di log primario che quello secondario prima di prendere in considerazione un punto di controllo perché la quantità di spazio di log è insufficiente.

Se non si definiscono più file di log primari rispetto ai file di log secondari, il gestore code potrebbe assegnare i file di log secondari prima di eseguire un punto di controllo. Ciò rende i file di log primari disponibili per il riutilizzo.

Gestione dei log

I log sono quasi autogestiti, ma a volte hanno bisogno di gestirli per risolvere i problemi di spazio.

Nel tempo, alcuni dei record di log scritti non sono più necessari per riavviare il gestore code. Se si sta utilizzando la registrazione circolare, il gestore code recupera lo spazio liberato nei file di log. Questa attività non è evidente all'utente e di solito non si vede ridurre la quantità di spazio su disco utilizzato poiché lo spazio allocato viene riutilizzato rapidamente.

Dei record di log, solo quelli scritti dall'inizio dell'ultimo punto di controllo completo e quelli scritti da qualsiasi transazione attiva, sono necessari per riavviare il gestore code. Pertanto, il log potrebbe essere riempito se un punto di controllo non è stato utilizzato per un lungo periodo di tempo o se una transazione di lunga durata ha scritto un record di log molto tempo fa. Il gestore code tenta di eseguire i checkpoint abbastanza spesso per evitare il primo problema.

Quando una transazione di lunga durata riempie il log, i tentativi di scrittura dei record di log hanno esito negativo e alcune chiamate MQI restituiscono MQRC_RESOURCE_PROBLEM. Lo spazio è riservato per eseguire il commit o il rollback di tutte le transazioni in corso, quindi **MQCMIT** o **MQBACK** non dovrebbero avere esito negativo.

Il gestore code esegue il rollback delle transazioni che utilizzano troppo spazio di log. Un'applicazione che ha una transazione viene sottoposta a rollback in questo modo non può eseguire operazioni **MQPUT** o **MQGET** successive specificando il punto di sincronizzazione nella stessa transazione. Un tentativo di inserire o richiamare un messaggio nel punto di sincronizzazione in questo stato restituisce MQRC_BACKED_OUT. L'applicazione può quindi emettere **MQCMIT**, che restituisce MQRC_BACKED_OUT o **MQBACK** e avviare una nuova transazione. Quando è stato eseguito il rollback della transazione che consuma troppo spazio di log, il relativo spazio di log viene rilasciato e il gestore code continua a funzionare normalmente.

Se il log si riempie, viene emesso il messaggio AMQ7463 . Inoltre, se il log si riempie perché una transazione di lunga durata ha impedito il rilascio dello spazio, viene emesso il messaggio AMQ7465 .

Infine, se i record vengono scritti nel log più velocemente di quanto il log possa elaborare, viene emesso il messaggio AMQ7466 . Se viene visualizzato questo messaggio, aumentare il numero di file di log o ridurre la quantità di dati elaborati dal gestore code.

Cosa succede quando un disco si riempie

Il componente di registrazione del gestore code può gestire un disco completo e file di log completi. Se il disco contenente il log si riempie, il gestore code emette il messaggio AMQ6708 e viene eseguito un record di errore.

I file di log vengono creati alla loro dimensione massima, piuttosto che essere estesi quando i record di log vengono scritti in essi. Ciò significa che WebSphere MQ può esaurire lo spazio su disco solo quando crea un nuovo file; non può esaurire lo spazio quando scrive un record nel log. WebSphere MQ sa sempre quanto spazio è disponibile nei file di log esistenti e gestisce di conseguenza lo spazio all'interno dei file.

Se si riempie l'unità contenente i file di log, è possibile liberare dello spazio su disco. Se si utilizza un log lineare, potrebbero essere presenti alcuni file di log inattivi nella directory di log ed è possibile copiare questi file su un'altra unità o dispositivo. Se lo spazio è ancora insufficiente, verificare che la configurazione del log nel file di configurazione del gestore code sia corretta. È possibile ridurre il numero di file di log primari o secondari in modo che il log non sia superiore allo spazio disponibile. Non è possibile modificare la dimensione dei file di log per un gestore code esistente. Il gestore code presuppone che tutti i file di log abbiano la stessa dimensione.

Gestione dei file di log

Assegnare spazio sufficiente per i file di log. Per la registrazione lineare, è possibile eliminare i vecchi file di log quando non sono più necessari.

Se si sta utilizzando la registrazione circolare, verificare che vi sia spazio sufficiente per conservare i file di log quando si configura il sistema (consultare “Impostazioni predefinite di log per IBM WebSphere MQ” a pagina 431 e “Log del gestore code” a pagina 440). La quantità di spazio su disco utilizzata dal log non aumenta oltre la dimensione configurata, incluso lo spazio per i file secondari da creare quando richiesto.

Se si utilizza un log lineare, i file di log vengono aggiunti continuamente quando vengono registrati i dati e la quantità di spazio su disco utilizzato aumenta con il tempo. Se la velocità dei dati registrati è elevata, lo spazio su disco viene utilizzato rapidamente dai nuovi file di log.

Nel tempo, i file di log meno recenti per un log lineare non sono più richiesti per riavviare il gestore code o per eseguire il ripristino dei supporti di tutti gli oggetti danneggiati. Di seguito sono riportati i metodi per determinare quali file di log sono ancora richiesti:

Messaggi di evento del programma di registrazione
Quando questa opzione è abilitata, i messaggi di evento del logger vengono generati quando i gestori code iniziano a scrivere i record di log in un nuovo file di log. Il contenuto dei messaggi di evento del programma di registrazione specifica i file di log ancora richiesti per il riavvio del gestore code e per il recupero del supporto. Per ulteriori informazioni sui messaggi di evento del logger, consultare Eventi del logger

Stato gestore code
L'esecuzione del comando MQSC, DISPLAY QMSTATUS, o del comando PCF, Inquire Queue Manager Status, restituisce le informazioni sul gestore code, inclusi i dettagli dei file di log richiesti. Per ulteriori informazioni sui comandi MQSC, consultare Script (MQSC) Commands e per informazioni sui comandi PCF, consultare Automazione delle attività di gestione.

Messaggi del gestore code
Periodicamente, il gestore code emette una coppia di messaggi per indicare quali file di log sono necessari:

- Il messaggio AMQ7467 fornisce il nome del file di log più vecchio richiesto per riavviare il gestore code. Questo file di log e tutti i file di log più recenti devono essere disponibili durante il riavvio del gestore code.
- Il messaggio AMQ7468 fornisce il nome del file di log più vecchio necessario per il ripristino del supporto.

Solo i file di log richiesti per il riavvio del gestore code, i file di log attivi, devono essere in linea. I file di log inattivi possono essere copiati su un supporto di archivio come ad esempio un nastro per il ripristino di emergenza e rimossi dalla directory di log. I file di log inattivi che non sono richiesti per il ripristino del supporto possono essere considerati come file di log superflui. È possibile eliminare i file di log superflui se non sono più di interesse per l'operazione.

Per determinare i file di log "più vecchi" e "più nuovi", utilizzare il numero del file di log piuttosto che le ore di modifica applicate dal file system.

Se non è possibile trovare alcun file di log necessario, viene emesso il messaggio dell'operatore AMQ6767 . Rendere il file di log e tutti i file di log successivi disponibili per il gestore code e ritentare l'operazione.

Nota: Quando si esegue il ripristino del supporto, tutti i file di log richiesti devono essere disponibili nella directory del file di log contemporaneamente. Assicurarsi di prendere regolarmente le immagini dei supporti di tutti gli oggetti che si desidera ripristinare per evitare di esaurire lo spazio su disco per contenere tutti i file di log richiesti. Per prendere un'immagine di supporto di tutti i tuoi oggetti nel tuo gestore code, esegui il comando **rcdmqimg** come mostrato nei seguenti esempi:

In Windows

```
rcdmqimg -m QMNAME -t all *
```

Su UNIX and Linux

```
rcdmqimg -m QMNAME -t all "*"
```

L'esecuzione di **rcdmqimg** sposta l'LSN (media log sequence number) in avanti. Per ulteriori dettagli sui numeri di sequenza log, consultare “Dump del contenuto del log utilizzando il comando dmpmqlog” a pagina 414. **rcdmqimg** non viene eseguito automaticamente, pertanto deve essere eseguito manualmente o da un'attività automatica creata. Per ulteriori informazioni relative a questo comando, consultare rcdmqimg e dmpmqlog.

Nota: I messaggi AMQ7467 e AMQ7468 possono essere emessi anche quando si esegue il comando `rcdmqimg` .

Determinazione dei file di log superflui
Quando si gestiscono i file di log lineari, è importante verificare quali file possono essere eliminati o archiviati. Queste informazioni ti aiuteranno a prendere questa decisione.

Non utilizzare le ore di modifica del file system per determinare i file di log "più vecchi". Utilizzare solo il numero del file di log. L'utilizzo dei file di log da parte del gestore code segue regole complesse, inclusa la pre - assegnazione e la formattazione dei file di log prima che siano necessari. È possibile visualizzare i file di log con le ore di modifica che potrebbero essere fuorvianti se si tenta di utilizzare queste ore per determinare l'età relativa.

Per determinare il file di log meno recente necessario per riavviare il gestore code, immettere il comando `DISPLAY QMSTATUS RECLOG`.

Per determinare il file di log più vecchio necessario per eseguire il ripristino del supporto, immettere il comando `DISPLAY QMSTATUS MEDIALOG`.

In generale, un numero di file di log inferiore implica un log meno recente. A meno che non si abbia un turnover dei file di log molto elevato, dell'ordine di 3000 file di log al giorno per 10 anni, non è necessario soddisfare il numero di wrapping di 9 999 999. In questo caso, è possibile archiviare qualsiasi file di log con un numero inferiore al valore RECLOG ed è possibile eliminare qualsiasi file di log con un numero inferiore ai valori RECLOG e MEDIALOG.

Se, tuttavia, si ha un turnover molto elevato dei file di log, o si desidera essere sicuri di far fronte al caso generale, di solito può essere utilizzato il seguente algoritmo:

```
S == riavviare il numero del file di log
          (da VISUALIZZA QMSTATUS RECLOG).
Contiamo M == numero file di log di recupero del supporto
           (da DISPLAY QMSTATUS MEDIALOG).
Lasciare L == un numero di file di log con idoneità per l'eliminazione o l'archiviazione
            che deve essere determinato.

minlog funzione (a, b) {
  if (abs (a - b) < 5000000)
    restituisci min (a, b); # Non incluso.
  else
    restituire max (a, b); # Avvolto.}

Un file di log L può essere eliminato se
       (L! = S & & L! = M & & minlog (L, minlog (S, M) == L).
Un file di log L può essere archiviato se
       (L! = S & & minlog (L, S) == L).
```

Ubicazione file di log

Quando si sceglie un'ubicazione per i propri file di log, tenere presente che l'operazione viene gravemente compromessa se WebSphere MQ non riesce a formattare un nuovo log a causa della mancanza di spazio su disco.

Se si utilizza un log circolare, verificare che vi sia spazio sufficiente sull'unità per almeno i file di log primari configurati. Inoltre, lasciare spazio per almeno un file di log secondario, che è necessario se il log deve crescere.

Se si utilizza un log lineare, consentire una quantità di spazio notevolmente maggiore; lo spazio utilizzato dal log aumenta continuamente man mano che vengono registrati i dati.

Idealmente, posizionare i file di log su un'unità disco separata dai dati del gestore code. Questo ha dei vantaggi in termini di prestazioni. Potrebbe anche essere possibile posizionare i file di log su più unità disco in una disposizione di mirroring. Ciò protegge da malfunzionamenti dell'unità che contiene il log. Senza il mirroring, è possibile tornare all'ultimo backup del sistema WebSphere MQ .

Utilizzo del log per il ripristino

Utilizzo dei log per il recupero da errori.

Esistono diversi modi in cui i dati possono essere danneggiati. WebSphere MQ consente di eseguire il ripristino da:

- Un oggetto dati danneggiato
- Una perdita di potenza nel sistema
- Un errore di comunicazione

Questa sezione esamina come vengono utilizzati i log per risolvere questi problemi.

Ripristino da perdita di alimentazione o errori di comunicazione

WebSphere MQ può essere ripristinato da errori di comunicazione e perdita di alimentazione. Inoltre, può a volte recuperare da altri tipi di problemi, come l'eliminazione involontaria di un file.

In caso di errore di comunicazione, i messaggi rimangono in coda fino a quando non vengono rimossi da un'applicazione ricevente. Se il messaggio è in fase di trasmissione, rimane nella coda di trasmissione fino a quando non può essere trasmesso correttamente. Per eseguire il ripristino da un errore di comunicazioni, di solito è possibile riavviare i canali utilizzando il collegamento non riuscito.

Se si perde l'alimentazione, quando il gestore code viene riavviato WebSphere MQ ripristina le code al loro stato di commit al momento dell'errore. Ciò garantisce che nessun messaggio persistente venga perso. I messaggi non persistenti vengono eliminati; non sopravvivono quando WebSphere MQ si arresta bruscamente.

Recupero degli oggetti danneggiati

Esistono modi in cui un oggetto IBM WebSphere MQ può diventare inutilizzabile, ad esempio a causa di danni involontari. È quindi necessario ripristinare il proprio sistema completo o una parte di esso. L'azione richiesta dipende dal momento in cui viene rilevato il danno, se il metodo di registrazione selezionato supporta il ripristino del supporto e quali oggetti sono danneggiati.

Ripristino supporti

Il ripristino dei supporti ricrea gli oggetti dalle informazioni registrate in un log lineare. Ad esempio, se un file oggetto viene inavvertitamente cancellato o diventa inutilizzabile per qualche altro motivo, il ripristino del supporto può ricrearlo. Le informazioni nel log richieste per il ripristino del supporto di un oggetto vengono denominate *immagine supporto*.

Un'immagine del supporto è una sequenza di record di log che contengono un'immagine di un oggetto da cui l'oggetto stesso può essere ricreato.

Il primo record di log richiesto per ricreare un oggetto è noto come *record di ripristino del supporto*; è l'inizio dell'ultima immagine del supporto per l'oggetto. Il record di recupero supporti di ciascun oggetto è una delle informazioni registrate durante un punto di controllo.

Quando un oggetto viene ricreato dalla sua immagine multimediale, è anche necessario riprodurre tutti i record di log che descrivono gli aggiornamenti eseguiti sull'oggetto dall'ultima immagine.

Considerare, ad esempio, una coda locale che ha un'immagine dell'oggetto della coda presa prima che un messaggio persistente venga inserito nella coda. Per ricreare l'immagine più recente dell'oggetto, è necessario riprodurre le voci del log che registrano l'inserimento del messaggio nella coda, oltre a riprodurre l'immagine stessa.

Quando un oggetto viene creato, i record di log scritti contengono informazioni sufficienti per ricrearlo completamente. Questi record costituiscono la prima immagine multimediale dell'oggetto. Quindi, ad ogni arresto, il gestore code registra automaticamente le immagini dei media come segue:

- Immagini di tutte le code e gli oggetti del processo non locali
- Immagini di code locali vuote

Le immagini del supporto possono anche essere registrate manualmente utilizzando il comando **rcdmqimg** , descritto nella sezione rcdmqimg. Questo comando scrive un'immagine del supporto dell'oggetto IBM WebSphere MQ . Quando è stata scritta un'immagine del supporto, solo i log che contengono l'immagine del supporto e tutti i log creati dopo questo periodo di tempo sono richiesti per ricreare gli oggetti danneggiati. Il vantaggio della creazione di immagini multimediali dipende da fattori quali la quantità di memoria libera disponibile e la velocità con cui vengono creati i file di log.

Ripristino da immagini multimediali

Un gestore code recupera automaticamente alcuni oggetti dall'immagine del supporto durante l'avvio del gestore code. Recupera automaticamente una coda se è stata coinvolta in una transazione che era incompleta quando il gestore code è stato chiuso l'ultima volta e risulta danneggiata o danneggiata durante il processo di riavvio.

È necessario recuperare altri oggetti manualmente, utilizzando il comando **rcrmqobj** , che riproduce i record nel log per creare nuovamente l'oggetto IBM WebSphere MQ . L'oggetto viene ricreato dalla sua ultima immagine trovata nel log, insieme a tutti gli eventi di log applicabili tra l'ora in cui l'immagine è stata salvata e l'ora in cui è stato emesso il comando di ricreazione. Se un oggetto IBM WebSphere MQ viene danneggiato, le uniche azioni valide che è possibile eseguire sono l'eliminazione o la ricreazione mediante questo metodo. I messaggi non persistenti non possono essere recuperati in questo modo.

Per ulteriori informazioni sul comando **rcrmqobj** , consultare rcrmqobj .

Il file di log contenente il record di ripristino del supporto e tutti i successivi file di log devono essere disponibili nella directory del file di log quando si tenta il ripristino del supporto di un oggetto. Se non è possibile trovare un file richiesto, viene emesso il messaggio operatore AMQ6767 e l'operazione di ripristino del supporto ha esito negativo. Se non si prendono immagini di supporti regolari degli oggetti che si desidera ricreare, lo spazio su disco potrebbe non essere sufficiente per contenere tutti i file di log richiesti per ricreare un oggetto.

Ripristino degli oggetti danneggiati durante l'avvio

Se il gestore code rileva un oggetto danneggiato durante l'avvio, l'azione che intraprende dipende dal tipo di oggetto e se il gestore code è configurato per supportare il ripristino dei supporti.

Se l'oggetto gestore code è danneggiato, il gestore code non può essere avviato a meno che non sia in grado di ripristinare l'oggetto. Se il gestore code è configurato con un log lineare e quindi supporta il ripristino dei supporti, IBM WebSphere MQ tenta automaticamente di ricreare l'oggetto gestore code dalle relative immagini dei supporti. Se il metodo di log selezionato non supporta il ripristino del supporto, è possibile ripristinare un backup del gestore code o eliminare il gestore code.

Se le transazioni erano attive quando il gestore code è stato arrestato, le code locali che contengono i messaggi persistenti, senza commit immessi o ricevuti all'interno di queste transazioni sono richieste anche per avviare correttamente il gestore code. Se una di queste code locali risulta danneggiata e il gestore code supporta il recupero dei supporti, tenta automaticamente di ricrearle dalle relative immagini dei supporti. Se una qualsiasi delle code non può essere ripristinata, IBM WebSphere MQ non può essere avviato.

Se le code locali danneggiate contenenti messaggi non sottoposti a commit vengono rilevate durante l'elaborazione di avvio su un gestore code che non supporta il ripristino dei supporti, le code vengono contrassegnate come oggetti danneggiati e i messaggi non sottoposti a commit vengono ignorati. Questa situazione è dovuta al fatto che non è possibile eseguire il ripristino dei supporti degli oggetti danneggiati su un gestore code di questo tipo e l'unica azione rimasta è eliminarli. Viene emesso il messaggio AMQ7472 per segnalare eventuali danni.

Recupero di oggetti danneggiati in altri momenti

Il ripristino dei supporti degli oggetti è automatico solo durante l'avvio. Altre volte, quando viene rilevato un danneggiamento dell'oggetto, viene emesso il messaggio dell'operatore AMQ7472 e la maggior parte delle operazioni che utilizzano l'oggetto ha esito negativo. Se l'oggetto del gestore code è danneggiato in qualsiasi momento dopo l'avvio del gestore code, il gestore code esegue una chiusura preventiva. Quando un oggetto è stato danneggiato, è possibile eliminarlo oppure, se il gestore code sta utilizzando un log lineare, tentare di recuperarlo dall'immagine del supporto utilizzando il comando `rcrmqobj` (per ulteriori dettagli, consultare rcrmqobj).

Protezione dei file di log IBM WebSphere MQ

Non toccare i file di log quando un gestore code è in esecuzione, il ripristino potrebbe essere impossibile. Utilizzare l'autorizzazione superutente o mqm per proteggere i file di log da modifiche involontarie.

Non rimuovere manualmente i file di log attivi quando è in esecuzione un gestore code IBM WebSphere MQ . Se un utente elimina inavvertitamente i file di log che un gestore code deve riavviare, IBM WebSphere MQ **non** emette errori e continua a elaborare i dati *inclusi i messaggi persistenti*. Il gestore code viene arrestato normalmente, ma il riavvio potrebbe non riuscire. Il recupero dei messaggi diventa quindi impossibile.

Gli utenti che dispongono dell'autorizzazione per rimuovere i log utilizzati da un gestore code attivo hanno anche l'autorizzazione per eliminare altre importanti risorse del gestore code (come i file di coda, il catalogo oggetti e i file eseguibili IBM WebSphere MQ). Possono quindi danneggiare, forse a causa dell'inesperienza, un gestore code in esecuzione o inattivo in un modo rispetto al quale IBM WebSphere MQ non può proteggersi.

Prestare attenzione quando si conferiscono le autorizzazioni di super utente o mqm.

Dump del contenuto del log utilizzando il comando dmpmqlog

Come utilizzare il comando `dmpmqlog` per eseguire il dump del contenuto del log del gestore code.

Utilizzare il comando `dmpmqlog` per eseguire il dump del contenuto del log del gestore code. Per impostazione predefinita, viene eseguito il dump di tutti i record di log attivi, ossia, il comando avvia il dump dall'inizio del log (di solito l'avvio dell'ultimo punto di controllo completato).

Il log può essere scaricato solo quando il gestore code non è in esecuzione. Poiché il gestore code prende un punto di controllo durante l'arresto, la porzione attiva del log di solito contiene un numero ridotto di record di log. Tuttavia, è possibile utilizzare il comando `dmpmqlog` per eseguire il dump di più record di log utilizzando una delle seguenti opzioni per modificare la posizione iniziale del dump:

- Avviare il dump dalla *base* del log. La base del log è il primo record di log nel file di log che contiene l'intestazione del log. La quantità di dati aggiuntivi di cui viene eseguito il dump in questo caso dipende da dove è posizionata l'intestazione del log nel file di log. Se è vicino all'inizio del file di log, viene eseguito il dump solo di una piccola quantità di dati aggiuntivi. Se l'intestazione è vicina alla fine del file di log, viene eseguito il dump di un numero significativamente maggiore di dati.
- Specificare la posizione iniziale del dump come singolo record di log. Ogni record di log è identificato da un *LSN (log sequence number)*univoco. Nel caso di registrazione circolare, questo record di log iniziale non può essere prima della base del log; questa restrizione non si applica ai log lineari. Potrebbe essere necessario ripristinare i file di log inattivi prima di eseguire il comando. È necessario specificare un LSN valido, preso dall'output `dmpmqlog` precedente, come posizione iniziale.

  Ad esempio, con la registrazione lineare è possibile specificare `nextlsn` dall'ultimo output `dmpmqlog` . `nextlsn` viene visualizzato in `Log File Header` e indica l'LSN del successivo record di log da scrivere. Utilizzarlo come posizione iniziale per formattare tutti i record di registrazione scritti dall'ultima volta che è stato eseguito il dump della registrazione.
- **Solo per i log lineari**, è possibile indicare a `dmpmqlog` di iniziare a formattare i record di log da una determinata estensione del file di log. In tal caso, `dmpmqlog` prevede di individuare questo file di log e ogni file successivo nella stessa directory dei file di log attivi. Questa opzione non si applica ai log circolari, dove `dmpmqlog` non può accedere ai record di log prima della base del log.

L'output del comando dmpmqlog è il `Log File Header` e una serie di record di log formattati. Il gestore code utilizza diversi record di log per registrare modifiche ai propri dati.

Alcune informazioni formattate vengono utilizzate solo internamente. Il seguente elenco include i record di log più utili:

Intestazione file di log
Ogni log ha una singola intestazione del file di log, che è sempre la prima cosa formattata dal comando dmpmqlog . Contiene i seguenti campi:

logattivo	Il numero di estensioni log principali.
loginattivo	Il numero di estensioni log secondarie.
dimensione_log	Il numero di pagine da 4 KB per estensione.
base	Il primo LSN nell'estensione log contenente l'intestazione del log.
Nextlsn	L'LSN del successivo record di log da scrivere.
intestazioni	L'LSN del record di log all'inizio del log.
tailsn	L'LSN che identifica la posizione di coda del registro.
hflag1	Se il log è CIRCULAR o LOG RETAIN (lineare).
HeadExtentHeadExtent	L'estensione del log contenente l'intestazione del log.

Intestazione record log
Ogni record di log all'interno del log ha un'intestazione fissa che contiene le seguenti informazioni:

LSN	Il numero di sequenza log.
LogRecdTipo	Il tipo di record di log.
XTranid	L'identificativo della transazione associato a questo record di log (se presente). Un *TranType* di MQI indica una transazione solo WebSphere MQ. Un *TranType* di XA è coinvolto con altri gestori risorse. Gli aggiornamenti coinvolti nella stessa unità di lavoro hanno lo stesso *XTranid*.
QueueName	La coda associata a questo record di log (se presente).
Qid	L'identificativo interno univoco per la coda.
PrevLSN	L'LSN del record di log precedente all'interno della stessa transazione (se presente).

Avvia gestore code
Questo log indica che il gestore code è stato avviato.

StartDate	La data di avvio del gestore code.
StartTime	L'ora in cui è stato avviato il gestore code.

Arresta gestore code
Questo log indica che il gestore code è stato arrestato.

StopDate	La data in cui il gestore code è stato arrestato.
StopTime	L'ora in cui il gestore code è stato arrestato.
ForceFlag	Il tipo di arresto utilizzato.

Avvia punto di controllo
Indica l'inizio di un checkpoint del gestore code.

Termina punto di controllo
Indica la fine di un checkpoint del gestore code.

ChkPtChkPt L'LSN del record di log che ha avviato questo punto di controllo.

Inserisci messaggio
Registra un messaggio persistente inserito in una coda. Se il messaggio è stato inserito nel punto di sincronizzazione, l'intestazione del record di log contiene un *XTranid*non null. Il resto del record contiene:

MapIndex Un identificativo per il messaggio sulla coda. Può essere utilizzato per far corrispondere il MQGET corrispondente utilizzato per richiamare questo messaggio dalla coda. In questo caso, è possibile trovare un record di log *Get Message* successivo contenente gli stessi QueueName e MapIndex. A questo punto l'identificativo MapIndex può essere riutilizzato per un messaggio di inserimento successivo a tale coda.

Dati Nel dump esadecimale per questo record di log sono contenuti vari dati interni seguiti dal descrittore del messaggio (eyecatcher MD) e dai dati del messaggio stessi.

Inserisci parte
I messaggi permanenti troppo grandi per un singolo record di log vengono registrati come più record di log *Put Part* seguiti da un singolo record *Put Message* . Se sono presenti *Put Part* record, il campo *PrevLSN* concatenerà i record *Put Part* e il record *Put Message* finale.

Dati Continua i dati del messaggio in cui è stato lasciato il record di log precedente.

Richiama messaggio
Vengono registrati solo i richiami dei messaggi persistenti. Se il messaggio è stato ottenuto nel punto di sincronizzazione, l'intestazione del record di log contiene un *XTranid*non null. Il resto del record contiene:

MapIndex Identifica il messaggio che è stato richiamato dalla coda. Il record di log *Put Message* più recente contenente lo stesso *QueueName* e *MapIndex* identifica il messaggio che è stato richiamato.

Priorità Q La priorità del messaggio richiamato dalla coda.

Avvia transazione
Indica l'inizio di una nuova transazione. Un TranType di MQI indica una transazione solo WebSphere MQ. Un TranType di XA indica uno che coinvolge altri gestori risorse. Tutti gli aggiornamenti effettuati da questa transazione avranno lo stesso *XTranid*.

Prepara transazione
Indica che il gestore code è preparato per eseguire il commit degli aggiornamenti associati al *XTranid*specificato. Questo record di log viene scritto come parte di un commit a due fasi che coinvolge altri gestori risorse.

Esegui commit transazione
Indica che il gestore code ha eseguito il commit di tutti gli aggiornamenti effettuati da una transazione.

Rollback transazione
Ciò denota l'intenzione del gestore code di eseguire il rollback di una transazione.

Fine transazione
Indica la fine di una transazione di cui è stato eseguito il rollback.

Tabella transazioni
Questo record viene scritto durante il punto di sincronizzazione. Registra lo stato di ogni transazione che ha effettuato aggiornamenti permanenti. Per ogni transazione vengono registrate le seguenti informazioni:

XTranid	L'identificativo della transazione.
FirstLSN	L'LSN del primo record di log associato alla transazione.
LastLSN	L'LSN dell'ultimo record di log associato alla transazione.

Partecipanti alla transazione
Questo record di log viene scritto dal componente Gestore transazioni XA del gestore code. Registra i gestori risorse esterni che partecipano alle transazioni. Per ogni partecipante viene registrato quanto segue:

NomeRM	Il nome del gestore risorse.
IDRM	L'identificativo del gestore risorse. Viene registrato anche nei successivi record di log *Transaction Prepared* che registrano le transazioni globali a cui partecipa il gestore risorse.
SwitchFile	Il file di caricamento switch per questo gestore risorse.
XAOpenString	La stringa di apertura XA per questo gestore risorse.
XACloseString	La stringa di chiusura XA per questo gestore risorse.

Transazione preparata
Questo record di log viene scritto dal componente Gestore transazioni XA del gestore code. Indica che la transazione globale specificata è stata preparata correttamente. A ciascun gestore risorse partecipante verrà richiesto di eseguire il commit. Il *RMID* di ogni gestore risorse preparato viene registrato nel record di log. Se il gestore code stesso partecipa alla transazione, sarà presente un *Participant Entry* con un *RMID* uguale a zero.

Transazione non utilizzata
Questo record di log viene scritto dal componente Gestore transazioni XA del gestore code. Segue il record di log *Transaction Prepared* quando la decisione di commit è stata consegnata a ogni partecipante.

Elimina coda
Questo registra il fatto che tutti i messaggi in una coda sono stati eliminati, ad esempio, utilizzando il comando MQSC CLEAR QUEUE.

Attributi Coda
Registra l'inizializzazione o la modifica degli attributi di una coda.

Crea oggetto
Questo registra la creazione di un oggetto WebSphere MQ .

ObjName	Il nome dell'oggetto creato.
UserId	L'ID utente che esegue la creazione.

Elimina oggetto
Questo registra l'eliminazione di un oggetto WebSphere MQ .

ObjName	Il nome dell'oggetto che è stato eliminato.

Backup e ripristino dei dati del gestore code IBM WebSphere MQ

Backup dei gestori code e dei dati del gestore code.

Periodicamente, è possibile adottare misure per proteggere i gestori code da possibili danneggiamenti causati da malfunzionamenti hardware. Esistono tre modi per proteggere un gestore code:

Eseguire il backup dei dati del gestore code

Se l'hardware ha esito negativo, è possibile che venga forzato l'arresto di un gestore code. Se i dati di log del gestore code vengono persi a causa di un errore hardware, il gestore code potrebbe non essere in grado di riavviarsi. Se si esegue il backup dei dati del gestore code, è possibile ripristinare alcuni o tutti i dati del gestore code persi.

In generale, più spesso si esegue il backup dei dati del gestore code, meno dati si perdono in caso di errore hardware che causa la perdita di integrità del log di recupero.

Per eseguire il backup dei dati del gestore code, il gestore code non deve essere in esecuzione.

Per eseguire il backup e ripristinare i dati del gestore code, consultare:

- "Backup dei dati del gestore code" a pagina 418.
- "Ripristino dei dati del gestore code" a pagina 419.

Utilizza un gestore code di backup

Se l'errore hardware è grave, un gestore code potrebbe non essere recuperabile. In questa situazione, se il gestore code non recuperabile ha un gestore code di backup dedicato, il gestore code di backup può essere attivato al posto del gestore code non recuperabile. Se è stato aggiornato regolarmente, il log del gestore code di backup può contenere dati di log che includono l'ultimo log completo dal gestore code non recuperabile.

Un gestore code di backup può essere aggiornato mentre il gestore code esistente è in esecuzione.

Per creare e attivare un gestore code di backup, consultare:

- "Creazione di un gestore code di backup" a pagina 420.
- "Avvio di un gestore code di backup" a pagina 421.

Solo backup della configurazione del gestore code

Se l'hardware ha esito negativo, è possibile che venga forzato l'arresto di un gestore code. Se la configurazione del gestore code e i dati di log vengono persi a causa di un errore hardware, il gestore code non sarà in grado di riavviarsi o di essere ripristinato dal log. Se si esegue il backup della configurazione del gestore code, sarà possibile ricreare il gestore code e tutti i relativi oggetti dalle definizioni salvate.

Per eseguire il backup della configurazione del gestore code, il gestore code deve essere in esecuzione.

Per eseguire il backup e il ripristino della configurazione del gestore code, consultare:

- "Backup della configurazione del gestore code" a pagina 422
- "Ripristino della configurazione del gestore code" a pagina 422

Backup dei dati del gestore code

Il backup dei dati del gestore code consente di evitare possibili perdite di dati causate da errori hardware.

Prima di iniziare

Assicurarsi che il gestore code non sia in esecuzione. Se si tenta di eseguire un backup di un gestore code in esecuzione, il backup potrebbe non essere congruente a causa degli aggiornamenti in corso durante la copia dei file. Se possibile, arrestare il gestore code eseguendo il comando `endmqm -w` (un arresto di attesa), solo se non riesce, utilizzare il comando `endmqm -i` (un arresto immediato).

Informazioni su questa attività

Per eseguire una copia di backup dei dati di un gestore code, completare le seguenti attività:

1. Ricercare le directory in cui il gestore code inserisce i suoi dati e i suoi file di log utilizzando le informazioni nei file di configurazione. Per ulteriori informazioni, vedere “Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code” a pagina 422.

   Nota: Potrebbe essere difficile comprendere i nomi visualizzati nella directory. I nomi vengono trasformati per garantire che siano compatibili con la piattaforma su cui si utilizza WebSphere MQ. Per ulteriori informazioni sulle trasformazioni dei nomi, consultare Understanding WebSphere MQ file names.
2. Eseguire copie di tutte le directory dei dati e dei file di log del gestore code, incluse tutte le sottodirectory.

   Assicurarsi di non perdere alcun file, specialmente il file di controllo log, come descritto in “Aspetto dei log” a pagina 402, e i file di configurazione come descritto in “File di inizializzazione e di configurazione” a pagina 71. Alcune delle directory potrebbero essere vuote, ma sono necessarie tutte per ripristinare il backup in un secondo momento.
3. Conservare le proprietà dei file. Per WebSphere MQ per sistemi UNIX and Linux , è possibile eseguire questa operazione con il comando `tar` . (Se si dispone di code superiori a 2 GB, non è possibile utilizzare il comando `tar` . Per ulteriori informazioni, consultare Abilitazione di code di grandi dimensioni.

   Nota: Quando si esegue l'aggiornamento a WebSphere MQ Versione 7.5 e versioni successive, assicurarsi di eseguire un backup del file **`.ini`** e delle voci di registro. Le informazioni sul gestore code sono memorizzate nel file **`.ini`** e possono essere utilizzate per ripristinare una versione precedente di WebSphere MQ.

Ripristino dei dati del gestore code

Effettuare le operazioni riportate di seguito per ripristinare un backup dei dati di un gestore code.

Prima di iniziare

Assicurarsi che il gestore code non sia in esecuzione.

Informazioni su questa attività

Per ripristinare un backup dei dati di un gestore code:

1. Individuare le directory in cui il gestore code inserisce i suoi dati e i suoi file di log, utilizzando le informazioni nei file di configurazione.
2. Svuotare le directory in cui si desidera inserire i dati di cui è stato eseguito il backup.
3. Copiare i dati del gestore code di cui è stato eseguito il backup e i file di log nelle ubicazioni corrette.
4. Aggiornare i file di informazioni di configurazione.

Controllare la struttura di directory risultante per assicurarsi di disporre di tutte le directory richieste.

Per ulteriori informazioni sulle directory e le sottodirectory IBM WebSphere MQ , consultare Directory structure on Windows systems e Directory content on UNIX and Linux systems .

Accertarsi di disporre di un file di controllo log e dei file di log. Verificare inoltre che i file di configurazione di IBM WebSphere MQ e del gestore code siano congruenti in modo che WebSphere MQ possa cercare i dati ripristinati nelle ubicazioni corrette.

Per la registrazione circolare, eseguire il backup dei dati del gestore code e delle directory dei file di log contemporaneamente in modo da ripristinare una serie coerente di dati e log del gestore code.

Per la registrazione lineare, eseguire contemporaneamente il backup dei dati del gestore code e delle directory dei file di log. È possibile ripristinare solo i file di dati del gestore code se è disponibile una sequenza completa corrispondente di file di log.

Nota: Quando si esegue l'aggiornamento a WebSphere MQ Versione 7.5 e versioni successive, assicurarsi di eseguire un backup del file **`.ini`** e delle voci di registro. Le informazioni sul gestore code sono

memorizzate nel file **.ini** e possono essere utilizzate per ripristinare una versione precedente di WebSphere MQ.

Risultati

Se è stato eseguito il backup e il ripristino corretto dei dati, il gestore code verrà avviato.

Utilizzo di un gestore code di backup

Un gestore code esistente può avere un gestore code di backup dedicato.

Un gestore code di backup è una copia inattiva del gestore code esistente. Se il gestore code esistente diventa irreversibile a causa di un grave errore hardware, il gestore code di backup può essere portato in linea per sostituire il gestore code irreversibile.

I file di log del gestore code esistenti devono essere regolarmente copiati nel gestore code di backup per garantire che il gestore code di backup rimanga un metodo efficace per il ripristino di emergenza. Non è necessario arrestare il gestore code esistente per copiare i file di log, tuttavia è necessario copiare un file di log solo se il gestore code ha terminato la scrittura su di esso. Poiché il log del gestore code esistente viene continuamente aggiornato, esiste sempre una leggera discrepanza tra il log del gestore code esistente e i dati del log copiati nel log del gestore code di backup. Gli aggiornamenti regolari al gestore code di backup riducono la discrepanza tra i due log.

Se un gestore code di backup deve essere portato in linea, deve essere attivato e quindi avviato. Il requisito di attivare un gestore code di backup prima che venga avviato è una misura preventiva da proteggere dall'avvio accidentale di un gestore code di backup. Una volta attivato, un gestore code di backup non può essere più aggiornato.

Per informazioni su come creare, aggiornare e avviare un gestore code di backup, consultare i seguenti argomenti:

- “Creazione di un gestore code di backup” a pagina 420
- “Aggiornamento di un gestore code di backup” a pagina 421
- “Avvio di un gestore code di backup” a pagina 421

Creazione di un gestore code di backup

È possibile utilizzare un gestore code di backup solo quando si utilizza la registrazione lineare.

Per creare un gestore code di backup per un gestore code esistente, effettuare le seguenti operazioni:

1. Creare un gestore code di backup per il gestore code esistente utilizzando il comando di controllo `crtmqm`. Il gestore code di backup richiede quanto segue:
   - Per avere gli stessi attributi del gestore code esistente, ad esempio il nome del gestore code, il tipo di registrazione e la dimensione del file di log.
   - Essere sulla stessa piattaforma del gestore code esistente.
   - Essere a un livello di codice uguale o superiore a quello del gestore code esistente.
2. Eseguire copie di tutte le directory dei file di log e dei dati del gestore code esistenti, incluse tutte le sottodirectory, come descritto in “Backup dei dati del gestore code” a pagina 418.
3. Sovrascrivere le directory dei file di log e dei dati del gestore code di backup, incluse le sottodirectory, con le copie prese dal gestore code esistente.
4. Eseguire il seguente comando di controllo sul gestore code di backup:

   ```
   strmqm -r BackupQMName
   ```

   Questo contrassegna il gestore code come gestore code di backup all'interno di WebSphere MQe riproduce tutte le estensioni di log copiate per portare il gestore code di backup al passo con il gestore code esistente.

Aggiornamento di un gestore code di backup

Per garantire che un gestore code di backup rimanga un metodo efficace per il ripristino di emergenza, è necessario aggiornarlo regolarmente.

L'aggiornamento regolare riduce la discrepanza tra il log del gestore code di backup e il log del gestore code corrente. Non è necessario arrestare il gestore code di cui eseguire il backup.

Per aggiornare un gestore code di backup, effettuare le seguenti operazioni:

1. Immettere il seguente comando di script (MQSC) sul gestore code di cui eseguire il backup:

   ```
   RESET QMGR TYPE(ADVANCELOG)
   ```

   Questa operazione arresta qualsiasi scrittura nel log corrente e quindi avanza la registrazione del gestore code all'estensione di log successiva. Ciò garantisce il backup di tutte le informazioni registrate all'ora corrente.
2. Ottenere il numero (nuovo) di estensione del log attivo corrente emettendo il seguente comando Script (MQSC) sul gestore code di cui eseguire il backup:

   ```
   DIS QMSTATUS CURRLOG
   ```
3. Copiare i file di estensione di log aggiornati dalla directory di log del gestore code corrente alla directory di log del gestore code di backup - copiare tutte le estensioni di log dall'ultimo aggiornamento e fino all'estensione corrente (ma non inclusa) indicata nel passo 2. Copiare solo i file di estensione log, quelli che iniziano con "S. ..".
4. Immettere il seguente comando di controllo sul gestore code di backup:

   ```
   strmqm -r BackupQMName
   ```

   Ciò riproduce tutte le estensioni di log copiate e porta il gestore code di backup al passo con il gestore code. Al termine della riproduzione, si riceve un messaggio che identifica tutte le estensioni di log richieste per il ripristino del riavvio e tutte le estensioni di log richieste per il ripristino del supporto.

   Avviso: Se si copia una serie di log di `non-contiguous` nella directory di log del gestore code di backup, verranno riprodotti solo i log fino al punto in cui si trova il primo log mancante.

Avvio di un gestore code di backup

È possibile sostituire un gestore code di backup con un gestore code non recuperabile.

A tal fine, effettuare i seguenti passi:

1. Eseguire il seguente comando di controllo per attivare il gestore code di backup:

   ```
   strmqm -a BackupQMName
   ```

   Il gestore code di backup è attivato. Ora attivo, il gestore code di backup non può più essere aggiornato.
2. Eseguire il seguente comando di controllo per avviare il gestore code di backup:

   ```
   strmqm BackupQMName
   ```

   WebSphere MQ considera questo come un ripristino del riavvio e utilizza il log dal gestore code di backup. Durante l'ultimo aggiornamento alla ripetizione del gestore code di backup, verrà eseguito il rollback solo delle transazioni attive dall'ultimo punto di controllo registrato.

   Quando un gestore code non recuperabile viene sostituito con un gestore code di backup, è possibile che alcuni dati del gestore code non recuperabili vengano persi. La quantità di dati persi dipende

dall'ultimo aggiornamento del gestore code di backup. Più recentemente l'ultimo aggiornamento, meno perdita di dati del gestore code.

3. Riavviare tutti i canali.

Controllare la struttura di directory risultante per assicurarsi di disporre di tutte le directory richieste.

Consultare Pianificazione del supporto file system per ulteriori informazioni sulle directory e le sottodirectory WebSphere MQ .

Accertarsi di disporre di un file di controllo log e dei file di log. Verificare inoltre che i file di configurazione di WebSphere MQ e del gestore code siano congruenti in modo che WebSphere MQ possa ricercare i dati ripristinati nelle ubicazioni corrette.

Se è stato eseguito il backup e il ripristino corretto dei dati, il gestore code verrà avviato.

Nota: Anche se i file di log e i dati del gestore code si trovano in directory differenti, eseguire il backup e ripristinare le directory contemporaneamente. Se i dati e i file di log del gestore code hanno età diverse, il gestore code non è in uno stato valido e probabilmente non verrà avviato. Se inizia, è probabile che i tuoi dati siano danneggiati.

Backup della configurazione del gestore code

Il backup della configurazione del gestore code consente di ricreare un gestore code dalle relative definizioni.

Per eseguire una copia di backup della configurazione di un gestore code:

1. Verificare che il gestore code sia in esecuzione.
2. a. Su AIX, HP-UX, Linux, Solaris o Windows: eseguire il comando di configurazione Dump di MQ (dmpmqcfg) utilizzando l'opzione di formattazione predefinita di (- f mqsc) MQSC e tutti gli attributi (-a), utilizzare il reindirizzamento di output standard per memorizzare le definizioni in un file, ad esempio:

```
dmpmqcfg -m MYQMGR -a > /mq/backups/MYQMGR.mqsc
```

Ripristino della configurazione del gestore code

Effettuare le operazioni riportate di seguito per ripristinare un backup della configurazione di un gestore code.

Per ripristinare un backup della configurazione di un gestore code:

1. Verificare che il gestore code sia in esecuzione. Tenere presente che il gestore code potrebbe essere stato ricreato se il danneggiamento dei dati e dei log non è recuperabile con altri mezzi.
2. A seconda della piattaforma, eseguire uno dei comandi riportati di seguito:
   a. Su AIX, HP-UX, Linux, Solaris o Windows: eseguire runmqsc rispetto al gestore code, utilizzare il reindirizzamento di input standard per ripristinare le definizioni da un file di script generato dal comando Dump di MQ Configuration (dmpmqcfg), ad esempio:

```
runmqsc MYQMGR < /mq/backups/MYQMGR.mqsc
```

Riferimenti correlati

dmpmqcfg

Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code

Modificare il comportamento di IBM WebSphere MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione.

È possibile modificare le informazioni di configurazione di IBM WebSphere MQ modificando i valori specificati su una serie di attributi di configurazione (o parametri) che gestiscono IBM WebSphere MQ.

Modificare le informazioni sull'attributo modificando i file di configurazione di IBM WebSphere MQ . Su IBM WebSphere MQ per le piattaforme Windows e Linux (x86 e x86-64), i file di configurazione IBM WebSphere MQ possono essere modificati utilizzando IBM WebSphere MQ Explorer.

Su sistemi Windows , è possibile utilizzare anche amqmdain per modificare le informazioni di configurazione, come descritto in amqmdain

Per ulteriori informazioni sulla configurazione di IBM WebSphere MQ e dei gestori code per la propria piattaforma, consultare i seguenti argomenti secondari:

Concetti correlati

“Configurazione” a pagina 5
Creare uno o più gestori code su uno o più computer e configurarli sui sistemi di sviluppo, test e produzione per elaborare i messaggi che contengono i dati di business.

Attività correlate

Pianificazione

Amministrazione di WebSphere MQ

Modifica delle informazioni di configurazione sui sistemi UNIX, Linux, and Windows

Gli attributi di configurazione vengono conservati nei file di configurazione, a livello del nodo e del gestore code.

Su piattaforme Windows, UNIX and Linux , è possibile modificare gli attributi di configurazione di IBM WebSphere MQ in:

- Un file di configurazione IBM WebSphere MQ (**mqs.ini**) per applicare le modifiche per IBM WebSphere MQ sul nodo nel suo complesso. Esiste un file mqs.ini per ogni nodo.
- Un file di configurazione del gestore code (**qm.ini**) per applicare le modifiche per specifici gestori code. Esiste un file qm.ini per ogni gestore code sul nodo.

Le opzioni di configurazione del client vengono conservate separatamente, nel file di configurazione del client.

Un file di configurazione (o file ***stanza***) contiene una o più stanze, che sono gruppi di righe nel file .ini che insieme hanno una funzione comune o definiscono parte di un sistema, come funzioni di log, funzioni di canale e servizi installabili.

Poiché il file di configurazione IBM WebSphere MQ viene utilizzato per individuare i dati associati ai gestori code, un file di configurazione non esistente o non corretto può causare l'esito negativo di alcuni o di tutti i comandi MQSC. Inoltre, le applicazioni non possono connettersi a un gestore code che non è definito nel file di configurazione IBM WebSphere MQ .

Qualsiasi modifica apportata a un file di configurazione di solito non diventa effettiva fino al successivo avvio del gestore code.

Su sistemi Windows e Linux (piattaformex86 e x86-64), è possibile modificare le informazioni di configurazione da IBM WebSphere MQ Explorer.

Sui sistemi Windows è anche possibile utilizzare il comando `amqmdain` per modificare i file di configurazione.

Per ulteriori informazioni relative alle opzioni di configurazione su sistemi Windows, UNIX and Linux , consultare i seguenti argomenti secondari:

Concetti correlati

“Configurazione” a pagina 5
Creare uno o più gestori code su uno o più computer e configurarli sui sistemi di sviluppo, test e produzione per elaborare i messaggi che contengono i dati di business.

“Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code” a pagina 422
Modificare il comportamento di IBM WebSphere MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione.

Attività correlate

Pianificazione

Amministrazione di WebSphere MQ

Riferimenti correlati

“Attributi per la modifica delle IBM WebSphere MQ informazioni di configurazione” a pagina 429
Su sistemi IBM WebSphere MQ per Windows e su IBM WebSphere MQ per sistemi Linux (piattaformex86 e x86-64), modificare le informazioni di configurazione utilizzando IBM WebSphere MQ Explorer. Su altri sistemi, modificare le informazioni modificando il file di configurazione mqs.ini .

“Modifica delle informazioni di configurazione del gestore code” a pagina 436
Gli attributi qui descritti modificano la configurazione di un singolo gestore code. Sovrascrivono le impostazioni per WebSphere MQ.

Modifica dei file di configurazione

Modificare i file di configurazione utilizzando i comandi o un editor di testo standard.

Prima di modificare un file di configurazione, eseguirne il backup in modo da disporre di una copia a cui è possibile tornare se necessario.

È possibile modificare i file di configurazione:

- Automaticamente, utilizzando i comandi che modificano la configurazione dei gestori code sul nodo
- Manualmente, utilizzando un editor di testo standard

È possibile modificare i valori predefiniti nei file di configurazione di WebSphere MQ dopo l'installazione.

Se si imposta un valore non corretto su un attributo del file di configurazione, il valore viene ignorato e viene emesso un messaggio operatore per indicare il problema. (L'effetto è lo stesso di perdere completamente l'attributo.)

Quando si crea un nuovo gestore code:

- Eseguire il backup del file di configurazione di WebSphere MQ
- Backup del nuovo file di configurazione del gestore code

I commenti possono essere inclusi nei file di configurazione aggiungendo un carattere ";" o un carattere "#" prima del testo del commento. Se si desidera utilizzare un carattere ";" o un carattere "#" senza che rappresenti un commento, è possibile anteporre al carattere un carattere "\" e verrà utilizzato come parte dei dati di configurazione.

Quando è necessario modificare un file di configurazione?

Modificare un file di configurazione per ripristinare il backup, spostare un gestore code, modificare il gestore code predefinito o per assistere il supporto IBM .

Potrebbe essere necessario modificare un file di configurazione se, ad esempio:

- Si perde un file di configurazione. (Recuperare dal backup, se possibile.)
- È necessario spostare uno o più gestori code in una nuova directory.
- È necessario modificare il gestore code predefinito; ciò potrebbe verificarsi se si elimina accidentalmente il gestore code esistente.
- Si consiglia di farlo dal centro di supporto IBM .

Priorità del file di configurazione

Il valore di un attributo è definito in più posizioni. Gli attributi impostati nei comandi hanno la precedenza rispetto agli attributi nei file di configurazione.

I valori degli attributi di un file di configurazione sono impostati secondo le seguenti priorità:

- I parametri immessi sulla linea di comando hanno la precedenza sui valori definiti nei file di configurazione
- I valori definiti nei file qm.ini hanno la precedenza sui valori definiti nel file mqs.ini

File di configurazione IBM WebSphere MQ , mqs.ini

Il file di configurazione IBM WebSphere MQ , mqs.ini, contiene informazioni relative a tutti i gestori code sul nodo. Viene creato automaticamente durante l'installazione.

Su IBM WebSphere MQ per prodotti UNIX and Linux , la directory dei dati e la directory dei log sono sempre `/var/mqm` e `/var/mqm/log` rispettivamente.

Sui sistemi Windows , l'ubicazione della directory di dati `mqs.inie` l'ubicazione della directory di log sono memorizzate nel registro, poiché la loro ubicazione può variare.

Inoltre, sui sistemi Windows , le informazioni di configurazione dell'installazione (contenute in `mqinst.ini` su IBM WebSphere MQ per sistemi UNIX and Linux) si trovano nel Registro di sistema, poiché non vi è alcun file `mqinst.ini` su Windows.

Il file mqs.ini per i sistemi Windows viene fornito dal WorkPath specificato nella chiave `HKLM\SOFTWARE\IBM\WepSphere MQ` . Il contenuto è:

- I nomi dei gestori code
- Il nome del gestore code predefinito
- L'ubicazione dei file associati a ciascuno di essi

La stanza `LogDefaults` fornita per una nuova installazione di IBM WebSphere MQ non contiene alcun valore esplicito per gli attributi. La mancanza di un attributo indica che l'impostazione predefinita per questo valore viene utilizzata al momento della creazione di un nuovo gestore code. I valori predefiniti vengono visualizzati per la stanza `LogDefaults` in Figura 71 a pagina 426. Un valore zero per l'attributo `LogBufferPages` indica 512.

Se si richiede un valore non predefinito, è necessario specificare esplicitamente tale valore nella sezione `LogDefaults` .

```
#*******************************************************************#
#* Module Name: mqs.ini                                            *#
#* Type       : WebSphere MQ Machine-wide Configuration File       *#
#* Function   : Define WebSphere MQ resources for an entire machine*#
#*******************************************************************#
#* Notes      :                                                    *#
#* 1) This is the installation time default configuration          *#
#*                                                                 *#
#*******************************************************************#
AllQueueManagers:
#*******************************************************************#
#* The path to the qmgrs directory, below which queue manager data *#
#* is stored                                                       *#
#*******************************************************************#
DefaultPrefix=/var/mqm

LogDefaults:
   LogPrimaryFiles=3
   LogSecondaryFiles=2
   LogFilePages=4096
   LogType=CIRCULAR
   LogBufferPages=0
   LogDefaultPath=/var/mqm/log

QueueManager:
   Name=saturn.queue.manager
   Prefix=/var/mqm
   Directory=saturn!queue!manager
   InstallationName=Installation1

QueueManager:
   Name=pluto.queue.manager
   Prefix=/var/mqm
   Directory=pluto!queue!manager
   InstallationName=Installation2

DefaultQueueManager:
   Name=saturn.queue.manager

ApiExitTemplate:
   Name=OurPayrollQueueAuditor
   Sequence=2
   Function=EntryPoint
   Module=/usr/ABC/auditor
   Data=123

ApiExitCommon:
   Name=MQPoliceman
   Sequence=1
   Function=EntryPoint
   Module=/usr/MQPolice/tmqp
   Data=CheckEverything
```

Figura 71. Esempio di file di configurazione IBM WebSphere MQ per i sistemi UNIX

File di configurazione del gestore code, qm.ini

Un file di configurazione del gestore code, qm.ini, contiene informazioni rilevanti per un determinato gestore code.

Esiste un file di configurazione del gestore code per ciascun gestore code. Il file qm.ini viene creato automaticamente quando viene creato il gestore code a cui è associato.

V 7.5.0.9 Da IBM WebSphere MQ Version 7.5.0, Fix Pack 9, il comando **strmqm** controlla la sintassi delle stanze CHANNELS e SSL nel file `qm.ini` prima di avviare completamente il gestore code, il che rende molto più semplice individuare gli errori e correggerli rapidamente se **strmqm** rileva che il file `qm.ini` contiene degli errori. Per ulteriori informazioni, vedere strmqm.

Ubicazione dei file qm.ini

UNIX Linux Windows

Su sistemi UNIX and Linux , un file qm.ini è contenuto nella root della struttura di directory occupata dal gestore code. Ad esempio, il percorso e il nome di un file di configurazione per un gestore code denominato QMNAME è:

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

Su sistemi Windows , l'ubicazione del file qm.ini è fornita dal WorkPath specificato nella chiave HKLM\SOFTWARE\IBM\WebSphere MQ . Ad esempio, il percorso e il nome di un file di configurazione per un gestore code denominato QMNAME è:

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

Il nome del gestore code può avere una lunghezza massima di 48 caratteri. Tuttavia, ciò non garantisce che il nome sia valido o univoco. Pertanto, viene generato un nome di directory basato sul nome del gestore code. Questo processo è noto come *trasformazione del nome*. Per una descrizione, consultare Understanding WebSphere MQ MQ.

File qm.ini di esempio

UNIX Linux

Il seguente esempio mostra in che modo i gruppi di attributi possono essere organizzati in un file di configurazione del gestore code in IBM WebSphere MQ per i sistemi UNIX and Linux .

```
#* Module Name: qm.ini                                               *#
#* Type       : WebSphere MQ queue manager configuration file      *#
#  Function   : Define the configuration of a single queue manager *#
#*                                                                  *#
#*******************************************************************#
#* Notes      :                                                     *#
#* 1) This file defines the configuration of the queue manager     *#
#*                                                                  *#
#*******************************************************************#

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

Service:
   Name=AuthorizationService
   EntryPoints=13

ServiceComponent:
   Service=AuthorizationService
   Name=MQSeries.UNIX.auth.service
   Module=opt/mqm/bin/amqzfu
   ComponentDataSize=0

Log:
   LogPrimaryFiles=3
   LogSecondaryFiles=2
   LogFilePages=4096
   LogType=CIRCULAR
   LogBufferPages=0[1]
   LogPath=/var/mqm/log/saturn!queue!manager/

AccessMode:
   SecurityGroup=wmq\wmq

XAResourceManager:
   Name=DB2 Resource Manager Bank
   SwitchFile=/usr/bin/db2swit
   XAOpenString=MQBankDB
   XACloseString=
   ThreadOfControl=THREAD
```

```
Channels: [2]
   MaxChannels=200
   MaxActiveChannels=100
   MQIBindType=STANDARD

AccessMode:
   SecurityGroup=wmq\wmq
TCP:
   KeepAlive = Yes
   SvrSndBuffSize=32768
   SvrRcvBuffSize=32768
   Connect_Timeout=0

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

ApiExitLocal:
   Name=ClientApplicationAPIchecker
   Sequence=3
   Function=EntryPoint
   Module=/usr/Dev/ClientAppChecker
   Data=9.20.176.20
```

Note:

1. Il valore di zero per `LogBufferPages` fornisce un valore di 512.
2. Per ulteriori informazioni sulla stanza del canale, consultare “File di inizializzazione e di configurazione” a pagina 71.
3. Il numero massimo di stanze XAResourceManager è limitato a 255. Tuttavia, è necessario utilizzare solo un numero ridotto di stanze per evitare la riduzione delle prestazioni della transazione.

WebSphere MQ in UNIX utilizza i file di configurazione con estensione .ini, ad esempio, qm.ini. Esistono alcuni programmi di utilità in WebSphereMQ, come **setmqm**, che eseguiranno una copia di backup temporanea dei file. Ad esempio, il file qm.ini crea una copia di backup denominata qm.ini.bak. Un programma di utilità modifica il file qm.ini , memorizza il file aggiornato, quindi elimina il file qm.ini.bak . Se il programma di utilità non riesce a memorizzare il file qm.ini , ripristina il contenuto di qm.ini dal file di backup qm.ini.bak, quindi elimina il file qm.ini.bak .

Se è presente un file qm.ini.bak , il programma di utilità ripristina il file qm.ini con il contenuto di qm.ini.bak ed elimina il file qm.ini.bak . Pertanto, non è necessario creare copie di backup dei file *.ini utilizzando l'estensione file .bak, poiché tali file di backup potrebbero essere eliminati dai programmi di utilità WebSphere MQ .

Consultare “Modifica delle informazioni di configurazione sui sistemi UNIX, Linux, and Windows” a pagina 423 per informazioni su quando le modifiche diventano effettive.

File di configurazione dell'installazione, mqinst.ini

Sistemi UNIX and Linux

Il file di configurazione dell'installazione, `mqinst.ini`, contiene informazioni su tutte le installazioni di IBM WebSphere MQ su un sistema UNIX o Linux .

Il file `mqinst.ini` si trova nella directory `/etc/opt/mqm` sui sistemi UNIX and Linux . Contiene informazioni su quale installazione, se presente, è l'installazione primaria e le seguenti informazioni per ciascuna installazione:

- Il nome dell'installazione
- La descrizione dell'installazione
- L'identificativo di installazione
- Il percorso di installazione

Questo file non deve essere modificato o a cui si fa riferimento direttamente poiché il formato non è fisso e potrebbe essere modificato. Utilizzare invece i seguenti comandi per creare, eliminare, interrogare e modificare i valori nel file mqinst.ini :

crtmqinst per creare voci.
dltmqinst per eliminare le voci.
dspmqinst per visualizzare le voci.
setmqinst per impostare le voci.

L'identificativo di installazione, solo per uso interno, è impostato automaticamente e non deve essere modificato.

Sistemi Windows

Le informazioni sulla configurazione dell'installazione sono contenute nella seguente chiave sui sistemi Windows :

```
HKLM\SOFTWARE\IBM\WebSphere MQ\Installation\<InstallationName>
```

Questa chiave non deve essere modificata o a cui si fa riferimento direttamente poiché il suo formato non è fisso e potrebbe cambiare. Utilizzare invece i seguenti comandi per eseguire la query e modificare i valori nel registro:

dspmqinst per visualizzare le voci.
setmqinst per impostare le voci.

Su Windows, i comandi **crtmqinst** e **dltmqinst** non sono disponibili. I processi di installazione e disinstallazione gestiscono la creazione e l'eliminazione delle voci di registro richieste.

Attributi per la modifica delle IBM WebSphere MQ informazioni di configurazione

Su sistemi IBM WebSphere MQ per Windows e su IBM WebSphere MQ per sistemi Linux (piattaformex86 e x86-64), modificare le informazioni di configurazione utilizzando IBM WebSphere MQ Explorer. Su altri sistemi, modificare le informazioni modificando il file di configurazione mqs.ini .

Consultare i seguenti argomenti secondari per attributi per componenti specifici:

Concetti correlati

“Configurazione” a pagina 5
Creare uno o più gestori code su uno o più computer e configurarli sui sistemi di sviluppo, test e produzione per elaborare i messaggi che contengono i dati di business.

“Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code” a pagina 422
Modificare il comportamento di IBM WebSphere MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione.

Attività correlate

Pianificazione

Amministrazione di WebSphere MQ

Riferimenti correlati

“Modifica delle informazioni di configurazione del gestore code” a pagina 436
Gli attributi qui descritti modificano la configurazione di un singolo gestore code. Sovrascrivono le impostazioni per WebSphere MQ.

Tutti i gestori code

Utilizzare la pagina delle proprietà `General` e `Extended` WebSphere MQ da IBM WebSphere MQ Explorer o la sezione `AllQueueManagers` nel file mqs.ini per specificare le seguenti informazioni su tutti i gestori code.

DefaultPrefix=*nome_directory*
Questo attributo specifica il percorso della directory qmgrs, all'interno della quale vengono conservati i dati del gestore code.

Se si modifica il prefisso predefinito per il gestore code, replicare la struttura di directory creata al momento dell'installazione.

In particolare, è necessario creare la struttura qmgrs. Arrestare WebSphere MQ prima di modificare il prefisso predefinito e riavviare WebSphere MQ solo dopo aver spostato le strutture nella nuova ubicazione e aver modificato il prefisso predefinito.

Nota: Non eliminare la directory `/var/mqm/errors` sui sistemi UNIX and Linux o la directory `\errors` sui sistemi Windows .

In alternativa alla modifica del prefisso predefinito, è possibile utilizzare la variabile di ambiente MQSPREFIX per sovrascrivere `DefaultPrefix` per il comando `crtmqm` .

A causa delle limitazioni del sistema operativo, mantenere il percorso fornito sufficientemente breve in modo che la somma della lunghezza del percorso e dei nomi dei gestori code abbia una lunghezza massima di 70 caratteri.

ConvEBCDICNewline= NL_TO_LF | TABLE | ISO
Le codepage EBCDIC contengono un carattere di nuova riga (NL) che non è supportato dalle codepage ASCII (anche se alcune varianti ISO di ASCII contengono un equivalente).

Utilizzare l'attributo ConvEBCDICNewline per specificare come WebSphere MQ deve convertire il carattere EBCDIC NL in formato ASCII.

NL_TO_LF
Convertire il carattere NL EBCDIC (X'15 ') nel carattere di avanzamento riga ASCII, LF (X'0A'), per tutte le conversioni da EBCDIC a ASCII.

NL_TO_LF è il valore predefinito.

TABELLA
Convertire il carattere EBCDIC NL in base alle tabelle di conversione utilizzate sulla piattaforma per tutte le conversioni da EBCDIC ad ASCII.

L'effetto di questo tipo di conversione può variare da piattaforma a piattaforma e da lingua a lingua; anche sulla stessa piattaforma, il comportamento potrebbe variare se si utilizzano CCSID differenti.

ISO
Converti:

- CCSID ISO che utilizzano il metodo TABLE
- Tutti gli altri CCSID che utilizzano il metodo NL_TO_CF

I CCSID ISO possibili vengono visualizzati in Tabella 32 a pagina 430.

Tabella 32. Elenco dei CCSID ISO possibili

CCSID	**Serie di codici**
819	ISO8859-1
912	ISO8859-2
915	ISO8859-5
1089	ISO8859-6
813	ISO8859-7
916	ISO8859-8
920	ISO8859-9

Tabella 32. Elenco dei CCSID ISO possibili (Continua)	
CCSID	**Serie di codici**
1051	roman8

Se il CCSID ASCII non è un sottoinsieme ISO, per impostazione predefinita ConvEBCDICNewline è NL_TO_LF.

Gestore code predefinito

Utilizzare la pagina delle proprietà `General` WebSphere MQ da IBM WebSphere MQ Explorer o la sezione `DefaultQueueManager` nel file mqs.ini per specificare il gestore code predefinito.

Nome =*default_queue_manager*
Il gestore code predefinito elabora tutti i comandi per cui non è specificato esplicitamente un nome gestore code. L'attributo `DefaultQueueManager` viene aggiornato automaticamente se si crea un nuovo gestore code predefinito. Se si crea inavvertitamente un nuovo gestore code predefinito e si desidera ripristinare l'originale, modificare manualmente l'attributo `DefaultQueueManager` .

Proprietà di uscita

Utilizzare la pagina delle proprietà `Extended` IBM WebSphere MQ da Esplora risorse di IBM WebSphere MQ o la stanza `ExitProperties` nel file mqs.ini per specificare le opzioni di configurazione utilizzate dai programmi di uscita del gestore code.

CLWLMode=SAFE| FAST
L'uscita del carico di lavoro cluster (CLWL) consente di specificare quale coda cluster nel cluster aprire in seguito a una chiamata MQI (ad esempio, `MQOPEN`, `MQPUT`). L'uscita CLWL viene eseguita in modalità FAST o SAFE in base al valore specificato nell'attributo CLWLMode. Se si omette l'attributo CLWLMode, l'uscita del carico di lavoro del cluster viene eseguita in modalità SAFE.

SAFE
Eseguire l'uscita CLWL in un processo separato dal gestore code. Questa è l'opzione predefinita.

Se si verifica un problema con l'uscita CLWL scritta dall'utente durante l'esecuzione in modalità SAFE, si verifica quanto segue:

- Il processo del server CLWL (amqzlwa0) ha esito negativo.
- Il gestore code riavvia il processo server CLWL.
- L'errore viene riportato nel log degli errori. Se è in corso una chiamata MQI, si riceve una notifica sotto forma di codice di ritorno.

L'integrità del gestore code viene preservata.

Nota: L'esecuzione dell'uscita CLWL in un processo separato può influire sulle prestazioni.

VELOCE
Eseguire l'uscita cluster in linea nel processo del gestore code.

Specificando questa opzione si migliorano le prestazioni evitando i costi di commutazione del processo associati all'esecuzione in modalità SAFE, ma a discapito dell'integrità del gestore code. Si consiglia di eseguire l'uscita CLWL in modalità FAST solo se si è certi che **non** vi sono problemi con l'uscita CLWL e si è particolarmente preoccupati per le prestazioni.

Se si verifica un problema quando l'uscita CLWL è in esecuzione in modalità FAST, il gestore code avrà esito negativo e si corre il rischio che l'integrità del gestore code venga compromessa.

Impostazioni predefinite di log per IBM WebSphere MQ

Utilizzare la pagina delle proprietà di `Default log settings` IBM WebSphere MQ dalla stanza IBM WebSphere MQ Explorero `LogDefaults` nel file mqs.ini per specificare le informazioni sui valori predefiniti di log per tutti i gestori code.

Se la stanza non esiste, verranno utilizzati i valori predefiniti di MQ . Gli attributi di log vengono utilizzati come valori predefiniti quando si crea un gestore code, ma possono essere sovrascritti se si specificano gli attributi di log nel comando `crtmqm` . Consultare **crtmqm** per dettagli su questo comando.

Una volta creato un gestore code, gli attributi di log per tale gestore code vengono ricavati dalle impostazioni descritte in "Log del gestore code" a pagina 440.

Il prefisso predefinito (specificato in "Tutti i gestori code" a pagina 429) e il percorso di log specificato per il particolare gestore code (specificato in "Log del gestore code" a pagina 440) consentono al gestore code e al relativo log di trovarsi in unità fisiche differenti. Questo è il metodo consigliato, anche se per impostazione predefinita si trovano sulla stessa unità.

Per informazioni sul calcolo delle dimensioni del log, consultare "Calcolo della dimensione del log" a pagina 407.

Nota: I limiti forniti nel seguente elenco di parametri sono limiti impostati da WebSphere MQ. I limiti del sistema operativo potrebbero ridurre la dimensione massima possibile del log.

LogPrimaryFiles=3|*2-254* (Windows) |*2-510* (sistemiUNIX and Linux)
I file di log assegnati quando viene creato il gestore code.

Il numero minimo di file di log primari che è possibile avere è 2 e il massimo è 254 su Windowso 510 su sistemi UNIX and Linux . Il valore predefinito è 3.

Il numero totale di file di log primari e secondari non deve superare 255 su Windowso 511 su sistemi UNIX and Linux e non deve essere inferiore a 3.

Una volta creato o avviato il gestore code, il valore viene configurato automaticamente. È possibile modificarlo una volta creato il gestore code. Tuttavia, una modifica del valore non è effettiva fino a quando il gestore code non viene riavviato e l'effetto potrebbe non essere immediato.

LogSecondaryFiles=2|*1-253* (Windows) |*1-509* (sistemiUNIX and Linux)
I file di log assegnati quando i file primari sono esauriti.

Il numero minimo di file di log secondari è 1 e il massimo è 253 su Windowso 509 su sistemi UNIX and Linux . Il numero predefinito è 2.

Il numero totale di file di log primari e secondari non deve superare 255 su Windowso 511 su sistemi UNIX and Linux e non deve essere inferiore a 3.

Il valore viene esaminato quando il gestore code viene avviato. È possibile modificare questo valore, ma le modifiche non diventano effettive fino a quando il gestore code non viene riavviato e anche in questo caso l'effetto potrebbe non essere immediato.

LogFilePages =*numero*
I dati di log sono contenuti in una serie di file denominati file di log. La dimensione del file di log è specificata in unità di pagine da 4 KB.

Il numero predefinito di pagine del file di log è 4096, fornendo una dimensione del file di log di 16 MB.

su sistemi UNIX and Linux il numero minimo di pagine del file di log è 64 e su Windows il numero minimo di pagine del file di log è 32; in entrambi i casi il numero massimo è 65 535.

Nota: La dimensione dei file di log specificati durante la creazione del gestore code non può essere modificata per un gestore code.

LogType=CIRCULAR| LINEAR
Il tipo di log da utilizzare. Il valore predefinito è CIRCULAR.

CIRCULAR
Avviare il ripristino utilizzando il log per eseguire il rollback delle transazioni che erano in corso quando il sistema è stato arrestato.

Consultare "Tipi di registrazione" a pagina 403 per una spiegazione più completa della registrazione circolare.

LINEARE
Sia per il ripristino del riavvio che per il ripristino del supporto o dell'inoltro (creazione di dati persi o danneggiati riproducendo il contenuto della registrazione).

Consultare “Tipi di registrazione” a pagina 403 per una spiegazione più completa della registrazione lineare.

Se si desidera modificare il valore predefinito, è possibile modificare l'attributo LogType o specificare la registrazione lineare utilizzando il comando crtmqm . Non è possibile modificare il metodo di registrazione dopo che è stato creato un gestore code.

LogBufferPages=0|*0 - 4096*
La quantità di memoria assegnata ai record buffer per la scrittura, specificando la dimensione dei buffer in unità di pagine da 4 KB.

Il numero minimo di pagine di buffer è 18 e il massimo è 4096. Buffer più grandi portano ad una maggiore velocità di trasmissione, specialmente per messaggi più grandi.

Se si specifica 0 (valore predefinito), il gestore code seleziona la dimensione. In WebSphere MQ Versione 7.0 , è 512 (2048 KB).

Se si specifica un numero compreso tra 1 e 17, il valore predefinito del gestore code è 18 (72 KB). Se si specifica un numero compreso nell'intervallo tra 18 e 4096, il gestore code utilizza il numero specificato per impostare la memoria assegnata.

LogDefaultPath =*nome_directory*
La directory in cui risiedono i file di log per un gestore code. La directory risiede su una periferica locale in cui il gestore code può scrivere e, preferibilmente, su un'unità differente dalle code di messaggi. La specifica di un'unità differente fornisce una protezione aggiuntiva in caso di errore del sistema.

Il valore predefinito è:

- <DefaultPrefix>\log per WebSphere MQ per Windows dove <DefaultPrefix> è il valore specificato nell'attributo DefaultPrefix nella pagina delle proprietà di All Queue Managers WebSphere MQ . Questo valore viene impostato al momento dell'installazione.
- /var/mqm/log per WebSphere MQ per sistemi UNIX and Linux

In alternativa, è possibile specificare il nome di una directory nel comando crtmqm utilizzando l'indicatore -ld. Quando un gestore code viene creato, viene creata anche una directory nella directory del gestore code, utilizzata per conservare i file di log. Il nome di questa directory è basato sul nome gestore code. Ciò garantisce che il percorso del file di log sia univoco e che sia conforme alle eventuali limitazioni sulle lunghezze dei nomi di directory.

Se non si specifica -ld nel comando crtmqm , viene utilizzato il valore dell'attributo LogDefaultPath nel file mqs.ini .

Il nome del gestore code viene aggiunto al nome della directory per garantire che più gestori code utilizzino directory di log differenti.

Quando il gestore code viene creato, viene creato un valore LogPath negli attributi di log nelle informazioni di configurazione, fornendo il nome completo della directory per il log del gestore code. Questo valore viene utilizzato per individuare il log quando il gestore code viene avviato o eliminato.

LogWriteIntegrity =SingleWrite|DoubleWrite| TripleWrite
Il metodo utilizzato dal programma di registrazione per scrivere in modo affidabile i record di log.

TripleWrite
È il metodo predefinito.

Nota: è possibile selezionare **DoubleWrite** ma, in tal caso, il sistema l'interpreta come **TripleWrite**.

SingleWrite
Si deve utilizzare **SingleWrite** solo se il file system o il dispositivo che ospita il log di ripristino di WebSphere MQ garantisce esplicitamente l'atomicità di scritture di 4KB.

Ossia, quando una scrittura di una pagina di 4KB non riesce per un qualsiasi motivo, i soli due stati possibili sono la pre-immagine o la post-immagine. Non deve essere possibile alcuno stato intermedio.

API (Advanced Configuration and Power Interface)

Utilizzare la pagina delle proprietà di ACPI WebSphere MQ da IBM WebSphere MQ Explorer, per specificare la modalità di funzionamento di WebSphere MQ quando il sistema riceve una richiesta di sospensione.

Windows supporta lo standard ACPI (Advanced Configuration and Power Interface). Ciò consente agli utenti di Windows con hardware abilitato ACPI di arrestare e riavviare i canali quando il sistema entra e riprende dalla modalità di sospensione.

Le impostazioni specificate nella pagina delle proprietà di ACPI WebSphere MQ vengono applicate solo quando il Controllo segnalazioni è in esecuzione. L'icona Controllo segnalazioni è presente sulla barra delle attività se il Controllo segnalazioni è in esecuzione.

DoDialog=Y | N
Visualizza la finestra di dialogo al momento della richiesta di sospensione.

DenySuspend= Y | N
Nega la richiesta di sospensione. Questa opzione viene utilizzata se DoDialog= N o se DoDialog= Y e una finestra di dialogo non possono essere visualizzati, ad esempio, perché il coperchio del notebook è chiuso.

CheckChannelsin esecuzione=Y | N
Verifica se i canali sono in esecuzione. Il risultato può determinare il risultato delle altre impostazioni.

La seguente tabella illustra l'effetto di ciascuna combinazione di questi parametri:

DoDialog	DenySuspend	CheckChannels in esecuzione	Azione
N	N	N	Accettare la richiesta di sospensione.
N	N	Y	Accettare la richiesta di sospensione.
N	Y	N	Negare la richiesta di sospensione.
N	Y	Y	Se sono in esecuzione canali, negare la richiesta di sospensione; in caso contrario, accettare la richiesta.
Y	N	N	Visualizzare la finestra di dialogo (consultare Nota; accettare la richiesta di sospensione). Questa è l'opzione predefinita.
Y	N	Y	Se nessun canale è in esecuzione, accettare la richiesta di sospensione; se viene visualizzata la finestra di dialogo (vedere Nota; accettare la richiesta).
Y	Y	N	Visualizzare la dialogo (Nota; negare la richiesta di sospensione).
Y	Y	Y	Se non è in esecuzione alcun canale, accettare la richiesta di sospensione; se viene visualizzata la finestra di dialogo (Nota; negare la richiesta).

Nota: Nei casi in cui l'azione consiste nel visualizzare la finestra di dialogo, se la finestra di dialogo non può essere visualizzata (ad esempio perché il coperchio del notebook è chiuso), l'opzione DenySuspend viene utilizzata per stabilire se la richiesta di sospensione viene accettata o negata.

Uscite API

Utilizzare il comando IBM WebSphere MQ Explorer o il comando `amqmdain` per modificare le voci per le uscite API.

Utilizzare la pagina delle proprietà di `Exits` IBM WebSphere MQ da IBM WebSphere MQ Explorero la sezione `ApiExitTemplate` e `ApiExitCommon` nel file mqs.ini per identificare le routine di uscita API per tutti i gestori code. Sui sistemi Windows , è anche possibile utilizzare il comando `amqmdain` per modificare le voci per le uscite API. (Per identificare le routine di uscita API per i singoli gestori code, utilizzare la sezione `ApiExitLocal` , come descritto in “Uscite API” a pagina 449.)

Per una descrizione completa degli attributi per queste stanze, consultare Configurazione delle uscite API.

Gestori code

Esiste una stanza `QueueManager` per ogni gestore code. Utilizzare la stanza per specificare l'ubicazione della directory del gestore code.

Su sistemi Windows, UNIX and Linux , esiste una stanza `QueueManager` per ciascun gestore code. Questi attributi specificano il nome del gestore code e il nome della directory contenente i file associati a tale gestore code. Il nome della directory si basa sul nome del gestore code, ma viene trasformato se il nome del gestore code non è un nome file valido. Consultare Informazioni su WebSphere MQ nomi file per ulteriori informazioni sulla trasformazione dei nomi.

Nome =*nome_gestore_coda*
Il nome del gestore code.

Prefisso =*prefisso*
La posizione in cui sono memorizzati i file del gestore code. Per impostazione predefinita, questo valore è lo stesso del valore specificato nell'attributo DefaultPrefix delle informazioni su tutti i gestori code.

Directory =*nome*
Il nome della sottodirectory nella directory `<prefix>\QMGRS` in cui sono memorizzati i file del gestore code. Questo nome si basa sul nome del gestore code, ma può essere trasformato se è presente un nome duplicato o se il nome del gestore code non è un nome file valido.

DataPath=*percorso*
Un percorso dati esplicito fornito quando è stato creato il gestore code, sostituisce Prefisso e Directory come percorso dei dati del gestore code.

InstallationName=*nome*
Il nome dell'installazione di WebSphere MQ associata a questo gestore code. I comandi da questa installazione devono essere utilizzati quando si interagisce con questo gestore code. Se non è presente alcun valore InstallationName , il gestore code è associato a un'installazione di WebSphere MQ precedente alla versione 7.1.

Concetti correlati

“Associazione di un gestore code a un'installazione” a pagina 17
Quando si crea un gestore code, viene automaticamente associato all'installazione che ha emesso il comando **`crtmqm`** . Su UNIX, Linux, and Windows, è possibile modificare l'installazione associata a un gestore code utilizzando il comando **`setmqm`** .

Sicurezza

Utilizzare la stanza `Security` nel file `qm.ini` per specificare opzioni per OAM (Object Authority Manager).

ClusterQueueAccessControl= RQMName | Xmitq
Impostare questo attributo per controllare il controllo accessi delle code cluster o delle code complete ospitate sui gestori code cluster.

RQMNAME
I profili controllati per il controllo accessi delle code ospitate in remoto sono le code denominate o i profili del gestore code.

XMITQ
I profili controllati per il controllo dell'accesso delle code ospitate in remoto vengono risolti in SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Xmitq è il valore predefinito.

GroupModel=GlobalGroups
Questo attributo determina se OAM controlla i gruppi globali durante la determinazione dell'appartenenza a un gruppo di un utente su Windows.

L'impostazione predefinita è di non controllare i gruppi globali.

GlobalGroups
OAM controlla i gruppi globali.

Con GlobalGroups impostato, i comandi di autorizzazione **setmqaut**, **dspmqaut**e **dmpmqaut** accettano i nomi di gruppi globali; consultare il parametro **setmqaut** -g.

Nota: L'impostazione di ClusterQueueAcessControl=RQMName e la presenza di una implementazione personalizzata del servizio di autorizzazione inferiore a MQZAS_VERSION_6 non comporta l'avvio del gestore code. In questa istanza, impostare ClusterQueueAcessControl=Xmitq o aggiornare il servizio di autorizzazione personalizzato a MQZAS_VERSION_6 o superiore.

Modifica delle informazioni di configurazione del gestore code

Gli attributi qui descritti modificano la configurazione di un singolo gestore code. Sovrascrivono le impostazioni per WebSphere MQ.

Sui sistemi UNIX and Linux , modificare le informazioni di configurazione del gestore code modificando il file di configurazione qm.ini . Quando si definisce una stanza in qm.ini, non è necessario avviare ogni elemento su una nuova riga. È possibile utilizzare un punto e virgola (;) o un carattere cancelletto (#) per indicare un commento.

Su sistemi Windows e Linux (piattaformex86 e x86-64), è possibile modificare alcune informazioni di configurazione utilizzando IBM WebSphere MQ Explorer. Tuttavia, poiché ci sono implicazioni significative per la modifica dei servizi installabili e dei loro componenti, i servizi installabili sono di sola lettura in IBM WebSphere MQ Explorer. È pertanto necessario apportare eventuali modifiche ai servizi installabili utilizzando **regedit** su Windowse modificando il file qm.ini su UNIX and Linux.

Per ulteriori dettagli sulla modifica delle informazioni di configurazione del gestore code, consultare i seguenti argomenti secondari:

Concetti correlati
“Configurazione” a pagina 5
Creare uno o più gestori code su uno o più computer e configurarli sui sistemi di sviluppo, test e produzione per elaborare i messaggi che contengono i dati di business.

“Modifica di IBM WebSphere MQ e delle informazioni di configurazione dei gestori code” a pagina 422
Modificare il comportamento di IBM WebSphere MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione.

Attività correlate
Pianificazione
Amministrazione di WebSphere MQ
Riferimenti correlati
“Attributi per la modifica delle IBM WebSphere MQ informazioni di configurazione” a pagina 429
Su sistemi IBM WebSphere MQ per Windows e su IBM WebSphere MQ per sistemi Linux (piattaformex86 e x86-64), modificare le informazioni di configurazione utilizzando IBM WebSphere MQ Explorer. Su altri sistemi, modificare le informazioni modificando il file di configurazione mqs.ini .

Modalità di accesso

Access Mode si applica solo ai server Windows . La stanza AccessMode viene impostata dall'opzione `-a [r]` sul comando **crtmqm** . Non modificare la stanza AccessMode dopo che il gestore code è stato creato.

Utilizzare il gruppo di accesso (`-a [r]`) opzione del comando **crtmqm** per specificare un gruppo di sicurezza Windows, ai cui membri verrà concesso l'accesso completo a tutti i file di dati del gestore code. Il gruppo può essere un gruppo locale o globale, a seconda della sintassi utilizzata. La sintassi valida per il nome gruppo è la seguente:

LocalGroup
Nome dominio \ *GlobalGroup nome*
Nome GlobalGroup@*Nome dominio*

È necessario definire il gruppo di accesso aggiuntivo prima di eseguire il comando crtmqm con l'opzione `-a [r]` .

Se si specifica il gruppo utilizzando `-ar` invece di `-a`, al gruppo mqm locale non viene concesso l'accesso ai file di dati del gestore code. Utilizzare questa opzione se il file system che ospita i file di dati del gestore code non supporta le voci di controllo accessi per i gruppi definiti localmente.

Il gruppo è in genere un gruppo di sicurezza globale, utilizzato per fornire ai gestori code a più istanze l'accesso a una cartella condivisa con log e dati dei gestori code. Utilizzare il gruppo di accesso di sicurezza aggiuntivo per impostare le autorizzazioni di lettura e scrittura sulla cartella o per condividere i file di log e i dati del gestore code in essa contenuti.

Il gruppo di accesso di sicurezza aggiuntivo è un'alternativa all'utilizzo del gruppo locale denominato `mqm` per impostare le autorizzazioni sulla cartella contenente i log e i dati del gestore code. A differenza del gruppo locale `mqm`, è possibile impostare il gruppo di accesso di sicurezza aggiuntivo come un gruppo locale o globale. Deve essere di tipo globale per impostare le autorizzazioni sulle cartelle condivise che contengono i dati e i file di log utilizzati dai gestori code a più istanze.

Il sistema operativo Windows controlla le autorizzazioni di accesso necessarie per leggere e scrivere i dati e i file di log del gestore code. Controlla le autorizzazioni dell'ID utente che esegue i processi dei gestori code. L'ID utente controllato dipende a seconda che il gestore code sia stato avviato come servizio o in modo interattivo. Se il gestore code è stato avviato come servizio, l'ID utente controllato dal sistema Windows è l'ID utente configurato con la procedura guidata **Prepara** IBM WebSphere MQ . Se si è avviato il gestore code in modo interattivo, l'ID utente controllato dal sistema Windows è l'ID utente che ha eseguito il comando **strmqm**.

L'ID utente deve essere membro del gruppo `mqm` locale per avviare il gestore code. Se l'ID utente è membro del gruppo di accesso di sicurezza aggiuntivo, il gestore code può leggere e scrivere i file per cui vengono fornite le autorizzazioni utilizzando il gruppo.

Limitazione: È possibile specificare un gruppo di accesso di sicurezza aggiuntivo solo sui sistemi operativi Windows. Se si specifica un gruppo di accesso di sicurezza aggiuntivo su altri sistemi operativi, il comando **crtmqm** restituisce un errore.

Concetti correlati

“Proteggere i file e le directory di log e i dati del gestore code non condivisi su Windows” a pagina 379
“Proteggere i dati del gestore code condiviso e le directory di log e i file su Windows” a pagina 376

Attività correlate

“Crea un gestore code a più istanze su server o workstation di dominio” a pagina 352

Riferimenti correlati

crtmqm

Servizi installabili

Modificare i servizi installabili su Windows utilizzando **regedit**e su UNIX and Linux utilizzando la stanza `Service` nel file `qm.ini` .

Nota: Ci sono implicazioni significative per la modifica dei servizi installabili e dei loro componenti. Per questo motivo, i servizi installabili sono di sola lettura in WebSphere MQ Explorer.

Per modificare i servizi installabili su sistemi Windows , utilizzare `regedit`o, su sistemi UNIX and Linux , utilizzare la stanza `Service` nel file qm.ini . Per ogni componente all'interno di un servizio, è necessario anche specificare nome e percorso del modulo contenente il codice per tale componente. Sui sistemi UNIX and Linux , utilizzare la stanza `ServiceComponent` per questo.

Nome =`AuthorizationService`|NameService
Il nome del servizio richiesto.

`AuthorizationService`
Per WebSphere MQ, il componente Authorization Service è noto come OAM (object authority manager).

La stanza `AuthorizationService` e la stanza `ServiceComponent` associata vengono aggiunte automaticamente quando viene creato il gestore code. Aggiungere manualmente altre `ServiceComponent` stanze.

NameService
Per impostazione predefinita, non viene fornito alcun servizio nomi. Se si richiede un servizio nomi, è necessario aggiungere manualmente la stanza `NameService` .

EntryPoints=*numero di voci*
Il numero di punti di entrata definiti per il servizio. Ciò include i punti di ingresso di inizializzazione e terminazione.

SecurityPolicy=`Default`|NTSIDsRequired (solo WebSphere MQ per Windows)
l'attributo SecurityPolicy si applica solo se il servizio specificato è il servizio di autorizzazione predefinito, ossia l'OAM. L'attributo SecurityPolicy consente di specificare la politica di sicurezza per ciascun gestore code. I valori possibili sono:

`Default`
Utilizzare la politica di sicurezza predefinita per rendere effettiva. Se un identificativo di sicurezza Windows (SID NT) non viene passato a OAM per un particolare ID utente, viene effettuato un tentativo di ottenere il SID appropriato ricercando i database di sicurezza pertinenti.

NTSIDsRequired
Passare un SID NT a OAM quando si eseguono i controlli di sicurezza.

Per ulteriori informazioni, consultare SID (security identifier) diWindows .

SharedBindingsUserId=*tipo - utente*
L'attributo SharedBindingsUserId si applica solo se il servizio specificato è il servizio di autorizzazione predefinito, ossia OAM. L'attributo SharedBindingsUserId viene utilizzato solo in relazione ai bind condivisi. Questo valore consente di specificare se il campo *UserIdentifier* nella struttura *IdentityContext* , dalla funzione MQZ_AUTHENTICATE_USER, è l'ID utente effettivo o l'ID utente reale. Per informazioni sulla funzione MQZ_AUTHENTICATE_USER, vedere MQZ_AUTHENTICATE_USER - Authenticate user . I valori possibili sono:

`Default`
Il valore del campo *UserIdentifier* è impostato come ID utente reale.

Reale
Il valore del campo *UserIdentifier* è impostato come ID utente reale.

Effettivo
Il valore del campo *UserIdentifier* è impostato come ID utente effettivo.

FastpathBindingsUserId=*tipo - utente*
L'attributoUserId FastpathBindingssi applica solo se il servizio specificato è il servizio di autorizzazione predefinito, ossia l'OAM. L'attributo FastpathBindingsUserId viene utilizzato solo in relazione ai collegamenti fastpath. Questo valore consente di specificare se il campo *UserIdentifier* nella struttura *IdentityContext* , dalla funzione MQZ_AUTHENTICATE_USER, è l'ID utente effettivo o l'ID utente reale. Per informazioni sulla funzione MQZ_AUTHENTICATE_USER, vedere MQZ_AUTHENTICATE_USER - Authenticate user . I valori possibili sono:

Default
Il valore del campo *UserIdentifier* è impostato come ID utente reale.

Reale
Il valore del campo *UserIdentifier* è impostato come ID utente reale.

Effettivo
Il valore del campo *UserIdentifier* è impostato come ID utente effettivo.

IsolatedBindingsUserId =*tipo - utente*
L'attributo IsolatedBindingsUserId si applica solo se il servizio specificato è il servizio di autorizzazione predefinito, ossia OAM. L'attributo IsolatedBindingsUserId viene utilizzato solo in relazione ai bind isolati. Questo valore consente di specificare se il campo *UserIdentifier* nella struttura *IdentityContext* , dalla funzione MQZ_AUTHENTICATE_USER, è l'ID utente effettivo o l'ID utente reale. Per informazioni sulla funzione MQZ_AUTHENTICATE_USER, vedere MQZ_AUTHENTICATE_USER - Authenticate user . I valori possibili sono:

Default
Il valore del campo *UserIdentifier* è impostato come ID utente effettivo.

Reale
Il valore del campo *UserIdentifier* è impostato come ID utente reale.

Effettivo
Il valore del campo *UserIdentifier* è impostato come ID utente effettivo.

Per ulteriori informazioni sui servizi e i componenti installabili, consultare Servizi e componenti installabili per UNIX, Linux e Windows.

Per ulteriori informazioni sui servizi di sicurezza in generale, consultare Impostazione della sicurezza su sistemi Windows, UNIX and Linux.

Riferimenti correlati
Informazioni di riferimento sui servizi installabili

Componenti del servizio
È necessario specificare le informazioni sul componente del servizio quando viene aggiunto un nuovo servizio installabile. Sui sistemi Windows utilizzare `regedite` sui sistemi UNIX and Linux utilizzare la stanza `ServiceComponent` nel file qm.ini . La stanza del servizio di autorizzazione è presente per impostazione predefinita e il componente associato, OAM, è attivo.

Specificare i componenti del servizio come segue:

Servizio =*nome_servizio*
Il nome del servizio richiesto. Deve corrispondere al valore specificato nell'attributo `Name` delle informazioni di configurazione del servizio.

Nome =*nome_componente*
Il nome descrittivo del componente servizio. Deve essere univoco e contenere solo caratteri validi per i nomi degli oggetti WebSphere MQ (ad esempio, nomi coda). Questo nome si verifica nei messaggi dell'operatore generati dal servizio. Si consiglia che questo nome inizi con un marchio aziendale o una stringa di distinzione simile.

Modulo =*nome_modulo*
Il nome del modulo che deve contenere il codice per questo componente. Questo deve essere un nome percorso completo.

ComponentDataDimensione =*dimensione*
La dimensione, in byte, dell'area dati del componente passata al componente su ciascuna chiamata. Specificare zero se non sono richiesti dati del componente.

Per ulteriori informazioni sui servizi e i componenti installabili, consultare Servizi e componenti installabili per UNIX, Linux e Windows.

Log del gestore code

Utilizzare la pagina delle proprietà del gestore code Log da Esplora risorse di IBM WebSphere MQ o la stanza Log nel file qm.ini per specificare le informazioni relative alla registrazione su un gestore code.

Per impostazione predefinita, queste impostazioni vengono ereditate dalle impostazioni specificate per le impostazioni di log predefinite del gestore code (descritte in "Impostazioni predefinite di log per IBM WebSphere MQ" a pagina 431). Modificare queste impostazioni solo se si desidera configurare questo gestore code in un modo diverso.

Per informazioni sul calcolo delle dimensioni del log, consultare "Calcolo della dimensione del log" a pagina 407.

Nota: I limiti forniti nel seguente elenco di parametri sono impostati da WebSphere MQ. I limiti del sistema operativo potrebbero ridurre la dimensione massima possibile del log.

LogPrimaryFiles =3 |*2-254* (Windows) |*2 - 510* (sistemiUNIX and Linux)
I file di log assegnati quando viene creato il gestore code.

Il numero minimo di file di log primari che è possibile avere è 2 e il massimo è 254 su Windowso 510 su sistemi UNIX and Linux . Il valore predefinito è 3.

Il numero totale di file di log primari e secondari non deve superare 255 su Windowso 511 su sistemi UNIX and Linux e non deve essere inferiore a 3.

Una volta creato o avviato il gestore code, il valore viene configurato automaticamente. È possibile modificarlo una volta creato il gestore code. Tuttavia, una modifica del valore non è effettiva fino a quando il gestore code non viene riavviato e l'effetto potrebbe non essere immediato.

LogSecondaryFiles =2 |*1-253* (Windows) |*1-509* (sistemiUNIX and Linux)
I file di log assegnati quando i file primari sono esauriti.

Il numero minimo di file di log secondari è 1 e il massimo è 253 su Windowso 509 su sistemi UNIX and Linux . Il numero predefinito è 2.

Il numero totale di file di log primari e secondari non deve superare 255 su Windowso 511 su sistemi UNIX and Linux e non deve essere inferiore a 3.

Il valore viene esaminato quando il gestore code viene avviato. È possibile modificare questo valore, ma le modifiche non diventano effettive fino a quando il gestore code non viene riavviato e anche in questo caso l'effetto potrebbe non essere immediato.

LogFilePages =*numero*
I dati di log sono contenuti in una serie di file denominati file di log. La dimensione del file di log è specificata in unità di pagine da 4 KB.

Il numero predefinito di pagine del file di log è 4096, fornendo una dimensione del file di log di 16 MB.

su sistemi UNIX and Linux il numero minimo di pagine del file di log è 64 e su Windows il numero minimo di pagine del file di log è 32; in entrambi i casi il numero massimo è 65 535.

Nota: La dimensione dei file di log specificati durante la creazione del gestore code non può essere modificata per un gestore code.

LogType=CIRCULAR | LINEAR
Il tipo di registrazione che deve essere utilizzato dal gestore code. Non è possibile modificare il tipo di registrazione da utilizzare una volta creato il gestore code. Fare riferimento alla descrizione dell'attributo LogType in "Impostazioni predefinite di log per IBM WebSphere MQ" a pagina 431 per informazioni sulla creazione di un gestore code con il tipo di registrazione richiesto.

CIRCULAR
Avviare il ripristino utilizzando il log per eseguire il rollback delle transazioni che erano in corso quando il sistema è stato arrestato.

Consultare "Tipi di registrazione" a pagina 403 per una spiegazione più completa della registrazione circolare.

LINEARE
Sia per il ripristino del riavvio che per il ripristino del supporto o dell'inoltro (creazione di dati persi o danneggiati riproducendo il contenuto della registrazione).

Consultare “Tipi di registrazione” a pagina 403 per una spiegazione più completa della registrazione lineare.

Pagine LogBuffer=0 |*0-4096*
La quantità di memoria assegnata ai record buffer per la scrittura, specificando la dimensione dei buffer in unità di pagine da 4 KB.

Il numero minimo di pagine di buffer è 18 e il massimo è 4096. Buffer più grandi portano ad una maggiore velocità di trasmissione, specialmente per messaggi più grandi.

Se si specifica 0 (valore predefinito), il gestore code seleziona la dimensione. In WebSphere MQ Versione 7.0 , è 512 (2048 KB).

Se si specifica un numero compreso tra 1 e 17, il valore predefinito del gestore code è 18 (72 KB). Se si specifica un numero compreso tra 18 e 4096, il gestore code utilizza il numero specificato per impostare la memoria assegnata.

Il valore viene esaminato quando il gestore code viene avviato. Il valore può essere aumentato o diminuito entro i limiti indicati. Tuttavia, una modifica del valore non sarà effettiva fino al successivo avvio del gestore code.

LogPath=*nome_directory*
La directory in cui risiedono i file di log per un gestore code. Deve esistere su una periferica locale su cui il gestore code può scrivere e, preferibilmente, su un'unità diversa dalle code messaggi. La specifica di un'unità differente fornisce una protezione aggiuntiva in caso di errore del sistema.

Il valore predefinito è:

- `C:\Program Files\IBM\WebSphere MQ\log` in WebSphere MQ per Windows .
- `/var/mqm/log` in WebSphere MQ per sistemi UNIX and Linux .

È possibile specificare il nome di una directory nel comando `crtmqm` utilizzando l'indicatore -ld. Quando un gestore code viene creato, viene creata anche una directory nella directory del gestore code, utilizzata per conservare i file di log. Il nome di questa directory è basato sul nome gestore code. Ciò garantisce che il percorso del file di log sia univoco e che sia conforme alle eventuali limitazioni sulle lunghezze dei nomi di directory.

Se non si specifica -ld nel comando `crtmqm` , viene utilizzato il valore dell'attributo `LogDefaultPath` .

In WebSphere MQ per sistemi UNIX and Linux , l'ID utente mqm e il gruppo mqm devono avere autorizzazioni complete per i file di log. Se si modificano le ubicazioni di questi file, è necessario fornire personalmente tali autorizzazioni. Ciò non è richiesto se i file di log si trovano nelle ubicazioni predefinite fornite con il prodotto.

LogWriteIntegrity =SingleWrite|DoubleWrite| `TripleWrite`
Il metodo utilizzato dal programma di registrazione per scrivere in modo affidabile i record di log.

`TripleWrite`
È il metodo predefinito.

Nota: è possibile selezionare **DoubleWrite** ma, in tal caso, il sistema l'interpreta come **TripleWrite**.

SingleWrite
Si deve utilizzare **SingleWrite** solo se il file system o il dispositivo che ospita il log di ripristino di WebSphere MQ garantisce esplicitamente l'atomicità di scritture di 4KB.

Ossia, quando una scrittura di una pagina di 4KB non riesce per un qualsiasi motivo, i soli due stati possibili sono la pre-immagine o la post-immagine. Non deve essere possibile alcuno stato intermedio.

Modalità limitata

Questa opzione si applica solo ai sistemi UNIX and Linux . La stanza `RestrictedMode` viene impostata dall'opzione -g sul comando **crtmqm** . Non modificare questa stanza dopo la creazione del gestore code. Se non si utilizza l'opzione -g, la stanza non viene creata nel file qm.ini .

Alcune directory in cui le applicazioni IBM WebSphere MQ creano file mentre sono connesse al gestore code all'interno della directory dei dati del gestore code. Per consentire alle applicazioni di creare i file in queste directory, viene loro concesso l'accesso in scrittura mondiale:

- `/var/mqm/sockets/`*`QMgrName`*`/@ipcc/ssem/`*`hostname`*`/`
- `/var/mqm/sockets/`*`QMgrName`*`/@app/ssem/`*`hostname`*`/`
- `/var/mqm/sockets/`*`QMgrName`*`/zsocketapp/`*`hostname`*`/`

dove *<QMGRNAME>* è il nome del gestore code e *<hostname>* è il nome host.

Su alcuni sistemi, non è possibile concedere a tutti gli utenti l'accesso in scrittura a tali directory. Ad esempio, gli utenti che non hanno bisogno di accedere al gestore code. La modalità limitata modifica le autorizzazioni delle directory che memorizzano i dati del gestore code. Le directory possono essere accedute solo dai membri del gruppo di applicazioni specificato. Anche le autorizzazioni sulla memoria condivisa IPC System V utilizzate per comunicare con il gestore code vengono modificate nello stesso modo.

Il gruppo di applicazioni è il nome del gruppo con i membri che dispongono dell'autorizzazione per eseguire le seguenti operazioni:

- esegui applicazioni MQI
- aggiornare tutte le risorse IPCC
- modificare il contenuto di alcune directory del gestore code

Per utilizzare la modalità limitata per un gestore code:

- Il creatore del gestore code deve essere nel gruppo `mqm` e nel gruppo di applicazioni.
- L'ID utente `mqm` deve essere nel gruppo di applicazioni.
- Tutti gli utenti che desiderano gestire il gestore code devono essere nel gruppo `mqm` e nel gruppo di applicazioni.
- tutti gli utenti che desiderano eseguire applicazioni IBM WebSphere MQ devono trovarsi nel gruppo di applicazioni.

Qualsiasi chiamata MQCONN o MQCONNX emessa da un utente che non fa parte del gruppo di applicazioni non è riuscita con codice motivo MQRC_Q_MGR_NOT_AVAILABLE.

La modalità con restrizioni funziona con il servizio di autorizzazione IBM WebSphere MQ . Pertanto, è necessario concedere agli utenti anche l'autorità di connettersi a IBM WebSphere MQ e accedere alle risorse richieste utilizzando il servizio di autorizzazione IBM WebSphere MQ .

Ulteriori informazioni sulla configurazione del servizio di autorizzazione IBM WebSphere MQ sono disponibili in Impostazione della sicurezza su sistemi Windows, UNIX and Linux.

Utilizzare la modalità limitataIBM WebSphere MQ solo quando il controllo fornito dal servizio di autorizzazione non fornisce un isolamento sufficiente delle risorse del gestore code.

Gestori risorse XA

Utilizzare la pagina delle proprietà del gestore code XA `resource manager` da Esplora risorse di IBM WebSphere MQ o la stanza XA`ResourceManager` nel file qm.ini per specificare le seguenti informazioni sui gestori risorse coinvolti nelle unità di lavoro globali coordinate dal gestore code.

Aggiungere manualmente le informazioni di configurazione del gestore risorse XA per ogni istanza di un gestore risorse che partecipa alle unità di lavoro globali; non vengono forniti valori predefiniti.

Consultare Coordinamento database per ulteriori informazioni sugli attributi del gestore risorse.

Nome =*nome* (obbligatorio)
Questo attributo identifica l'istanza del gestore risorse.

Il valore `Name` può contenere un massimo di 31 caratteri. È possibile utilizzare il nome del gestore risorse come definito nella relativa struttura XA - switch. Tuttavia, se si utilizza più di un'istanza dello stesso gestore risorse, è necessario creare un nome univoco per ciascuna istanza. È possibile garantire l'univocità includendo il nome del database nella stringa `Name` , ad esempio.

WebSphere MQ utilizza il valore `Name` nei messaggi e nell'output del comando `dspmqtrn` .

Non modificare il nome di un'istanza del gestore risorse o eliminare la relativa voce dalle informazioni di configurazione, una volta avviato il gestore code associato e attivato il nome del gestore risorse.

SwitchFile=*nome* (obbligatorio)
Il nome completo del file di caricamento contenente la struttura dello switch XA del gestore risorse.

Se si sta utilizzando un gestore code a 64 bit con applicazioni a 32 bit, il valore `name` deve contenere solo il nome di base del file di caricamento che contiene la struttura dello switch XA del gestore risorse.

Il file a 32 bit verrà caricato nell'applicazione dal percorso specificato da `ExitsDefaultPath`.

Il file a 64 bit verrà caricato nel gestore code dal percorso specificato da `ExitsDefaultPath64`.

XAOpenString=*stringa* (facoltativo)
La stringa di dati da passare al punto di ingresso xa_open del gestore risorse. Il contenuto della stringa dipende dal gestore risorse stesso. Ad esempio, la stringa potrebbe identificare il database a cui deve accedere questa istanza del gestore risorse. Per ulteriori informazioni sulla definizione di questo attributo, consultare:

- Aggiunta di informazioni di configurazione del gestore risorse per DB2
- Aggiunta di informazioni di configurazione del gestore risorse per Oracle
- Aggiunta di informazioni di configurazione del gestore risorse per Sybase
- Aggiunta di informazioni di configurazione del gestore risorse per Informix

e consultare la documentazione del gestore risorse per la stringa appropriata.

XACloseString=*stringa* (facoltativo)
La stringa di dati da trasmettere al punto di ingresso xa_close del gestore risorse. Il contenuto della stringa dipende dal gestore risorse stesso. Per ulteriori informazioni sulla definizione di questo attributo, consultare:

- Aggiunta di informazioni di configurazione del gestore risorse per DB2
- Aggiunta di informazioni di configurazione del gestore risorse per Oracle
- Aggiunta di informazioni di configurazione del gestore risorse per Sybase
- Aggiunta di informazioni di configurazione del gestore risorse per Informix

e consultare la documentazione del database per la stringa appropriata.

ThreadOfControl=THREAD |PROCESS
Questo attributo è obbligatorio per WebSphere MQ per Windows. Il gestore code utilizza questo valore per la serializzazione quando deve richiamare il gestore risorse da uno dei propri processi a più thread.

THREAD
Il gestore risorse è completamente *thread aware*. In un processo WebSphere MQ a più thread, è possibile effettuare chiamate di funzioni XA al gestore risorse esterno da più thread contemporaneamente.

PROCESS
Il gestore risorse non è *thread safe*. In un processo WebSphere MQ a più thread, è possibile effettuare una sola chiamata di funzione XA alla volta al gestore risorse.

La voce ThreadOfControl non si applica alle chiamate alla funzione XA emesse dal gestore code in un processo dell'applicazione a più thread. In generale, un'applicazione che ha unità di lavoro simultanee su thread differenti richiede che questa modalità di operazione sia supportata da ciascuno dei gestori risorse.

Attributi delle stanze dei canali

Questi attributi determinano la configurazione di un canale.

Queste informazioni non sono applicabili a WebSphere MQ per la piattaforma z/OS .

Utilizzare la pagina delle proprietà del gestore code Channels da WebSphere MQ Explorer o la sezione CHANNELS nel file qm.ini per specificare le informazioni sui canali.

MaxChannels=100 |*numero*
Il numero massimo di canali *correnti* consentiti.

Il valore deve essere compreso tra 1 e 65535. Il valore predefinito è 100.

MaxActiveChannels =*MaxChannels_value*
Il numero massimo di canali che possono essere *attivi* in qualsiasi momento. Il valore predefinito è quello specificato per l'attributo MaxChannels.

MaxInitiators=3 |*numero*
Il numero massimo di iniziatori. Il valore predefinito e massimo è 3.

MQIBindType= FASTPATH | STANDARD
Il bind per le applicazioni:

Percorso veloce
I canali si collegano utilizzando MQCONNX FASTPATH; non esiste alcun processo agent.

STANDARD
I canali si collegano utilizzando STANDARD.

PipeLineLunghezza =1 |*numero*
Il numero massimo di thread simultanei che un canale utilizzerà. Il valore predefinito è 1. Qualsiasi valore maggiore di 1 viene considerato come 2.

Quando si utilizza la pipeline, configurare i gestori code ad entrambe le estremità del canale in modo che *PipeLineLength* sia maggiore di 1.

Nota: Il pipelining è efficace solo per i canali TCP/IP.

AdoptNewMCA=NO| SVR | SDR | RCVR | CLUSRCVR | ALL | FASTPATH
Se WebSphere MQ riceve una richiesta di avvio di un canale, ma rileva che un'istanza del canale è già in esecuzione, in alcuni casi l'istanza del canale esistente deve essere arrestata prima che possa essere avviata quella nuova. L'attributo AdoptNewMCA permette di controllare quali tipi di canali possono essere terminati in questo modo.

Se si specifica l'attributo AdoptNewMCA per un particolare tipo di canale, ma il nuovo canale non si avvia perché un'istanza del canale corrispondente è già in esecuzione:

1. Il nuovo canale tenta di arrestare il canale precedente richiedendone l'arresto.
2. Se il server del canale precedente non risponde a questa richiesta entro la scadenza dell'intervallo di attesa MCATimeout AdoptNew, il thread o il processo per il server del canale precedente viene terminato.
3. Se il server del canale precedente non è terminato dopo il passaggio 2 e dopo che l'intervallo di attesa MCATimeout di AdoptNewscade per una seconda volta, WebSphere MQ termina il canale con un errore CHANNEL IN USE .

La funzionalità MCA AdoptNewsi applica ai canali server, mittente, ricevente e ricevente cluster. Nel caso di un canale mittente o server, solo un'istanza di un canale con un determinato nome può essere in esecuzione nel gestore code di ricezione. Nel caso di un canale ricevente o cluster - ricevente, più istanze di un canale con un determinato nome potrebbero essere in esecuzione nel gestore code

ricevente, ma solo un'istanza può essere eseguita contemporaneamente da un particolare gestore code remoto.

Nota: AdoptNewMCA non è supportato sui canali di richiesta o di connessione server.

Specificare uno o più valori, separati da virgole o spazi, dal seguente elenco:

NO
La funzione AdoptNewMCA non è richiesta. Questa è l'opzione predefinita.

SVR
Utilizzare i canali server.

SDR
Utilizzare i canali mittente.

RCVR
Utilizzare i canali riceventi.

CLUSRCVR
Utilizzare i canali riceventi cluster.

TUTTO
Adottare tutti i tipi di canale tranne i canali FASTPATH.

Percorso veloce
Adottare il canale se è un canale FASTPATH. Ciò si verifica solo se viene specificato anche il tipo di canale appropriato, ad esempio: AdoptNewMCA=RCVR,SVR,FASTPATH.

Attenzione!: L'attributo MCA AdoptNewpotrebbe comportarsi in modo imprevedibile con i canali FASTPATH. Prestare particolare attenzione quando si abilita l'attributo MCA AdoptNewper i canali FASTPATH.

AdoptNewMCATimeout=60 | 1-3600
La quantità di tempo, in secondi, per cui la nuova istanza del canale attende la fine della vecchia. Immettere un valore compreso nell'intervallo tra 1 e 3600. Il valore predefinito è 60.

AdoptNewMCACheck = QM | INDIRIZZO | NOME | ALL
Il tipo di controllo richiesto quando si abilita l'attributo AdoptNewMCA . Se possibile, eseguire un controllo completo per proteggere i canali dall'arresto, involontario o doloso. Come minimo, verificare che i nomi dei canali corrispondano.

Specificare uno o più dei seguenti valori, separati da virgole o spazi nel caso di *QM*, *NAME*o *ALL*:

QM
Verificare che i nomi dei gestori code corrispondano.

Si noti che il nome del gestore code stesso corrisponde, non il QMID.

ADDRESS
Controllare l'indirizzo IP di origine delle comunicazioni. Ad esempio, l'indirizzo TCP/IP.

Nota: I valori CONNAME separati da virgole si applicano agli indirizzi di destinazione e, pertanto, non sono rilevanti per questa opzione.

Nel caso in cui un gestore code a più istanze esegua il failover da hosta a hostb, i canali in uscita da tale gestore code utilizzeranno l'indirizzo IP di origine hostb. Se è diverso da hosta, AdoptNewMCACheck=*ADDRESS* non corrisponde.

È possibile utilizzare SSL o TLS con l'autenticazione reciproca per impedire a un aggressore di interrompere un canale in esecuzione esistente. In alternativa, utilizzare una soluzione di tipo HACMP con takeover IP invece di gestori code a più istanze oppure utilizzare un programma di bilanciamento del carico di rete per mascherare l'indirizzo IP di origine.

NOME
Verificare che i nomi dei canali corrispondano.

TUTTO
Controllare i nomi dei gestori code corrispondenti, l'indirizzo di comunicazioni e i nomi dei canali corrispondenti.

Il valore predefinito è `AdoptNewMCACheck=NAME,ADDRESS,QM`.

Concetti correlati

“Stati del canale” a pagina 56
Un canale può essere in uno dei tanti stati in qualsiasi momento. Alcuni stati hanno anche sottostati. Da un determinato stato un canale può spostarsi in altri stati.

TCP, LU62, NETBIOS e SPX

Utilizzare queste pagine delle proprietà del gestore code o le stanze nel file qm.ini per specificare i parametri di configurazione del protocollo di rete. Sovrascrivono gli attributi predefiniti per i canali.

TCP
Utilizzare la pagina delle proprietà del gestore code TCP da Esplora risorse di IBM WebSphere MQ o la sezione TCP nel file qm.ini per specificare i parametri di configurazione TCP/IP (Transmission Control Protocol/Internet Protocol).

Porta =1414|*numero_porta*
Il numero di porta predefinito, in notazione decimale, per le sessioni TCP/IP. Il numero di porta *ben noto* per WebSphere MQ è 1414.

Library1 =*DLLName1* (solo WebSphere MQ per Windows)
Il nome della DLL socket TCP/IP.

Il valore predefinito è WSOCK32.

KeepAlive=NO|SÌ
Attivare o disattivare la funzione KeepAlive . KeepAlive=YES fa sì che TCP/IP controlli periodicamente che l'altra estremità della connessione sia ancora disponibile. In caso contrario, il canale viene chiuso.

ListenerBacklog= numero
Sovrascrivere il numero predefinito di richieste in sospeso per il listener TCP/IP.

Quando si riceve su TCP/IP, viene impostato un numero massimo di richieste di connessione in sospeso. Questo può essere considerato un *backlog* di richieste in attesa sulla porta TCP/IP affinché il listener accetti la richiesta. I valori di backlog del listener predefiniti vengono visualizzati in Tabella 33 a pagina 446.

Tabella 33. Richieste di connessione in sospeso predefinite (TCP)

Piattaforma	**Valore predefinito ListenerBacklog**
Server Windows	100
Workstation Windows	5
Linux	100
Solaris	100
HP-UX	20
AIX V4.2 o successiva	100
AIX V4.1 o precedente	10

Nota: Alcuni sistemi operativi supportano un valore maggiore del valore predefinito visualizzato. Utilizzare questa opzione per evitare di raggiungere il limite di connessione.

Al contrario, alcuni sistemi operativi potrebbero limitare la dimensione del backlog TCP, quindi il backlog TCP effettivo potrebbe essere più piccolo di quanto richiesto qui.

Se il backlog raggiunge i valori mostrati in Tabella 33 a pagina 446, la connessione TCP/IP viene rifiutata e non è possibile avviare il canale. Per i canali di messaggi, ciò fa sì che il canale entri in uno stato RETRY e ritenti la connessione in un secondo momento. Per le connessioni client, il client riceve un codice motivo MQRC_Q_MGR_NOT_AVAILABLE da MQCONN e ritenta la connessione in un momento successivo.

SvrSndBuffSize=32768|numero
La dimensione in byte del buffer di invio TCP/IP utilizzato dall'estremità del server di un canale di connessione server di connessione client.

SvrRcvBuffSize=32768|numero
La dimensione in byte del buffer di ricezione TCP/IP utilizzato dall'estremità server di un canale di connessione server di connessione client.

Connect_Timeout=0|numero
Il numero di secondi prima del timeout di un tentativo di connessione del socket. Il valore predefinito zero specifica che non esiste alcun timeout di connessione.

LU62 (solo WebSphere MQ per Windows)
Utilizzare la pagina delle proprietà del gestore code LU6.2 da IBM WebSphere MQ Explorer o la sezione LU62 nel file qm.ini per specificare i parametri di configurazione del protocollo SNA LU 6.2 .

TPName
Il nome TP da avviare sul sito remoto.

Library1 =*NomeDLL 1*
Il nome della DLL APPC.

Il valore predefinito è WCPIC32.

Libreria2 =*NomeDL2*
Lo stesso di Library1, utilizzato se il codice è memorizzato in due librerie separate.

Il valore predefinito è WCPIC32.

NETBIOS (WebSphere MQ solo per Windows)
Utilizzare la pagina delle proprietà del gestore code Netbios da Esplora risorse di IBM WebSphere MQ o la sezione NETBIOS nel file qm.ini , per specificare i parametri di configurazione del protocollo NetBIOS .

LocalName=*nome*
Il nome con cui questa macchina è nota sulla LAN.

AdapterNum=0|*numero_adattatore*
Il numero dell'adattatore LAN. Il valore predefinito è l'adattatore 0.

NumSess=1|*numero_di_sessioni*
Il numero di sessioni da assegnare. Il valore predefinito è 1.

NumCmds=1|*numero_di_comandi*
Il numero di comandi da assegnare. Il valore predefinito è 1.

NumNames=1|*numero_di_nomi*
Il numero di nomi da assegnare. Il valore predefinito è 1.

Library1 =*NomeDL1*
Il nome della DLL NetBIOS.

Il valore predefinito è NETAPI32.

SPX (WebSphere MQ solo per Windows)
Utilizzare la pagina delle proprietà del gestore code SPX da IBM WebSphere MQ Explorer o la stanza SPX nel file qm.ini per specificare i parametri di configurazione del protocollo SPX.

Socket =5E86|*numero_socket*
Il numero di socket SPX in notazione esadecimale. Il valore predefinito è X'5E86'.

BoardNum=0|*numero_adattatore*
Il numero dell'adattatore LAN. Il valore predefinito è l'adattatore 0.

KeepAlive= NO | SÌ
Attivare o disattivare la funzione KeepAlive .

KeepAlive=YES fa sì che SPX controlli periodicamente che l'altra estremità della connessione sia ancora disponibile. In caso contrario, il canale viene chiuso.

Library1 =*NomeDL1*
Il nome della DLL SPX.

Il valore predefinito è WSOCK32.DLL.

Libreria2 =*NomeDL2*
Lo stesso di LibraryName1, utilizzato se il codice è memorizzato in due librerie separate.

Il valore predefinito è WSOCK32.DLL.

ListenerBacklog= numero
Sovrascrivere il numero predefinito di richieste in sospeso per il listener SPX.

Quando si riceve su SPX, viene impostato un numero massimo di richieste di connessione in sospeso. Questo può essere considerato un *backlog* di richieste in attesa sul socket SPX affinché il listener accetti la richiesta. I valori di backlog del listener predefiniti vengono visualizzati in Tabella 34 a pagina 448.

Tabella 34. Richieste di connessione in sospeso predefinite (SPX)

Piattaforma	**Valore predefinito ListenerBacklog**
Server Windows	100
Workstation Windows	5

Nota: Alcuni sistemi operativi supportano un valore maggiore del valore predefinito visualizzato. Utilizzare questa opzione per evitare di raggiungere il limite di connessione.

Al contrario, alcuni sistemi operativi potrebbero limitare la dimensione del backlog SPX, quindi il backlog SPX effettivo potrebbe essere più piccolo di quanto richiesto qui.

Se il backlog raggiunge i valori riportati in Tabella 34 a pagina 448, la connessione SPX viene rifiutata e il canale non può essere avviato. Per i canali di messaggi, ciò fa sì che il canale entri in uno stato RETRY e ritenti la connessione in un secondo momento. Per le connessioni client, il client riceve un codice motivo MQRC_Q_MGR_NOT_AVAILABLE da MQCONN e deve ritentare la connessione in un secondo momento.

Percorso uscita

Utilizzare la pagina delle proprietà del gestore code `Exits` da Esplora risorse di IBM WebSphere MQ o la stanza `ExitPath` nel file qm.ini per specificare il percorso per i programmi di uscita utente sul sistema del gestore code.

ExitsDefaultPercorso =*stringa*
L'attributo ExitsDefaultPath specifica l'ubicazione di:

- Uscite di canale a 32 bit per i client
- Uscite di canali a 32 bit e uscite di conversione dati per server
- File di caricamento switch XA non qualificati

ExitsDefaultPath64 =*stringa*
L'attributo ExitsDefaultPath64 specifica l'ubicazione di:

- Uscite di canale a 64 bit per client
- Uscite di canali a 64 bit e uscite di conversione dati per server
- File di caricamento switch XA non qualificati

Uscite API

Per un server, utilizzare la pagina delle proprietà del gestore code `Exits` da IBM WebSphere MQ Explorero la stanza `ApiExitLocal` nel file `qm.ini` per identificare le routine di uscita API per un gestore code. Per un client, modificare la sezione `ApiExitLocal` nel file mqclient.ini per identificare le routine di uscita API per un gestore code.

Sui sistemi Windows , è anche possibile utilizzare il comando amqmdain per modificare le voci per le uscite API. (Per identificare le routine di uscita API per tutti i gestori code, utilizzare le stanze `ApiExitCommon` e `ApiExitTemplate` , come descritto in “Uscite API” a pagina 435.)

Si noti che, affinché l'uscita API funzioni correttamente, il messaggio dal server deve essere inviato al client non convertito. Dopo che l'uscita API ha elaborato il messaggio, il messaggio deve essere convertito sul client. Ciò, quindi, richiede che siano state installate tutte le uscite di conversione sul client.

Per una descrizione completa degli attributi per queste stanze, consultare Configurazione delle uscite API.

Stanza QMErrorLog su UNIX, Linux, and Windows

Utilizzare la pagina delle proprietà del gestore code `Extended` da WebSphere MQ Explorer o la stanza `QMErrorLog` nel file qm.ini per adattare l'operazione e il contenuto dei log degli errori del gestore code.

Attenzione: È possibile utilizzare WebSphere MQ Explorer per apportare le modifiche, solo se si utilizza un gestore code locale sulla piattaforma Windows .

ErrorLogDimensione =*maxsize*
Specifica la dimensione del log degli errori del gestore code in cui viene copiato nel backup. *maxsize* deve essere compreso tra 32768 e 2147483648 byte. Se `ErrorLogSize` non è specificato, viene utilizzato il valore predefinito di 2097152 byte (2 MB).

ExcludeMessage=*msgIds*
Specifica i messaggi che non devono essere scritti nel log degli errori del gestore code. Se il sistema WebSphere MQ è fortemente utilizzato, con molti canali in fase di arresto e avvio, un numero elevato di messaggi informativi viene inviato alla console z/OS e al log di copia cartacea. Anche il bridge WebSphere MQ-IMS e il gestore buffer potrebbero produrre un numero elevato di messaggi informativi, pertanto l'esclusione dei messaggi impedisce di ricevere un numero elevato di messaggi, se necessario. *msqIds* contiene un elenco separato da virgole di ID messaggio dai seguenti:

5211 - È stata superata la lunghezza massima del nome proprietà.
5973 - Sottoscrizione di pubblicazione / sottoscrizione distribuita non abilitata
5974 - Pubblicazione di pubblicazione / sottoscrizione distribuita non abilitata
6254 - Il sistema non è stato in grado di caricare dinamicamente la libreria condivisa
7234 - Numero di messaggi caricati
9001 - Programma del canale terminato normalmente
9002 - Programma del canale avviato
9202 - Host remoto non disponibile
9208 - Errore di ricezione dall'host
9209 - Connessione chiusa
9228 - Impossibile avviare il responder del canale
9489 - Limite massimo di istanze SVRCONN superato
9490 - Limite massimo di istanze SVRCONN per client superato
9508 - Impossibile connettersi al gestore code
9524 - Gestore code remoto non disponibile
9528 - Chiusura del canale richiesta dall'utente
9558 - Canale remoto non disponibile
9637 - Al canale manca un certificato
9776 - Il canale è stato bloccato dall'ID utente
9777 - Il canale è stato bloccato dalla mappa NOACCESS
9782 - La connessione è stata bloccata dall'indirizzo
9999 - Programma del canale terminato in modo anomalo

SuppressMessage=*msgIds*
Specifica i messaggi scritti nel log degli errori del gestore code una sola volta in un intervallo di tempo specificato. Se il sistema WebSphere MQ è fortemente utilizzato, con molti canali in fase di arresto e avvio, un numero elevato di messaggi informativi viene inviato alla console z/OS e al log di copia cartacea. WebSphere MQ-IMS bridge and buffer manager potrebbe anche produrre un numero elevato di messaggi informativi, quindi la soppressione dei messaggi impedisce di ricevere un numero di messaggi ripetuti, se necessario. L'intervallo di tempo è specificato da `SuppressInterval`. *msqIds* contiene un elenco separato da virgole di ID messaggio dai seguenti:

5211 - È stata superata la lunghezza massima del nome proprietà.
5973 - Sottoscrizione di pubblicazione / sottoscrizione distribuita non abilitata
5974 - Pubblicazione di pubblicazione / sottoscrizione distribuita non abilitata
6254 - Il sistema non è stato in grado di caricare dinamicamente la libreria condivisa
7234 - Numero di messaggi caricati
9001 - Programma del canale terminato normalmente
9002 - Programma del canale avviato
9202 - Host remoto non disponibile
9208 - Errore di ricezione dall'host
9209 - Connessione chiusa
9228 - Impossibile avviare il responder del canale
9489 - Limite massimo di istanze SVRCONN superato
9490 - Limite massimo di istanze SVRCONN per client superato
9508 - Impossibile connettersi al gestore code
9524 - Gestore code remoto non disponibile
9528 - Chiusura del canale richiesta dall'utente
9558 - Canale remoto non disponibile
9637 - Al canale manca un certificato
9776 - Il canale è stato bloccato dall'ID utente
9777 - Il canale è stato bloccato dalla mappa NOACCESS
9782 - La connessione è stata bloccata dall'indirizzo
9999 - Programma del canale terminato in modo anomalo

Se lo stesso ID messaggio viene specificato sia in `SuppressMessage` che in `ExcludeMessage`, il messaggio viene escluso.

SuppressInterval=*lunghezza*
Specifica l'intervallo di tempo, in secondi, in cui i messaggi specificati in `SuppressMessage` vengono scritti nel log degli errori del gestore code una sola volta. *lunghezza* deve essere compreso tra 1 e 86400 secondi. Se `SuppressInterval` non viene specificato, viene utilizzato il valore predefinito di 30 secondi.

Tipo di bind predefinito del gestore code

Utilizzare la pagina delle proprietà del gestore code `Extended` da Esplora risorse di IBM WebSphere MQ o la sezione `Connection` nel file qm.ini per specificare il tipo di bind predefinito.

DefaultBindTipo =SHARED|ISOLATED
Se il tipo DefaultBindè impostato su ISOLATO, le applicazioni e il gestore code vengono eseguiti in processi separati e non viene condivisa alcuna risorsa.

Se il tipo DefaultBindè impostato su SHARED, le applicazioni e il gestore code vengono eseguiti in processi separati, ma alcune risorse vengono condivise tra loro.

L'impostazione predefinita è shared.

Stanza SSL e TLS del file di configurazione del gestore code

Utilizzare la sezione SSL del file di configurazione del gestore code per configurare i canali SSL o TLS sul gestore code.

OCSP (Certificate Status Protocol Online)

Un certificato può contenere un'estensione AuthorityInfoAccess. Questa estensione specifica un server da contattare tramite OCSP (Online Certificate Status Protocol). Per consentire ai canali SSL o TLS sul gestore code di utilizzare le estensioni di accesso AuthorityInfo, assicurarsi che il server OCSP in essi indicato sia disponibile, configurato correttamente e accessibile sulla rete. Per ulteriori informazioni, consultare Gestione dei certificati revocati.

CDP (CrlDistributionPoint)

Un certificato può contenere un'estensione punto CrlDistribution. Questa estensione contiene un URL che identifica sia il protocollo utilizzato per scaricare un CRL (Certificate Revocation List) sia il server da contattare.

Se vuoi consentire ai canali SSL o TLS sul tuo gestore code di utilizzare le estensioni del punto CrlDistribution, assicurati che il server CDP in essi indicato sia disponibile, configurato correttamente e accessibile sulla rete.

La stanza SSL

Utilizzare la sezione SSL nel file `qm.ini` per configurare il modo in cui i canali SSL o TLS sul gestore code tentano di utilizzare le seguenti funzioni e il modo in cui reagiscono se si verificano dei problemi durante l'utilizzo.

In ciascuno dei seguenti casi, se il valore fornito non è uno dei valori validi elencati, viene utilizzato il valore predefinito. Non viene scritto alcun messaggio di errore che indica che è specificato un valore non valido.

CDPCheckExtensions=YES|NO

CDPCheckExtensions specifica se i canali SSL o TLS su questo gestore code tentano di controllare i server CDP denominati nelle estensioni del certificato CrlDistributionPoint.

- YES: i canali SSL o TLS tentano di controllare i server CDP per determinare se un certificato digitale è revocato.
- NO: i canali SSL o TLS non tentano di verificare i server CDP. Questo è il valore predefinito.

OCSPAuthentication=REQUIRED|WARN|OPTIONAL

OCSPAuthentication specifica l'azione da intraprendere quando uno stato di revoca non può essere determinato da un server OCSP.

Se il controllo OCSP è abilitato, un programma di canale SSL o TLS tenta di contattare un server OCSP.

Se il programma del canale non è in grado di contattare alcun server OCSP, o se nessun server può fornire lo stato di revoca del certificato, viene utilizzato il valore del parametro OCSPAuthentication.

- OBBLIGATORIO: se non si riesce a stabilire lo stato di revoca, la connessione viene chiusa con un errore. Questo è il valore predefinito.
- WARN: se non si determina lo stato di revoca, viene scritto un messaggio di avviso nel log degli errori del gestore code, ma la connessione può continuare.
- FACOLTATIVO: l'errore nel determinare lo stato di revoca consente alla connessione di procedere in modalità non presidiata. Non vengono forniti avvisi o errori.

OCSPCheckExtensions=YES|NO

OCSPCheckExtensions specifica se i canali SSL e TLS su questo gestore code tentano di controllare i server OCSP denominati nelle estensioni certificato di accesso AuthorityInfo.

- YES: i canali SSL e TLS tentano di controllare i server OCSP per determinare se un certificato digitale è revocato. Questo è il valore predefinito.
- NO: i canali SSL e TLS non tentano di controllare i server OCSP.

SSLHTTPProxyName=*stringa*
La stringa è il nome host o l'indirizzo di rete del server proxy HTTP che deve essere utilizzato da GSKit per i controlli OCSP. Questo indirizzo può essere seguito da un numero di porta facoltativo, racchiuso tra parentesi. Se non si specifica alcun numero, viene utilizza la porta HTTP predefinita (80). Sulle piattaforme HP-UX PA - RISC e Sun Solaris SPARC, e per i client a 32 bit su AIX, l'indirizzo di rete può essere solo un indirizzo IPv4 ; su altre piattaforme può essere un indirizzo IPv4 o IPv6 .

Questo attributo potrebbe essere necessario se, ad esempio, un firewall impedisce l'accesso all'URL del responder OCSP.

Proprietà di uscita

Utilizzare la pagina delle proprietà del gestore code del cluster da IBM WebSphere MQ Explorer, o la stanza ExitPropertieslocale nel file qm.ini , per specificare le informazioni sulle proprietà di uscita su un gestore code. In alternativa, è possibile impostarlo utilizzando il comando **amqmdain** .

Per impostazione predefinita, questa impostazione viene ereditata dall'attributo CLWLMode nella stanza ExitProperties della configurazione della macchina (descritta in “Proprietà di uscita” a pagina 431). Modificare questa impostazione solo se si desidera configurare questo gestore code in un modo diverso. Questo valore può essere sovrascritto per i gestori code individuali utilizzando l'attributo della modalità del workload del cluster nella pagina delle proprietà del gestore code del cluster.

CLWLMode=SAFE| FAST
L'uscita del carico di lavoro cluster (CLWL) consente di specificare quale coda cluster nel cluster aprire in seguito a una chiamata MQI (ad esempio, MQOPEN, MQPUT). L'uscita CLWL viene eseguita in modalità FAST o SAFE in base al valore specificato nell'attributo CLWLMode. Se si omette l'attributo CLWLMode, l'uscita del carico di lavoro del cluster viene eseguita in modalità SAFE.

SAFE
Eseguire l'uscita CLWL in un processo separato dal gestore code. Questa è l'opzione predefinita.

Se si verifica un problema con l'uscita CLWL scritta dall'utente durante l'esecuzione in modalità SAFE, si verifica quanto segue:

- Il processo del server CLWL (amqzlwa0) ha esito negativo.
- Il gestore code riavvia il processo server CLWL.
- L'errore viene riportato nel log degli errori. Se è in corso una chiamata MQI, si riceve una notifica sotto forma di codice di ritorno.

L'integrità del gestore code viene preservata.

Nota: L'esecuzione dell'uscita CLWL in un processo separato può influire sulle prestazioni.

VELOCE
Eseguire l'uscita cluster in linea nel processo del gestore code.

Specificando questa opzione si migliorano le prestazioni evitando i costi di commutazione del processo associati all'esecuzione in modalità SAFE, ma a discapito dell'integrità del gestore code. Si consiglia di eseguire l'uscita CLWL in modalità FAST solo se si è certi che **non** vi sono problemi con l'uscita CLWL e si è particolarmente preoccupati per le prestazioni.

Se si verifica un problema quando l'uscita CLWL è in esecuzione in modalità FAST, il gestore code avrà esito negativo e si corre il rischio che l'integrità del gestore code venga compromessa.

Pool secondario

Questa stanza è creata da WebSphere MQ. Non modificarlo.

Il pool secondario della stanza e il nome dell'attributo ShortSubpoolall'interno di tale sezione, vengono scritti automaticamente da WebSphere MQ quando si crea un gestore code. WebSphere MQ sceglie un valore per ShortSubpoolNome. Non modificare questo valore.

Il nome corrisponde a una directory e a un collegamento simbolico creati all'interno della directory /var/mqm/sockets , che WebSphere MQ utilizza per le comunicazioni interne tra i suoi processi in esecuzione.

ConfigurazioneHP Integrity NonStop Server

Utilizzare queste informazioni per configurare il client IBM WebSphere MQ per l'installazione di HP Integrity NonStop Server .

Per i dettagli sulla configurazione di un client utilizzando un file di configurazione, consultare “Configurazione di un client utilizzando un file di configurazione” a pagina 128.

Per dettagli sulla configurazione di un client utilizzando le variabili di ambiente, consultare “Utilizzo delle variabili di ambiente WebSphere MQ” a pagina 146.

Se si sta eseguendo il client IBM WebSphere MQ per le operazioni HP Integrity NonStop Server in TMF/Gateway, consultare gli argomenti secondari per informazioni su come configurare TMF/Gateway. Sono incluse una panoramica del processo Gateway, la sua configurazione per l'esecuzione in Pathway e la configurazione del file di inizializzazione del client per abilitare il client IBM WebSphere MQ per HP Integrity NonStop Server a raggiungere il gateway TMF.

Questa sezione contiene anche IBM WebSphere MQ client per HP Integrity NonStop Server informazioni specifiche sulla concessione di autorizzazioni ai canali.

Panoramica del processo gateway

TMF (Transaction Management Facility) HP NonStop fornisce servizi per consentire la registrazione di un processo gateway come gestore risorse. Il processo TMF/Gateway fornito da IBM WebSphere MQ viene eseguito in Pathway.

IBM WebSphere MQ registra un processo gateway singolo per ogni gestore code coordinato da TMF, pertanto è necessario configurare un TMF/Gateway separato per ciascun gestore code che deve partecipare alle unità di lavoro coordinate TMF. Questa registrazione è in modo che ogni gestore code sia un gestore risorse indipendente e, per scopi amministrativi, la registrazione di ogni gestore code una volta con HP NonStop TMF risulta in un'associazione di facile comprensione.

Per più installazioni di IBM WebSphere MQ, è necessario denominare un singolo processo gateway da una di queste installazioni per ciascun gestore code che deve essere coordinato da TMF.

L'interfaccia per il processo Gateway supporta qualsiasi client alla stessa versione o a una versione precedente.

Per ulteriori informazioni sulla gestione del processo gateway, consultare Amministrazione HP Integrity NonStop Server.

Configurazione del gateway per l'esecuzione in Pathway

TMF/gateway è l'interfaccia tra HP NonStop Transaction Management Facility (TMF) e IBM WebSphere MQ che consente a TMF di essere il coordinatore delle transazioni IBM WebSphere MQ .

Il TMF/Gateway fornito da IBM WebSphere MQ converte le transazioni dal coordinamento TMF nel coordinamento delle transazioni eXtended Architecture (XA) per comunicare con il gestore code remoto.

È necessario disporre di un TMF/Gateway per gestore code che richiede coordinazione e la configurazione del client è richiesta in modo che il client possa connettersi al gateway corretto.

TMF/Gateway può utilizzare tutti i meccanismi disponibili per il client per comunicare con un gestore code. Configurare il TMF/Gateway come si farebbe per le altre applicazioni.

TMF/Gateway non è una coppia di processi HP Integrity NonStop Server ed è progettato per essere eseguito in un ambiente Pathway. TMF/Gateway crea risorse permanenti all'interno di TMF, che riutilizza nelle esecuzioni successive, quindi TMF/Gateway deve essere sempre eseguito con la stessa autorizzazione utente.

Definizione della classe server

TMF/Gateway è ospitato come una classe server all'interno di un ambiente Pathway. Per definire la classe server, è necessario impostare i seguenti attributi del server:

PROCESSTYPE=OSS
Specifica il tipo di server nella classe server. Il processo Gateway è un programma OSS a più thread. Questo attributo è obbligatorio e deve essere impostato su OSS.

MAXSERVERS=1
Specifica il numero massimo di processi server in questa classe server che possono essere eseguiti contemporaneamente. Ci può essere solo un singolo processo Gateway per qualsiasi gestore code. Questo attributo è obbligatorio e deve essere impostato su 1.

NUMSTATIC=1
Specifica il numero massimo di server statici all'interno di questa classe server. Il processo Gateway deve essere eseguito come server statico. Questo attributo è obbligatorio e deve essere impostato su 1.

TMF=ON
Specifica se i server in questa classe server possono bloccare e aggiornare i file di dati controllati dal sottosistema TMF. Il processo Gateway partecipa alle transazioni TMF delle applicazioni client IBM WebSphere MQ pertanto questo attributo deve essere impostato su ON.

PROGRAM=<OSS installation path>/opt/mqm/bin/runmqtmf
Per il client IBM WebSphere MQ per IBM WebSphere MQ, questo attributo deve essere `runmqtmf`. Questo attributo deve essere il nome percorso OSS assoluto. Il caso è significativo.

ARGLIST=-*m < nome QMgr*>[, - c < nome canale>] [, - p < porta>] [, - h < nome host>] [, - n < thread massimi>]
Questi attributi forniscono i parametri al processo Gateway, dove:

- `QMgrName` è il nome del gestore code per questo processo Gateway. Se si sta utilizzando un gruppo di condivisione code (o altra tecnologia di distribuzione di porta), questo parametro deve essere indirizzato a uno specifico gestore code. Questo parametro è obbligatorio.
- `nome canale` è il nome del canale server sul gestore code che deve essere utilizzato dal processo Gateway. Questo parametro è facoltativo.
- `port` è la porta TCP/IP per il gestore code. Questo parametro è facoltativo.
- `nome host` è il nome host per il gestore code. Questo parametro è facoltativo.
- `max threads` è il numero massimo di thread di lavoro creati dal processo Gateway. Questo parametro può essere un valore di 10 o superiore. Il valore più basso utilizzato è 10 anche se viene specificato un valore inferiore a 10. Se non viene fornito alcun valore, il processo Gateway crea fino a un massimo di 50 thread.

Utilizzare `-c`, `-pe` `-h` come metodo alternativo per fornire informazioni di connessione al gateway, in aggiunta a quanto descritto in "Configurazione di TMF/Gateway utilizzando le variabili di ambiente" a pagina 455. Se si specificano uno o più attributi, ma non tutti gli attributi `-c`, `-pe` `-h` , tali attributi non vengono specificati per impostazione predefinita con i seguenti valori:

- Il valore predefinito di `nome canale` è `SYSTEM.DEF.SVRCONN`
- Il valore predefinito di `nome host` è `localhost`
- Il valore predefinito di `port` è `1414`

Se uno dei parametri forniti non è valido, il TMF/Gateway emette il messaggio diagnostico AMQ5379 al log degli errori e termina.

OWNER=ID
L'ID utente con cui viene eseguito il gateway e a cui deve essere concessa l'autorizzazione di connessione al gestore code.

SECURITY="value"
Specifica gli utenti, in relazione all'attributo `Owner` , che possono accedere al Gateway da una applicazione client IBM WebSphere MQ .

LINKDEPTH e MAXLINKS devono essere configurati con valori appropriati per il numero previsto di applicazioni client IBM WebSphere MQ che potrebbero voler comunicare simultaneamente con il gateway. Se questi valori sono impostati su un valore troppo basso, è possibile che venga visualizzato il messaggio di errore AMQ5399 emesso dalle applicazioni client.

Per ulteriori informazioni su questi attributi server, consultare *HP NonStop TS/MP 2.5 System Management Manual*.

Configurazione di TMF/Gateway utilizzando le variabili di ambiente

Uno dei metodi più comunemente utilizzati per la definizione di TMF/Gateway è quello di impostare la variabile di ambiente MQSERVER, ad esempio:

```
ENV MQSERVER=<channel name>/<transport>/<host name>(<listener port>)
```

ENV all'inizio del comando è la notazione Pathway.

Configurazione del file di inizializzazione client

Se si sta utilizzando HP NonStop Transaction Management Facility (TMF), è necessario disporre di un file di inizializzazione client IBM WebSphere MQ per abilitare il proprio client IBM WebSphere MQ affinché HP Integrity NonStop Server raggiunga il gateway TMF.

Un file di inizializzazione client IBM WebSphere MQ per HP Integrity NonStop Server può essere conservato in diverse ubicazioni, per ulteriori informazioni, consultare “Ubicazione del file di configurazione client” a pagina 129.

Per i dettagli del contenuto del file di configurazione, insieme a un esempio, consultare “Configurazione di un client utilizzando un file di configurazione” a pagina 128. Utilizzare la stanza TMF per specificare i dettagli del gestore code e del server TMF; per ulteriori informazioni, consultare “stanze TMF e TMF/Gateway” a pagina 146.

Un esempio delle voci per un IBM WebSphere MQ client per HP Integrity NonStop Server è:

```
TMF:
  PathMon=$PSD1P

TmfGateway:
  QManager=MQ5B
  Server=MQ-MQ5B

TmfGateway:
  QManager=MQ5C
  Server=MQ-MQ5C
```

Per ulteriori informazioni sulla configurazione di un client utilizzando le variabili di ambiente, consultare “Utilizzo delle variabili di ambiente WebSphere MQ” a pagina 146.

Concessione delle autorizzazioni ai canali

La concessione di autorizzazioni ai canali sul client IBM WebSphere MQ per HP Integrity NonStop Server è identica ad altri sistemi operativi, tuttavia è necessario conoscere l'identificazione del proprietario con cui viene eseguito il gateway.

È quindi possibile utilizzare l'identificazione del proprietario del gateway per concedere le autorizzazioni appropriate. La differenza importante è che la concessione delle autorizzazioni ai canali del gestore code non è sotto l'autorizzazione di alcuna applicazione.

Utilizzare il comando **setmqaut** sia per concedere un'autorizzazione, ovvero, fornire a un principal IBM WebSphere MQ o a un gruppo di utenti l'autorizzazione per eseguire un'operazione, sia per revocare un'autorizzazione, ovvero, rimuovere l'autorizzazione per eseguire un'operazione.

Informazioni particolari

Queste informazioni sono state sviluppate per i prodotti ed i 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. È comunque responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri programmi e/o prodotti, fatta eccezione per quelli espressamente indicati dall'IBM.

IBM potrebbe disporre di applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La fornitura di questo documento non concede alcuna licenza a tali brevetti. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

IBM Director of Commercial Relations
IBM Corporation
Guida del Castello del Nord
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
Legge sulla proprietà intellettuale e legale
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.

Queste informazioni potrebbero includere inesattezze 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 in queste informazioni a siti Web nonIBM viene fornito solo per convenienza e non serve in alcun modo da approvazione di tali 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

Rochester, MN 55901
U.S.A.

Tali informazioni possono essere disponibili, in base a termini e condizioni appropriati, incluso, in alcuni casi, il pagamento di una tassa.

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 sulle prestazioni qui contenuti 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 effettuate su sistemi a livello di sviluppo e non vi è alcuna garanzia che tali misurazioni siano le stesse sui sistemi generalmente disponibili. Inoltre, alcune misurazioni possono essere state stimate tramite estrapolazione. I risultati effettivi 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. Le domande sulle capacità dei prodotti nonIBM devono essere indirizzate 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.

Queste informazioni contengono esempi di dati e report utilizzati nelle operazioni aziendali quotidiane. Per illustrarle nel modo più completo possibile, gli esempi includono i nomi di individui, 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 completamente testati in tutte le condizioni. 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 IBM WebSphere MQ.

Queste informazioni, tuttavia, possono contenere diagnosi, modifica e regolazione delle informazioni. Le informazioni di diagnosi, modifica e ottimizzazione vengono fornite per consentire il debug del software dell'applicazione.

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 e/o in altri paesi.

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 (http://www.eclipse.org/).

Java e tutti i marchi e i logo basati su Java sono marchi o marchi registrati di Oracle e / o delle sue consociate.

Numero parte:

(1P) P/N: