9.1

Configurazione di IBM MQ

Nota

Prima di utilizzare queste informazioni e il prodotto che supportano, leggere le informazioni in “Informazioni particolari” a pagina 1013.

Questa edizione si applica alla versione 9 release 1 di IBM® MQ e a tutte le successive release e modifiche se non diversamente indicato nelle nuove edizioni.

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

Indice

Configurazione..... 7
Creazione di gestori code su più piattaforme.....7
Directory effimera configurabile..... 10
Directory dati utente..... 11
Creazione di un gestore code predefinito.....12
Impostazione di un gestore code esistente come predefinito.....13
Backup dei file di configurazione dopo la creazione di un gestore code..... 14
Configurazione delle connessioni tra client e server..... 15
Il tipo di comunicazione da utilizzare..... 15
Configurazione di un client transazionale esteso.....18
Definizione di canali MQI..... 28
Creazione e utilizzo di canali AMQP.....29
Creazione di definizioni di connessione server e di connessione client su piattaforme differenti.... 35
Creazione di definizioni di connessioni server e client sul server.....40
Programmi di uscita canale per canali MQI.....57
Connessione di un client a un gruppo di condivisione code..... 61
Utilizzo delle variabili d'ambiente IBM MQ..... 62
Descrizioni delle variabili di ambiente..... 63
Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms.....83
File di configurazione IBM MQ , mqs.ini..... 84
File di configurazione del gestore code, qm.ini..... 97
File di configurazione dell'installazione, mqinst.ini..... 145
IBM MQ MQI client file di configurazione, mqclient.ini.....146
File di configurazione della traccia di attività, mqat.ini.....173
Configurazione dell'accodamento distribuito.....176
Tecniche di accodamento distribuito IBM MQ..... 177
Introduzione alla gestione delle code distribuite.....197
Monitoraggio e controllo dei canali su UNIX, Linux, and Windows..... 228
Monitoraggio e controllo dei canali su IBM i..... 253
Configurazione di un cluster di gestore code..... 275
Configurazione della messaggistica di pubblicazione/sottoscrizione..... 396
Impostazione degli attributi dei messaggi di pubblicazione / sottoscrizione accodati..... 396
Avvio della pubblicazione / sottoscrizione accodata..... 398
Arresto della pubblicazione / sottoscrizione in coda..... 398
Aggiunta di uno stream..... 399
Eliminazione di uno stream.....400
Aggiunta di un punto di sottoscrizione..... 400
Configurazione delle reti di pubblicazione / sottoscrizione distribuite..... 401
Configurazione di più installazioni.....421
Connessione di applicazioni in un ambiente di installazione multiplo..... 421
Modifica dell'installazione primaria.....430
Associazione di un gestore code a un'installazione..... 432
Ricerca di installazioni di IBM MQ su un sistema.....433
Configurazione dell'alta disponibilità, ripristino e riavvio.....434
Riconnessione automatica del client.....436
Monitoraggio dei messaggi della console.....442
Configurazioni HA (High Availability)..... 446
Registrazione: verifica che i messaggi non vengano persi..... 593
Backup e ripristino dei dati del gestore code IBM MQ.....621
Modifiche al ripristino da errori cluster (su server diversi da z/OS)..... 629
Configurazione delle risorse JMS..... 631
Configurazione di factory di connessione e destinazioni in un namespace JNDI..... 632

Configurazione di oggetti JMS utilizzando IBM MQ Explorer....636
Configurazione di oggetti JMS utilizzando lo strumento di gestione....637
Configurazione di risorse JMS in WebSphere Application Server....646
Configurazione del server delle applicazioni per utilizzare il livello di manutenzione dell'adattatore di risorse più recente....656
Configurazione della proprietà JMS **PROVIDERVERSION**....658
Rimozione di sottoscrizioni durevoli WebSphere Application Server....667
Configurazione di Managed File Transfer....669
Opzioni di configurazione MFT su Multiplatforms....670
MFT opzioni di configurazione su z/OS....671
Configurazione di Redistributable Managed File Transfer Agent....672
Creazione di un dataset del comando Logger o dell'agent MFT....676
Configurazione di Managed File Transfer for z/OS....677
Configurazione di MFT su IBM i....708
Configurazione di MFT per il primo utilizzo....709
Configurazione di un programma di registrazione MFT....719
Configurazione del bridge Connect:Direct....748
Configurazione degli agenti MFT con MSCS....753
Agent ad alta disponibilità in Managed File Transfer....754
Configurazione di IBM MQ Console e REST API....760
Configurazione di base per il server mqweb....760
Configurazione della sicurezza....764
Configurazione del nome host HTTP....764
Configurazione delle porte HTTPS e HTTP....765
Configurazione del timeout di risposta....766
Configurazione dell'avvio automatico....767
Configurazione della registrazione nei log....768
Configurazione del token LTPA....770
Configurazione del gateway administrative REST API....772
Configurazione di messaging REST API....773
Configurazione di REST API per MFT....775
Ottimizzazione della JVM del server mqweb....777
Struttura del file del componente di installazione IBM MQ Console e REST API....779
Configurazione della registrazione dell'utilizzo del server mqweb su z/OS....781
Definizione di una connessione Aspera gateway su Linux....783
Configurazione IBM MQ per l'utilizzo con il IBM Cloud Private servizio di misurazione....786
Configurazione di un gestore code per l'utilizzo con l'istanza del servizio di misurazione su IBM Cloud Private....788
Connessione al servizio di misurazione IBM Cloud Private tramite un proxy HTTP....790
Risoluzione dei problemi di connessione al servizio di misurazione....791
Configurazione di IBM MQ per l'utilizzo con gli argomenti push Salesforce e gli eventi della piattaforma....791
Configurazione di IBM MQ Bridge to Salesforce....793
Opzioni di configurazione aggiuntive per IBM MQ Bridge to Salesforce....798
Creazione di messaggi di eventi per eventi della piattaforma Salesforce....800
Esecuzione di IBM MQ Bridge to Salesforce....806
Configurazione di IBM MQ per l'utilizzo con blockchain....808
Creazione del file di configurazione per IBM MQ Bridge to blockchain....810
File delle credenziali di rete di Hyperledger Fabric di esempio....812
Esecuzione di IBM MQ Bridge to blockchain....814
Opzioni di configurazione aggiuntive per IBM MQ Bridge to blockchain....820
Configurazione dei gestori code su z/OS....821
Preparazione alla personalizzazione dei gestori code su z/OS....822
Configurazione di IBM MQ for z/OS....827
Test di un gestore code su z/OS....892
Impostazione delle comunicazioni con altri gestori code su z/OS....901
Utilizzo di IBM MQ con IMS....932
Utilizzo di IBM MQ con CICS....941

Aggiornamento e applicazione del servizio a Language Environment o z/OS Callable Services..... 941
Utilizzo delle uscite OTMA in IMS..... 943
Utilizzo di IBM z/OSMF per automatizzare IBM MQ..... 948
Configurazione di IBM MQ Advanced for z/OS VUE..... 959
Abilitazione della connettività dell'agente MFT ai gestori code z/OS remoti..... 960
Configurazione di IBM MQ Advanced for z/OS VUE per l'utilizzo con blockchain..... 960
Configurazione di IBM MQ Internet Pass-Thru..... 970
Supporto per HTTP in MQIPT..... 970
Supporto SOCKS in MQIPT..... 972
Supporto SSL/TLS in MQIPT..... 973
Java security manager in MQIPT..... 1002
Uscite di sicurezza in MQIPT..... 1004
Controllo numero porta in MQIPT..... 1008
Crittografia delle password memorizzate in MQIPT..... 1008
Altre considerazioni sulla sicurezza per MQIPT..... 1010
Log di connessione in MQIPT..... 1011
Configurazione di IBM MQ Internet Pass-Thru utilizzando i container..... 1012

Informazioni particolari..... 1013
Informazioni sull'interfaccia di programmazione..... 1014
Marchi..... 1014

Configurazione di IBM MQ

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.

Informazioni su questa attività

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

Esistono diversi metodi che è possibile utilizzare per creare, configurare e amministrare i gestori code e le relative risorse in IBM 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 MQ.

Per istruzioni su come creare, avviare, arrestare ed eliminare un gestore code, consultare “Creazione di gestori code su più piattaforme” a pagina 7.

Per informazioni su come creare i componenti richiesti per collegare le applicazioni e le installazioni IBM MQ , consultare “Configurazione dell'accodamento distribuito” a pagina 176.

Per istruzioni su come collegare i propri client a un server IBM MQ utilizzando metodi diversi, consultare “Configurazione delle connessioni tra client e server” a pagina 15.

Per istruzioni su come configurare un cluster di gestori code, consultare “Configurazione di un cluster di gestore code” a pagina 275.

È possibile modificare il comportamento di IBM MQ o di un gestore code modificando le informazioni di configurazione. Per ulteriori informazioni, consultare “Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms” a pagina 83. 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.

z/OS Per istruzioni su come configurare IBM MQ for z/OS, consultare “Configurazione dei gestori code su z/OS” a pagina 821.

Concetti correlati

IBM MQ - Sommario tecnico

Attività correlate

Amministrazione di oggetti IBM MQ locali

Gestione di oggetti IBM MQ remoti

IBM i Amministrazione di IBMi

z/OS AmministrazioneIBM MQ for z/OS

Pianificazione

z/OS Pianificazione dell'ambiente IBM MQ su z/OS

“Configurazione dei gestori code su z/OS” a pagina 821

Utilizzare queste istruzioni per configurare i gestori code su IBM MQ for z/OS.

Multi Creazione di gestori code su più piattaforme

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

Prima di iniziare

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

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

L'installazione associata al gestore code
Per creare un gestore code, utilizzare il IBM MQ comando di controllo **crtmqm**. 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 . Tenere presente 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 MQ su UNIX, Linux®, and 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 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. Inoltre, se si utilizza la rete per la messaggistica di pubblicazione / sottoscrizione, le sottoscrizioni vengono associate al nome del gestore code che le ha create. Pertanto, se i gestori code nel cluster o nella gerarchia hanno lo stesso nome, è possibile che le pubblicazioni non le raggiungano.

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 nomi di gestori code differenti.

Se si sta utilizzando IBM MQ per la comunicazione con altre aziende, è anche possibile includere il proprio nome aziendale come prefisso. Questo non è mostrato 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 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 di 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, quest'ultimo sostituisce qualsiasi specifica del gestore code predefinito 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 12.

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. Fare riferimento a Visualizzazione e modifica degli attributi del gestore 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 indicare 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 "Configurazione dell'alta disponibilità, ripristino e riavvio" a pagina 434.

UNIX **Solo per sistemi IBM MQ for 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 non riesce con un First Failure Support Technology (FFST) messaggio. Se la directory non è vuota, viene creata una nuova directory.

Informazioni su questa attività

Per creare un gestore code, utilizzare il IBM MQ comando di controllo **crtmqm**. Per ulteriori informazioni, consultare **crtmqm**. Il comando **crtmqm** crea automaticamente gli oggetti predefiniti richiesti e gli oggetti di sistema (consultare 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.

Windows Sui sistemi Windows è possibile avviare più istanze del gestore code utilizzando l'opzione *sax* del comando **crtmqm** .

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

Procedura

- Per informazioni sulla creazione e la gestione dei gestori code, consultare i topic secondari riportati di seguito:
  - “Creazione di un gestore code predefinito” a pagina 12
  - “Impostazione di un gestore code esistente come predefinito” a pagina 13
  - “Backup dei file di configurazione dopo la creazione di un gestore code” a pagina 14

Concetti correlati

Uso dei gestori code

Attività correlate

Creazione di un gestore code denominato QM1

“Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms” a pagina 83
È possibile modificare il comportamento di IBM MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione modificando le informazioni nei file di configurazione (`.ini`). È anche possibile modificare le opzioni di configurazione per IBM MQ MQI clients.

“Configurazione dei gestori code su z/OS” a pagina 821
Utilizzare queste istruzioni per configurare i gestori code su IBM MQ for z/OS.

Riferimenti correlati

Oggetti di sistema e predefiniti

crtmqm

Linux UNIX V 9.1.3 Directory effimera configurabile

IBM MQ 9.1.3 in poi, include il concetto di directory effimera configurabile, che definisce l'ubicazione in cui devono andare i dati effimeri per il gestore code. Questo può essere utilizzato per consentire ai socket del dominio UNIX and Linux di essere posizionati su un filesystem non montato in un ambiente Red Hat® OpenShift® .

Prima di IBM MQ 9.1.3, sulle piattaforme UNIX and Linux , quando un gestore code è in esecuzione, i socket di dominio UNIX and Linux vengono creati nella directory `/var/mqm/sockets` .

Quando si esegue il gestore code in un contenitore, con `/var/mqm` come file system montato, alcune piattaforme Linux possono impedire la creazione di questi socket di dominio, poiché consentono ad alcuni processi esterni al contenitore di interferire con le operazioni all'interno del contenitore.

Questo problema impedisce l'esecuzione di IBM MQ in una piattaforma del contenitore Red Hat OpenShift , nel contesto di sicurezza predefinito.

Da IBM MQ 9.1.3, l'attributo **EphemeralPrefix** può essere utilizzato per configurare l'ubicazione della directory effimera. Se non si utilizza questo attributo, non verrà visualizzato alcun cambiamento nel comportamento.

Quando una voce del gestore code viene creata in `mqs.ini` (utilizzando i comandi **crtmqm** o **addmqinf**), l'attributo **EphemeralPrefix** viene aggiunto se:

- Impostare l'attributo **DefaultEphemeralPrefix** nella stanza AllQueueManagers .
- Impostare la variabile di ambiente MQ_EPHEMERAL_PREFIX.
- Specificare **-v** *EphemeralPrefix* solo per il comando **addmqinf** .

È anche possibile aggiungere esplicitamente l'attributo **EphemeralPrefix** a un gestore code esistente quando viene arrestato e questo viene aggiunto quando il gestore code viene riavviato.

Se si specifica un **EphemeralPrefix**, quando il gestore code viene avviato, i dati effimeri per il gestore code vengono creati con tale prefisso piuttosto che con la normale ubicazione. Cioè:

- I file socket di solito presenti in `/var/mqm/sockets/<QM>` ora si trovano in `/<EphemeralPrefix>/sockets/<QM>`
- I file del pool secondario di solito presenti in `/<Prefix>/qmgrs/<QM>/@<Subpool>` ora si trovano in `/<EphemeralPrefix>/qmgrs/<QM>/@<Subpool>`

Note:

- `/var/mqm/sockets/@SYSTEM` rimane nella sua posizione fissa e non fa parte di **EphemeralPrefix**.
- AMQCLCHL.TAB rimane in `/<Prefix>/qmgrs/<QM>/@ipcc` e non fa parte di **EphemeralPrefix**.

Su piattaforme UNIX and Linux **EphemeralPrefix** è limitato a 12 caratteri.

Se si specifica un **EphemeralPrefix** che è troppo lungo o che non esiste, si riceve il messaggio AMQ7001E: `l'ubicazione specificata per il gestore code non è valida`.

Multi V 9.1.5 Directory dati utente

IBM MQ 9.1.5 in poi ha una directory `userdata` in cui è possibile memorizzare lo stato dell'applicazione persistente.

Ogni gestore code IBM MQ dispone di un filesystem dedicato per il relativo stato persistente, che include sia i dati della coda che il log di recupero. Il file system include una directory `userdata` che è possibile utilizzare per memorizzare le informazioni sullo stato persistente per le applicazioni. Consultare Contenuto della directory su Unix e Linux Systems e Contenuto della directory su sistemi Windows.

La directory `userdata` può essere utile in diverse situazioni, ad esempio:

- Nelle configurazioni RDQM in modo che le informazioni dell'applicazione vengano spostate anche quando un gestore code esegue il failover su un altro nodo (consultare “Archiviazione dello stato dell'applicazione persistente” a pagina 546).
- Per i gestori code a più istanze, in modo che lo stato dell'applicazione sia ubicato con i relativi dati del gestore code sul filesystem di rete condiviso.
- Più in generale, dove le applicazioni sono servizi del gestore code configurati.

Se si sceglie di memorizzare lo stato dell'applicazione nella directory `userdata` , è necessario tenere presente che i dati scritti in questa ubicazione potrebbero consumare lo spazio su disco disponibile assegnato al gestore code. È necessario assicurarsi che sia disponibile spazio su disco sufficiente per il gestore code per scrivere i dati della coda, i log e altre informazioni sullo stato persistente.

La directory `userdata` ha la proprietà utente e gruppo mqm ed è leggibile in modo che gli utenti possano accedervi senza dover far parte del gruppo di amministratori IBM MQ (mqm). Non è possibile modificare le autorizzazioni della directory `userdata` , ma è possibile creare il contenuto in essa con qualsiasi proprietà e autorizzazione richiesti.

Multi 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 MQ comando di controllo **crtmqm**.

Prima di iniziare

Prima di creare un gestore code predefinito, leggere le considerazioni descritte in "Creazione di gestori code su più piattaforme" a pagina 7.

UNIX Quando si utilizza **crtmqm** per creare un gestore code su UNIX, 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 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 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

Gestione delle code locali

Attività correlate

“Backup dei file di configurazione dopo la creazione di un gestore code” a pagina 14
Le informazioni di configurazione IBM MQ sono memorizzate nei file di configurazione su UNIX, Linux, and Windows. 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.

Visualizzazione e modifica degli attributi del gestore code

Riferimenti correlati

Oggetti di sistema e predefiniti

Multi Impostazione di un gestore code esistente come predefinito

È possibile rendere un gestore code esistente il gestore code predefinito manualmente utilizzando un editor di testo oppure, su Windows e Linux, utilizzando IBM MQ Explorer.

Informazioni su questa attività

Per utilizzare un editor di testo per rendere un gestore code esistente il gestore code predefinito, completare la seguente procedura.

Linux Windows Su sistemi Windows e Linux (piattaformex86 e x86-64), se si preferisce utilizzare IBM MQ Explorer per apportare questa modifica, consultare “Utilizzo di IBM MQ Explorer per impostare un gestore code come predefinito” a pagina 14.

Quando si crea un gestore code predefinito, il nome viene inserito nell'attributo `Name` della stanza `DefaultQueueManager` nel file di configurazione IBM 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.

Attività correlate

“Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms” a pagina 83
È possibile modificare il comportamento di IBM MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione modificando le informazioni nei file di configurazione (`.ini`). È anche possibile modificare le opzioni di configurazione per IBM MQ MQI clients.

Linux Windows Utilizzo di IBM MQ Explorer per impostare un gestore code come predefinito

Su sistemi Windows e Linux (x86 e x86-64), è possibile utilizzare IBM MQ Explorer per rendere un gestore code esistente il gestore code predefinito.

Informazioni su questa attività

Per utilizzare IBM MQ Explorer per rendere un gestore code esistente il gestore code predefinito sui sistemi Windows e Linux (piattaformex86 e x86-64), completare la seguente procedura.

Se si preferisce utilizzare un editor di testo per apportare questa modifica manualmente, consultare “Impostazione di un gestore code esistente come predefinito” a pagina 13.

Procedura

1. Aprire IBM MQ Explorer.
2. Fare clic con il tasto destro del mouse su **IBM MQ**, quindi selezionare **Proprietà**. Viene visualizzato il pannello **Proprietà per IBM MQ** .
3. Immettere il nome del gestore code predefinito nel campo **Nome gestore code predefinito** .
4. Fare clic su **OK**.

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

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

Informazioni su questa attività

Come regola generale, eseguire il backup dei file di configurazione ogni volta che si crea un nuovo gestore code.

Esistono due tipi di file di configurazione:

- Quando si installa il prodotto, viene creato il file di configurazione IBM MQ (`mqs.ini`). Contiene un elenco di gestori code che viene aggiornato ogni volta che si crea o si elimina un gestore code. È presente 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.

Se è stato installato il servizio AMQP, è necessario eseguire il backup di un altro file di configurazione:

- Windows Su sistemi Windows : `amqp_win.properties`
- Linux UNIX Su sistemi UNIX e Linux : `amqp_unix.properties`

Attività correlate

“Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms” a pagina 83
È possibile modificare il comportamento di IBM MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione modificando le informazioni nei file di configurazione (`.ini`). È anche possibile modificare le opzioni di configurazione per IBM MQ MQI clients.

“Backup e ripristino dei dati del gestore code IBM MQ” a pagina 621
È possibile proteggere i gestori code da possibili danneggiamenti causati da errori hardware eseguendo il backup dei gestori code e dei dati del gestore code, eseguendo solo il backup della configurazione del gestore code e utilizzando un gestore code di backup.

Configurazione delle connessioni tra client e server

Per configurare i link di comunicazione tra IBM MQ MQI clients e server, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del link, avviare un listener e definire canali.

Informazioni su questa attività

In IBM MQ, i collegamenti di comunicazioni logiche tra oggetti sono denominati *canali*. I canali utilizzati per collegare IBM MQ MQI clients a server sono denominati canali MQI. Si configurano le definizioni di canale a ciascuna estremità del proprio collegamento in modo che l'applicazione IBM MQ sul IBM MQ MQI client possa comunicare con il gestore code sul server.

Prima di definire i canali MQI, è necessario decidere quale forma di comunicazione utilizzare e definire la connessione ad ogni estremità del canale.

Se si sta definendo un canale MQI tra un IBM MQ MQI client e un gestore code che si trovano su reti fisiche differenti o che comunicano tramite firewall, l'utilizzo di IBM MQ Internet Pass-Thru potrebbe semplificare la configurazione. Per ulteriori informazioni, consultare IBM MQ Internet Pass-Thru.

Procedura

1. Decidi il tipo di comunicazione che stai per utilizzare.

   Consultare “Il tipo di comunicazione da utilizzare” a pagina 15.
2. Definire la connessione ad ogni estremità del canale.

   Per definire la connessione, è necessario:

   a) Configurare la connessione.

   b) Registrare i valori dei parametri necessari per le definizioni di canali.

   c) Abilitare il server per rilevare le richieste di rete in entrata da IBM MQ MQI client, avviando un *listener*.

Concetti correlati

“IBM MQ MQI client file di configurazione, mqclient.ini” a pagina 146
I client vengono configurati 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

“Utilizzo delle variabili d'ambiente IBM MQ” a pagina 62
È possibile utilizzare i comandi per visualizzare le impostazioni correnti o per reimpostare i valori delle variabili di ambiente IBM MQ .

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 combinazione di IBM MQ MQI client e delle piattaforme server.

Tipi di protocollo di trasmissione per i canali MQI

A seconda delle piattaforme client e server, ci sono fino a quattro tipi di protocollo di trasmissione per i canali MQI:

- TCP/IP
- LU 6.2

- NetBIOS
- SPX

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 IBM MQ MQI clients, può essere utile disporre di canali MQI alternativi che utilizzano protocolli di trasmissione differenti.

La scelta del protocollo di trasmissione dipende anche dalla particolare combinazione di piattaforme client e server IBM MQ . Le combinazioni possibili sono mostrate nella seguente tabella.

Tabella 1. Protocolli di trasmissione - combinazione di piattaforme server e IBM MQ MQI client

Protocollo di trasmissione	**IBM MQ MQI client**	**IBM MQ server**
TCP/IP "1" a pagina 16	IBM i IBM i UNIX UNIX Windows Windows	IBM i IBM i UNIX UNIX Windows Windows z/OS z/OS
LU 6.2	UNIX UNIX "2" a pagina 16 Windows Windows	IBM i IBM i UNIX UNIX "2" a pagina 16 Windows Windows z/OS z/OS
NetBIOS	Windows Windows	Windows Windows
SPX	Windows Windows	Windows Windows

Note:

1. MQ Adv. CD V 9.1.4 Un canale messaggi che utilizza TCP/IP può essere puntato a IBM Aspera fasp.io Gateway, che utilizza un tunnel TCP/IP veloce, in grado di aumentare notevolmente la velocità di trasmissione della rete. Consultare Definizione di una connessione Aspera gateway su Linux.
2. Tranne Linux (piattaforma POWER)

Concetti correlati

"Definizione di un collegamento TCP su Windows" a pagina 240
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 247
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 TCP su IBM i" a pagina 268
È possibile definire una connessione TCP all'interno della definizione di canale utilizzando il campo Nome connessione.

"Definizione di un collegamento TCP su z/OS" a pagina 923

Per definire una connessione TCP, è necessario configurare diverse impostazioni.

“Definizione di una connessione LU 6.2 su Windows” a pagina 242
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 251
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 IBM i” a pagina 270
Definire i dettagli delle comunicazioni LU 6.2 utilizzando un nome modalità, un nome TP e un nome connessione di una connessione LU 6.2 completa.

“Definizione di una connessione NetBIOS su Windows” a pagina 243
Una connessione NetBIOS si applica solo a un client e a un server su cui è in esecuzione Windows. IBM MQ utilizza tre tipi di risorsa NetBIOS quando stabilisce una connessione NetBIOS a un altro prodotto IBM 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.

Attività correlate

“Definizione di una connessione Aspera gateway su Linux” a pagina 783
IBM Aspera fasp.io Gateway fornisce un tunnel TCP/IP veloce che può aumentare in modo significativo la velocità di trasmissione di rete per IBM MQ. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux.

Riferimenti correlati

“Limiti di connessione TCP/IP” a pagina 17
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 LU6.2 per z/OS utilizzando APPC / MVS” a pagina 926
Per definire una connessione LU6.2 è necessario configurare una serie di impostazioni.

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 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 2. Numero massimo di richieste di connessione in sospeso accodate su una porta TCP/IP

Piattaforma server	**Numero massimo di richieste di connessione**
AIX	100
	20
Linux	100
IBM i	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 MQRC_HOST_NOT_AVAILABLE dalla chiamata MQCONN e un errore AMQ9202 nel log degli errori del client (/var/mqm/errors/AMQERR0n.LOG su sistemi UNIX and Linux o amqerr0n.log nella sottodirectory degli errori dell'installazione del client IBM 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.

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.

Windows **Microsoft Transaction Server (solo sistemiWindows)**
Solo su sistemi Windows , l'interfaccia del gestore risorse XA supporta anche Microsoft Transaction Server (MTS). Il supporto IBM 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 IBM WebSphere MQ supportava WebSphere Application Server 4 o 5 e richiedevano di eseguire alcune attività di configurazione per utilizzare il client transazionale esteso. WebSphere Application Server 6 e versioni successive includono un provider di messaggistica IBM WebSphere MQ o IBM MQ , quindi non è necessario utilizzare il client transazionale esteso.

Configurazione di gestori transazioni compatibili con XA

Per prima cosa, configurare il client di base IBM MQ , quindi configurare la funzione transazionale estesa utilizzando le informazioni 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 prima configurare il client di base IBM MQ come descritto in:

- AIX Installazione di un client di IBM MQ su AIX
- Linux Installazione di un client di IBM MQ su Linux
- Solaris Installazione di un client di IBM MQ su Solaris
- Windows Installazione di un client di IBM MQ su Windows
- IBM i Installazione di un client di IBM MQ su IBM i

Utilizzando le informazioni per la propria piattaforma, è possibile configurare la funzione transazionale estesa per un gestore transazioni compatibile con XA come 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 utilizza un client transazionale esteso; un'applicazione client che utilizza un client di base IBM MQ 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 20.

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 24.

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 26
- “Configurazione di un client transazionale esteso per Tuxedo” a pagina 27

Concetti correlati

“I parametri CHANNEL, TRPTYPE, CONNAME e QMNAME della stringa xa_open” a pagina 22
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 24
La chiamata xa_open ha esito negativo in determinate circostanze.

Attività correlate

“Utilizzo del client transazionale esteso con canali TLS” a pagina 25
Non è possibile impostare un canale TLS 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 23
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 24
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.

z/OS *Considerazioni IBM MQ for z/OS per le connessioni client transazionali estese*

Alcuni gestori transazioni XA utilizzano sequenze di chiamate di coordinamento transazioni incompatibili con le funzioni normalmente disponibili per i client che si collegano a IBM MQ for z/OS.

Se viene rilevata una sequenza non compatibile, IBM MQ for z/OS potrebbe emettere una fine anomala per la connessione e restituire una risposta di errore al client.

Ad esempio, `xa_prepare` riceve l'interruzione 5C6-00D4007D, con codice di ritorno -3 (XAER_RMERR) restituito al client.

Un altro esempio è che `xa_end` riceve l'abend 5C6-00D40079.

Assicurarsi di aver abilitato le modifiche alle connessioni del client XA su IBM MQ for z/OS che consentono al gestore transazioni di preparare una transazione su una connessione differente.

Note:

- La modifica non è abilitata per impostazione predefinita. Per utilizzare la modifica è necessario specificare la parola chiave CSQSERVICE1 (in maiuscolo) in qualsiasi punto del campo di descrizione del canale SVRCONN utilizzato dal client XA.
- I canali con la chiave CSQSERVICE1 hanno le seguenti restrizioni:
  - La disposizione dell'unità di recupero GROUP non è consentita. È consentita solo la disposizione dell'unità di ripristino QMGR . La disposizione è determinata dal nome fornito nella chiamata `xa_open` . Se viene utilizzato il nome del gruppo di condivisione code, la connessione XA richiede un'unità di ripristino del gruppo.

    Una chiamata `xa_open` che specifichi il nome del gruppo di condivisione code nel parametro **`xa_info`** ha esito negativo con *xaer_inval*.
  - Le opzioni *MQGMO_LOCK* e *MQGMO_UNLOCK* non sono consentite. Una chiamata MQGET con *MQGMO_LOCK* o *MQGMO_UNLOCK* ha esito negativo con MQRC_ENVIRONMENT_ERROR.

Concetti correlati

“Configurazione di gestori transazioni compatibili con XA” a pagina 18
Per prima cosa, configurare il client di base IBM MQ , quindi configurare la funzione transazionale estesa utilizzando le informazioni in questi argomenti.

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 protocolli 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 di 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 possibile specificare più host e porte per un gestore code utilizzando un separatore punto e virgola, ad esempio:

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

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 del gruppo di condivisione code, 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** .

z/OS Per ulteriori informazioni sull'utilizzo dell'unità di ripristino GROUP, consultare Disposizione dell'unità di ripristino in un gruppo di condivisione code.

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.

UID
L'ID utente fornito per l'autenticazione al gestore code. Se questo parametro viene fornito, è necessario fornire anche il parametro **PWD** . Se l'ID utente e la password forniti sono autenticati, l'ID utente viene utilizzato per identificare la connessione del gestore transazioni. L'ID utente e la password popolano l'oggetto MQCSP sulla chiamata MQCONNX.

I parametri **UID** e **PWD** sono validi per i collegamenti client e server.

PWD
La password fornita al gestore code per l'autenticazione. Se questo parametro viene fornito, è necessario fornire anche il parametro **UID** .

Avviso: In alcuni casi, la password in una struttura MQCSP per un'applicazione client verrà inviata attraverso una rete in testo semplice. Per assicurarsi che le password dell'applicazione client siano protette in modo appropriato, consultare IBM MQCSP password protection.

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** vengono 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 del 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 l'applicazione si connette a un gestore code con una versione precedente rispetto a IBM WebSphere MQ 7.0.1, la chiamata xa_open ha esito positivo ma la transazione ha un'unità QMGR di disposizione di ripristino. z/OS Accertarsi che le applicazioni che richiedono la disposizione dell'unità di ripristino GROUP si connettano solo a gestori code in IBM WebSphere MQ 7.0.1 o successivi.

z/OS Se l'applicazione utilizza un nome del gruppo di condivisione code nel campo del parametro **QMNAME** e la proprietà GROUPUR è disabilitata sul gestore code a cui si connette, la chiamata xa_open non riesce.

z/OS Se il client delle applicazioni si connette a un gestore code z/OS su IBM WebSphere MQ 7.0.1 o versioni successive, può 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. Per ulteriori informazioni sulla disposizione dell'unità di ripristino GROUP, vedere Disposizione dell'unità di ripristino.

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 verifica che il valore del parametro **QMgrName** nella chiamata MQCONN o MQCONNX sia il nome del gestore code all'estremità 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 del 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 3 a pagina 23 per i valori assunti del parametro AXLIB.

Tabella 3. Valori assunti del parametro AXLIB

Valore di TPM	Piattaforma	Valore assunto di AXLIB
CICS	AIX AIX	/usr/lpp/encina/lib/libEncServer.a(EncServer_shr.o)

Tabella 3. Valori assunti del parametro AXLIB (Continua)		
Valore di TPM	**Piattaforma**	**Valore assunto di AXLIB**
CICS	Solaris Solaris	/opt/encina/lib/libEncServer.so
CICS	Sistemi Windows Windows	libEnc
Tuxedo	AIX AIX	/usr/lpp/tuxedo/lib/libtux.a(libtux.so.60)
Tuxedo	Solaris Solaris	/opt/tuxedo/lib/libtux.so.60
Tuxedo	Sistemi Windows 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.

Pertanto, è necessario assicurarsi che tutte le unità di lavoro incomplete siano state risolte prima di apportare modifiche alle informazioni di configurazione.

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 4 a pagina 25.

Tabella 4. Librerie IBM MQ contenenti le strutture di switch XA

Piattaforma	Libreria contenente le strutture di switch XA
AIX AIX Linux Linux Solaris Solaris	*MQ_INSTALLATION_PATH*/lib/libmqcxa
Sistemi Windows Windows	*MQ_INSTALLATION_PATH*\bin\mqcxa.dll [1]

MQ_INSTALLATION_PATH rappresenta la directory di livello superiore in cui è installato IBM MQ .

Il nome del gestore risorse IBM 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 25
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 TLS
Non è possibile impostare un canale TLS 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 TLS 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 TLS 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 tabella di definizione del canale client (CCDT) 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 TLS necessari per eseguire correttamente l'autenticazione, incluso SSLCIPH, CipherSpec.

Configurazione di un client transazionale esteso per CICS

Configurare 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 RDO (CICS resource definition online), **`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
- Solaris
- 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 5 a pagina 26 per il nome percorso completo di ciascun file di caricamento switch.

Tabella 5. I file di caricamento switch

Piattaforma	File di caricamento switch
AIX Linux Solaris	*MQ_INSTALLATION_PATH*/lib/amqczsc
Windows	*MQ_INSTALLATION_PATH*\bin\mqcc4swi.dll [1]

MQ_INSTALLATION_PATH rappresenta la directory di livello superiore in cui è installato IBM MQ .

Di seguito è riportato un esempio di definizione di risorsa XAD per i sistemi Windows :

```
cicsadd -c xad -r REGION1 WMQXA \
    ResourceDescription="IBM MQ queue manager MARS" \
```

```
    XAOpen="channel=MARS.SVR,trptype=tcp,conname=MARS(1415),qmname=MARS,tpm=cics" \
    SwitchLoadFile="C:\Program Files\IBM\MQ\bin\mqcc4swi.dll"
```

Per ulteriori informazioni sull'aggiunta di una definizione di risorsa XAD a una region CICS , consultare *CICS Administration Reference* e *CICS Administration Guide* per la propria piattaforma.

Tenere presente le seguenti informazioni sull'utilizzo di CICS con un client transazionale esteso:

- Puoi aggiungere solo una definizione di risorsa XAD per IBM MQ a una regione CICS . Ciò significa che solo un gestore code può essere associato a una region e tutte le applicazioni CICS eseguite nella region possono connettersi solo a quel gestore code. Se si desidera eseguire le applicazioni CICS che si connettono a un gestore code differente, è necessario eseguire le applicazioni in una regione diversa.
- 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 le applicazioni IBM MQ MQI client successivamente elaborate dal server delle applicazioni utilizzano lo stesso canale MQI.
- Quando viene avviato un canale MQI e non è presente alcuna uscita di protezione all'estremità client del canale, l'ID utente che passa dal sistema client alla connessione server MCA è `cics` . In determinate circostanze, il gestore code utilizza questo ID utente per i controlli di autorizzazione quando l'MCA di connessione del server tenta successivamente di accedere alle risorse del gestore code per conto di un'applicazione client. Se questo ID utente viene utilizzato per i controlli dell'autorità, è necessario assicurarsi che disponga dell'autorizzazione per accedere a tutte le risorse a cui deve accedere.

  Per informazioni su quando il gestore code utilizza questo ID utente per i controlli di autorizzazione, consultare Protezione.
- Le uscite di fine attività CICS fornite per l'utilizzo su sistemi client IBM MQ sono elencate in Tabella 6 a pagina 27 . Le uscite vengono configurate nello stesso modo in cui vengono configurate le uscite corrispondenti per sistemi server IBM MQ . Per queste informazioni, quindi, consultare Abilitazione delle uscite utente CICS.

Tabella 6. Uscite di terminazione attività CICS

Piattaforma	Sorgente	Libreria
AIX 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 una 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.

  UNIX Sulle piattaforme seguenti, il nome del file è `ubbstxcx.cfg`:

  – AIX
  – Solaris

  Windows Windows, il nome del file è `ubbstxcn.cfg`.

- Nella voce per un gestore code nella tabella del gestore risorse Tuxedo, specificare il nome di una struttura switch XA e il nome percorso completo della libreria che contiene la struttura:
  - UNIX In AIX e Solaris, specificare `udataobj/RM`.
  - Windows In Windows, specificare `udataobj\rm`.

  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.

Windows Server Microsoft Transaction

Non è richiesta alcuna configurazione aggiuntiva prima di poter utilizzare Microsoft Transaction Server (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 dei canali e fornire all'applicazione IBM MQ sulla macchina IBM MQ MQI client l'accesso al canale.

Questi due metodi sono descritti in dettaglio:

1. Creare una definizione di canale sul client IBM MQ e l'altra sul server.

   Ciò si applica a qualsiasi combinazione di piattaforme IBM MQ MQI client e server. 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 35 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 macchine IBM MQ MQI client contemporaneamente.

   Consultare “Creazione di definizioni di connessioni server e client sul server” a pagina 40 per i dettagli su come utilizzare questo metodo.

Canali definiti automaticamente

I prodotti IBM 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 server appropriata su tale gestore code, IBM MQ crea una definizione automaticamente 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).

Concetti correlati

“Funzione di controllo canale” a pagina 206
La funzione di controllo del canale consente di definire, monitorare e controllare i canali.

ULW Creazione e utilizzo di canali AMQP

Quando si installa il supporto IBM MQ per le API MQ Light nell'installazione di IBM MQ , è possibile eseguire i comandi IBM MQ MQSC (**runmqsc**) per definire, modificare, eliminare, avviare e arrestare un canale. È anche possibile visualizzare lo stato di un canale.

Prima di iniziare

Questa attività presuppone che sia installato il canale AMQP. A tal fine, selezionare il componente Servizio AMQP durante l'installazione di IBM MQ. Per ulteriori informazioni, segui il link per la tua piattaforma e trova la riga della tabella per "AMQP Service":

- AIX Componenti IBM MQ per sistemi AIX
- Linux IBM MQ per sistemi Linux
- Linux IBM MQ Debian per sistemi Linux Ubuntu
- Solaris IBM MQ per sistemi Solaris
- Windows Funzioni IBM MQ per sistemi Windows

Per effettuare una connessione di test al gestore code, è necessario disporre di un client MQ Light . Sono disponibili client MQ Light per Node.js, Ruby, Javae Python. Per ulteriori informazioni sui client disponibili, consultare il sito Web della community IBM MQ Light.

Questa attività si basa sul client MQ Light Node.js . Tuttavia, i passaggi relativi al gestore code IBM MQ sono gli stessi per qualsiasi client.

Informazioni su questa attività

La seguente procedura presuppone che si disponga di un gestore code esistente.

Se si richiede un nuovo gestore code, viene incluso uno script di esempio, ubicato nella directory *mqinstall*/amqp/samples . Lo script crea un nuovo gestore code, avvia il servizio AMQP, crea un nuovo canale denominato SAMPLE.AMQP.CHANNELe avvia il canale.

Nota: I canali AMQP non supportano i servizi AMQP definiti dall'utente. I canali AMQP supportano solo il sistema predefinito SYSTEM.AMQP.SERVICE .

Linux Windows Se si esegue lo script di esempio, SampleMQM.sh su Linuxo SampleMQM.bat su Windows, è possibile avviare la seguente procedura da “6” a pagina 31.

È possibile utilizzare il canale predefinito, SYSTEM.DEF.AMQP, per verificare le connessioni MQ Light al gestore code, oppure è possibile creare un nuovo canale.

La seguente procedura utilizza il canale predefinito.

Procedura

1. Avviare **runmqsc** dalla directory *mqinstall*/bin/ :

   ```
   runmqsc QMNAME
   ```

2. V 9.1.0
   (Necessario solo se il gestore code è IBM MQ 9.0.4 o precedente.) Verificare che la funzione AMQP sia installata e che funzioni correttamente.
   Utilizzare il comando **START SERVICE** per avviare il servizio IBM MQ , che controlla la JVM:

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

   Nota: Da IBM MQ 9.1 il SYSTEM.AMQP.SERVICE ha il proprio attributo **CONTROL** impostato su *QMGR*. In questo modo, il servizio viene avviato automaticamente all'avvio del gestore code. Impostando l'attributo **CONTROL** su *MANUAL*, è possibile impedire l'avvio del servizio all'avvio del gestore code.

   All'avvio del gestore code, il servizio AMQP e il canale AMQP, se definiti, vengono avviati automaticamente.

3. Impostare l'ID utente MCAUSER .
   Quando un client AMQP si connette a un canale, il canale specifica un ID utente MCAUSER , che viene utilizzato sulle connessioni al gestore code. Il valore predefinito di MCAUSER è vuoto. Prima che qualsiasi client AMQP possa connettersi al gestore code, è necessario specificare un valore MCAUSER , che deve essere un utente IBM MQ valido autorizzato a pubblicare e sottoscrivere gli argomenti IBM MQ .

   Nota: Windows Su Windows, prima di IBM MQ 9.1.1, l'impostazione ID utente MCAUSER è supportata solo per gli ID utente con una lunghezza massima di 12 caratteri.

   V 9.1.1 Da IBM MQ 9.1.1, il limite di 12 caratteri è stato rimosso.

   a) Utilizzare il comando **ALTER CHANNEL** per impostare l'ID utente MCAUSER :

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

   b) Utilizzare i due comandi **setmqaut** riportati di seguito per autorizzare l'ID utente MCAUSER a pubblicare e sottoscrivere argomenti:

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

e

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

Se il canale è in esecuzione mentre l'ID utente MCAUSER viene aggiunto o modificato, è necessario arrestare e riavviare il canale.

Nota: Se l'ID utente MCAUSER non è impostato oppure se l'ID utente MCAUSER non è autorizzato a pubblicare o sottoscrivere argomenti IBM MQ , si riceverà un messaggio di errore nel client AMQP.

4. Utilizzare il comando **START CHANNEL** per avviare il sistema SYSTEM.DEF.AMQP :

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

5. Se si desidera controllare lo stato del canale, utilizzare il comando **DISPLAY CHSTATUS** :

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

Quando il canale viene eseguito correttamente, STATUS(RUNNING) viene visualizzato nell'output del comando.

6. Modificare la porta predefinita.

La porta predefinita per le connessioni AMQP 1.0 è 5672. Se si sta già utilizzando la porta 5672, che è possibile se è stato precedentemente installato MQ Light, è necessario modificare la porta utilizzata dal canale AMQP. Utilizzare il comando **ALTER CHANNEL** per modificare la porta:

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

7. Se non si desidera bloccare o filtrare le connessioni al canale AMQP utilizzando le regole di autenticazione di canale (CHLAUTH), disabilitare l'autenticazione di canale sul gestore code nel modo seguente:

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

Si consiglia di non disabilitare l'autenticazione della connessione su un gestore code di produzione. È necessario disabilitare solo l'autenticazione della connessione in un ambiente di sviluppo.

In alternativa, configurare le regole di autenticazione del canale del gestore code per consentire connessioni specifiche al canale AMQP.

8. Opzionale: Se si desidera abilitare la codifica SSL/TLS sul canale, utilizzando il repository delle chiavi configurato per il gestore code, è necessario impostare l'attributo SSLCIPH per il canale su una specifica di cifratura appropriata. Per impostazione predefinita, la specifica di cifratura è vuota, il che significa che la codifica SSL/TLS non viene utilizzata nel canale. Utilizzare il comando **ALTER CHANNEL** per impostare una specifica di cifratura. Ad esempio:

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

Inoltre, ci sono una serie di altre opzioni di configurazione del canale associate alla crittografia SSL/TLS che puoi impostare come segue:

- Per impostazione predefinita, il certificato nel repository delle chiavi del gestore code con l'etichetta corrispondente all'attributo **CERTLABL** del gestore code è il nome utilizzato dalla codifica

SSL/TLS per il canale. È possibile selezionare un certificato differente impostando **CERTLABL**. Utilizzare il comando **ALTER CHANNEL** per specificare l'etichetta per il certificato richiesto:

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

- È possibile configurare il canale per richiedere un certificato dalle connessioni client SSL/TLS. È possibile selezionare se un certificato è richiesto da una connessione client SSL/TLS impostando l'attributo **SSLCAUTH** . Utilizzare il comando **ALTER CHANNEL** per impostare se un certificato è richiesto da una connessione client SSL/TLS. Ad esempio:

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

- V 9.1.5 V 9.1.0.5 Se si imposta l'attributo **SSLCAUTH** su REQUIRED, è possibile controllare il DN (Distinguished Name) del certificato dal client. Per controllare il DN del certificato dal client, impostare l'attributo **SSLPEER** . Utilizzare il comando **ALTER CHANNEL** per controllare il DN (Distinguished Name) del certificato dal client. Ad esempio:

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

  In alternativa, è possibile utilizzare i record di autenticazione di canale anche per consentire o bloccare le connessioni perché questo metodo offre una maggiore granularità rispetto all'utilizzo dell'attributo **SSLPEER** . Per ulteriori informazioni sull'impostazione di **SSLPEER** e sull'utilizzo dei record di autenticazione di canale come alternativa, vedi Peer SSL.

9. Installa il client MQ Light Node.js immettendo il seguente comando:

```
npm install mqlight
```

10. Passare alla directory `node_modules/mqlight/samples` ed eseguire l'applicazione del destinatario di esempio:
    - Se si sta utilizzando il numero di porta predefinito, è possibile eseguire l'applicazione del destinatario di esempio:

      ```
      node recv.js
      ```

    - Se il canale AMQP è stato configurato per utilizzare un numero di porta differente, è possibile eseguire l'applicazione del destinatario di esempio con un parametro per specificare il nuovo numero di porta:

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

    Una connessione corretta al canale predefinito visualizza il messaggio seguente:

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

    L'applicazione è ora connessa al gestore code ed è in attesa di ricevere messaggi. È sottoscritto all'argomento `public`.

    Nota: Il `client-id` viene generato automaticamente, a meno che non ne venga specificato uno utilizzando il parametro `-i` .

11. In una nuova finestra di comandi, passare alla directory `node_modules/mqlight/samples` ed eseguire l'applicazione mittente di esempio eseguendo il seguente comando:

```
node send.js
```

Nella finestra comandi per l'applicazione ricevente, viene visualizzato il messaggio `Hello World` .

12. Utilizzare l'esempio **AMQSSUB** IBM MQ per ricevere un MQ Light messaggio di esempio.
    Su Linux e Windows, l'esempio è disponibile nelle seguenti ubicazioni:
    - Linux *mqinstall*`/samp/bin` su Linux.
    - Windows *mqinstall*`/Tools\c\Samples\Bin` su Windows.

    a) Eseguire l'esempio immettendo il seguente comando:

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

    b) Inviare un messaggio all'applicazione IBM MQ eseguendo nuovamente il seguente comando:

    ```
    node send.js
    ```

13. Utilizzare il comando **DEFINE CHANNEL** per creare più canali AMQP:

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

    Quando si definisce un canale, è necessario avviarlo manualmente, utilizzando il comando **START CHANNEL** :

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

    Per controllare che il canale sia in esecuzione correttamente, è possibile eseguire l'applicazione ricevente di esempio, specificando la porta del nuovo canale:

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

Operazioni successive

È possibile utilizzare i comandi riportati di seguito per visualizzare le connessioni IBM MQ , arrestare il canale ed eliminare il canale:

DISPLAY CONN(*) TYPE(*CONN*) WHERE (*CHANNEL EQ SYSTEM.DEF.AMQP*)
Visualizza la connessione IBM MQ effettuata dal canale AMQP sul gestore code.

DISPLAY CHSTATUS(*) CHLTYPE(*AMQP*) CLIENTID(*) ALL
Visualizza un elenco di client AMQP connessi al canale specificato.

STOP CHANNEL (*MY.AMQP.CHANNEL*)
Arresta un canale AMQP e chiude la porta su cui è in ascolto.

DELETE CHANNEL (*MY.AMQP.CHANNEL*)
Elimina tutti i canali creati.

Nota: Non eliminare il canale predefinito SYSTEM.DEF.AMQPAMQP.

È possibile determinare se la funzionalità AMQP è installata nell'installazione di IBM MQ e se ad essa è associato un gestore code, utilizzando **runmqsc** o PCF:

- Utilizzando **runmqsc**, visualizzare gli attributi del gestore code e controllare `AMQPCAP(YES)`.
- Utilizzando PCF, utilizzare il comando **MQCMD_INQUIRE_Q_MGR** e verificare il valore di `MQIA_AMQP_CAPABILITY`.

Attività correlate

Sviluppo di applicazioni client AMQP

Protezione dei client AMQP

Riferimenti correlati
strmqm

ULW Rimozione del canale AMQP dai gestori code

È possibile eliminare il canale AMQP dai gestori code rimuovendo cartelle dalla directory di installazione.

Procedura

1. Chiudere il gestore code.
2. Rimuovere il supporto IBM MQ per le API MQ Light :
   - AIX Su AIX, eseguire il seguente comando:

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

   - Linux Su Linux, rimuovere l'RPM AMQP. Se si è riassemblato l'RPM prima di installarlo, specificare il nome dell'RPM riassemblato.

     ```
     rpm -e MQSeriesAMQP
     ```

   - Windows Su Windows, eliminare la cartella amqp dall'installazione di IBM MQ . Verificare che nessun altro file o cartella nel percorso di installazione di IBM MQ venga rimosso.
3. Riavviare il gestore code.

Attività correlate
Sviluppo di applicazioni client AMQP
Protezione dei client AMQP

ULW File di log del canale AMQP

I file di log per i canali AMQP sono memorizzati nella stessa directory di dati IBM MQ dei file di log IBM MQ .

La directory dei dati predefinita in Windows è `C:\ProgramData\IBM\MQ`.

La directory dei dati predefinita su Linux è `/var/mqm`.

Il canale AMQP scrive le informazioni di log nei seguenti file di log, disponibili nella directory di dati IBM MQ :

- `amqp.stdout`, scritto nella cartella `qmgrs/`*`QM-name`* .
- `amqp.stderr`, scritto nella cartella `qmgrs/`*`QM-name`* .
- `amqp_*.log` , scritto nella cartella `qmgrs/`*`QM-name`*`/errors` .

Se un client MQ Light riceve un errore di autenticazione o di autorizzazione, l'amministratore può trovare informazioni dettagliate sul motivo dell'errore di sicurezza nel file `amqp_0.log` e nei file `MQ AMQERR*.log` .

Tutti i file FDC vengono creati come file `AMQP*.FDC` , scritti nella cartella *`data-directory`*`/errors` .

Alcuni file di configurazione vengono scritti nella directory `qmgrs/`*`QM-name`*`/amqp` . Non è necessario modificare i file in questa directory.

Concetti correlati
Log degli errori su UNIX, Linux, and Windows
Attività correlate
Sviluppo di applicazioni client AMQP
Protezione dei client AMQP

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. Tuttavia, esistono delle limitazioni su come è possibile creare definizioni di canale su un computer client.

Informazioni su questa attività

Su tutte le piattaforme, è possibile utilizzare i comandi IBM MQ Script (MQSC), i comandi PCF (programmable command format) o IBM MQ Explorer per definire un canale di connessione server sulla macchina server.

z/OS Su z/OS è anche possibile utilizzare i pannelli Operazione e Controllo.

IBM i Su IBM i è anche possibile utilizzare l'interfaccia del pannello.

Poiché i comandi MQSC non sono disponibili su una macchina in cui IBM MQ è stato installato solo come IBM MQ MQI client , è necessario utilizzare diversi metodi di definizione di un canale di connessione client sulla macchina client.

Le seguenti considerazioni si applicano quando **runmqsc**:

- È possibile specificare il parametro **-c** e, facoltativamente, il parametro **-u** per connettersi **runmqsc** come client al gestore code che si desidera gestire.
- Se si utilizza il parametro **-u** per specificare un ID utente, viene richiesta una password corrispondente.
- Se il record `CONNAUTH AUTHINFO` è stato configurato con `CHCKLOCL(REQUIRED)` o `CHCKLOCL(REQDADM)`, è necessario utilizzare il parametro **-u** altrimenti non sarà possibile gestire il gestore code con **runmqsc**.

Procedura

- Per definire un canale di connessione server sul server, consultare “Definizione di un canale di connessione server sul server” a pagina 35.
- Per creare un canale di collegamento client su IBM MQ MQI client, consultare “Creazione di un canale di connessione client su IBM MQ MQI client utilizzando MQSERVER” a pagina 36.

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 e 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) oggetto TLS. Per ulteriori informazioni, consultare Record di autenticazione di canale

Creazione di un canale di connessione client su IBM MQ MQI client utilizzando MQSERVER

È possibile definire un canale di connessione client su una workstation client utilizzando la variabile di ambiente **MQSERVER** .

Informazioni su questa attività

È possibile utilizzare la variabile di ambiente **MQSERVER** per specificare una semplice definizione di canale di connessione client. È semplice nel senso che è possibile specificare solo alcuni attributi del canale utilizzando questo metodo.

Se si utilizza la variabile di ambiente **MQSERVER** per definire il canale tra la macchina IBM MQ MQI client e una macchina server, questo è l'unico canale disponibile per l'applicazione e non viene fatto alcun riferimento alla CCDT (client channel definition table).

Se la richiesta MQCONN o MQCONNX specifica un gestore code diverso da quello a cui è connesso il listener o se il **MQSERVER** parametro *TransportType* non viene riconosciuto, la richiesta MQCONN o MQCONNX ha esito negativo con codice di ritorno MQRC_Q_MGR_NAME_ERROR.

Linux UNIX Su UNIX 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 quindi 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 priorità su qualsiasi definizione di canale client indicata dalle variabili di ambiente **MQCHLLIB** e **MQCHLTAB** .

Procedura

- In base alla piattaforma, utilizzare uno dei seguenti comandi per specificare la definizione di canale con **MQSERVER**.

– Windows Su Windows, specificare una definizione di canale semplice come segue:

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

Ad esempio:

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

– Linux UNIX Su UNIX and Linux, specificare una definizione di canale semplice come segue:

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

Ad esempio:

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

– IBM i Su IBM i, specificare una definizione di canale semplice come segue:

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

Ad esempio:

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

Note:

– *ChannelName* deve essere lo stesso nome definito sul server. 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 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.

– Il *TransportType* può essere uno tra LU62, TCP, NETBIOS, SPX, a seconda della piattaforma client IBM MQ .

– Linux UNIX Su UNIX and Linux, *TransportType* è sensibile al maiuscolo / minuscolo e deve essere maiuscolo. Una chiamata MQCONN o MQCONNX restituisce 2058 se il tipo di trasporto non è riconosciuto

– *ConnectionName* è il nome del server come definito nel protocollo di comunicazione (*TransportType*). Deve essere un nome di rete completo, ad esempio AMACHINE.ACOMPANY.COM(1414).

– *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 dei nomi delle connessioni potrebbe essere utilizzato come alternativa ai gruppi di gestori code per specificare più collegamenti per il client da provare. Se si sta configurando un gestore code a più istanze, è possibile utilizzare un elenco di nomi di connessione per specificare diverse istanze del gestore code.

- Per annullare **MQSERVER** e tornare alla tabella di definizione del canale client indicata da **MQCHLLIB** e **MQCHLTAB**, immettere il seguente comando:

– Linux UNIX Su UNIX and Linux:

```
unset MQSERVER
```

– Windows Su Windows:

```
SET MQSERVER=
```

Esempio

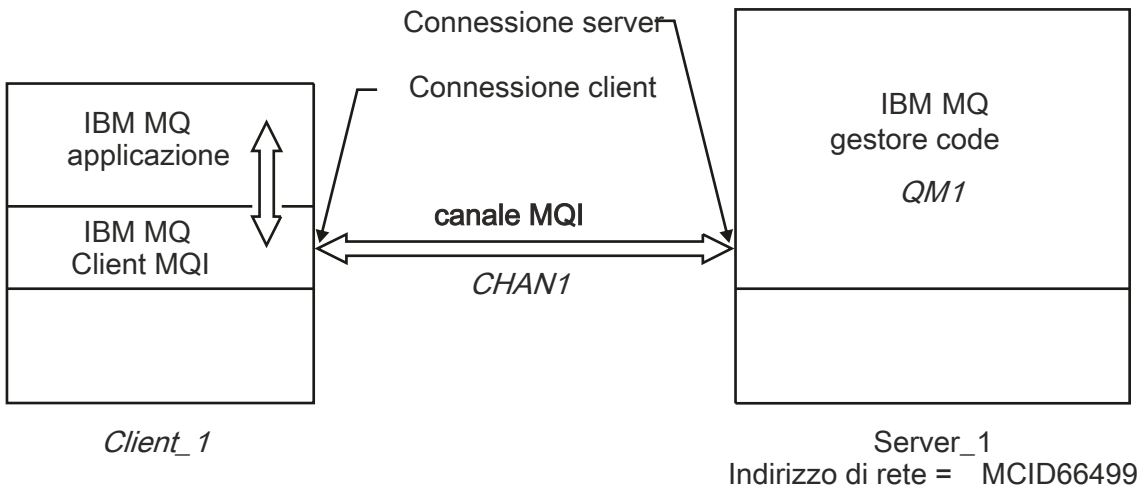


Figura 1. Esempio di una definizione di canale semplice

Per creare la definizione di canale semplice mostrata nella Figura 1 a pagina 38, utilizzare i seguenti comandi:

- Linux UNIX Su UNIX and Linux:

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

- Windows Su Windows:

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

Nota: Per informazioni su come modificare il numero di porta TCP/IP, consultare "Porta predefinita TCP/IP" a pagina 39.

Di seguito sono riportati altri esempi di definizioni di canali semplici:

- Windows Su Windows:

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

- Linux UNIX Su UNIX and Linux:

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

dove B0X99 è la LU 6.2 ConnectionName.

- IBM i Su IBM i:

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

Su IBM MQ MQI client, 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**.

Attività correlate

"Utilizzo delle variabili d'ambiente IBM MQ" a pagina 62
È possibile utilizzare i comandi per visualizzare le impostazioni correnti o per reimpostare i valori delle variabili di ambiente IBM MQ .

"Creazione di un canale di connessione client su IBM MQ MQI client utilizzando MQCNO" a pagina 40
È possibile definire un canale di connessione client sulla stazione di lavoro client utilizzando la struttura MQCNO su una chiamata MQCONNX.

Porta predefinita TCP/IP

Per impostazione predefinita, per TCP/IP, IBM MQ presuppone che il canale sia connesso alla porta 1414.

È possibile modificare questo valore:

- Aggiunta del numero di porta tra parentesi come ultima parte di ConnectionName:
  - Windows Su Windows:

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

  - Linux UNIX Su 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 IBM MQ al file dei servizi come descritto in "Utilizzo del listener TCP/IP su UNIX and Linux" a pagina 249.

Socket predefinito SPX

Per impostazione predefinita, per SPX, IBM MQ presuppone che il canale sia 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 e il server IBM MQ 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
```

Creazione di un canale di connessione client su IBM MQ MQI client utilizzando MQCNO

È possibile definire un canale di connessione client sulla stazione di lavoro client utilizzando la struttura MQCNO su una chiamata MQCONNX.

Informazioni su questa attività

Un'applicazione IBM MQ MQI client 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.

Notare 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 del canale di essere richiamati all'estremità client di un canale MQI.

Se un canale utilizza TLS (Transport Layer Security), un'applicazione client può fornire anche informazioni relative a TLS nella struttura MQCD. Ulteriori informazioni relative a TLS possono essere fornite nella struttura delle opzioni di configurazione 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.

Attività correlate

“Creazione di un canale di connessione client su IBM MQ MQI client utilizzando MQSERVER” a pagina 36
È possibile definire un canale di connessione client su una workstation client utilizzando la variabile di ambiente **MQSERVER** .

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.

Informazioni su questa attività

Definire prima un canale di connessione server e quindi definire un canale di connessione client:

- Su tutte le piattaforme, è possibile utilizzare i comandi IBM MQ Script (MQSC), i comandi PCF (programmable command format) per definire un canale di connessione server sulla macchina server.
- Linux Windows In Linux e Windows, è possibile utilizzare anche IBM MQ Explorer.
- z/OS Su z/OS, è anche possibile utilizzare i pannelli Operazione e Controllo.
- IBM i Su IBM i è anche possibile utilizzare l'interfaccia del pannello.

Le definizioni di canale di connessione client create sul server vengono rese disponibili ai client utilizzando una CCDT (client channel definition table).

Procedura

1. Per definire un canale di connessione server, consultare “Definizione del canale di connessione server sul server” a pagina 54.
2. Per definire un canale di connessione client, consultare “Definizione del canale di connessione client nel server” a pagina 54.

Attività correlate

“Configurazione di un formato binario CCDT” a pagina 42
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 Multiplatforms, una CCDT binaria contenente le impostazioni predefinite viene creata automaticamente quando viene creato il gestore code. Utilizzare il comando **runmqsc** per aggiornare una CCDT binaria.

“Definizione del canale di connessione server sul server” a pagina 54
Creare una definizione di canale di connessione server per il gestore code.

“Definizione del canale di connessione client nel server” a pagina 54
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 55
È possibile rendere la tabella di definizione del canale client (CCDT) disponibile per le applicazioni client copiandola o condividendolo, quindi specificarne l'ubicazione e il nome sul computer client. Da IBM MQ 9.0, IBM MQ fornisce anche la possibilità di individuare una CCDT (client channel definition table) tramite un URL.

Configurazione delle tabelle di definizione del canale client

Una tabella di definizione del canale client (CCDT) definisce i canali di connessione client e i loro attributi. I client leggono questo file per determinare a quali gestori code connettersi. Il file CCDT può essere in formato JSON o binario.

Informazioni su questa attività

Il gestore code non legge il file CCDT. Viene utilizzato solo per fornire definizioni di canale e informazioni di autenticazione ai client.

V 9.1.2 Prima di IBM MQ 9.1.2, CCDT è disponibile solo in formato binario. Da IBM MQ 9.1.2, puoi creare anche una CCDT in formato JSON (JavaScript Object Notation).

Un formato binario CCDT viene creato automaticamente quando viene creato un gestore code. Le definizioni di canale client memorizzate in questa tabella vengono aggiornate utilizzando solo il comando **runmqsc** .

V 9.1.2 Un formato JSON CCDT è un file di testo semplice con estensione .json. Creare e aggiornare manualmente questa tabella, che è meno restrittiva rispetto all'uso del comando **runmqsc** .

z/OS I client z/OS JMS in esecuzione in un server delle applicazioni utilizzano una CCDT per fare riferimento ai dettagli di connessione del gestore code remoto. Da IBM MQ 9.1, IBM MQ Advanced for z/OS Value Unit Edition consente ai client JMS di connettersi in remoto ai gestori code su altre LPAR z/OS . Pertanto questi client possono utilizzare anche i CCDT.

Per facilitare la configurazione dei CCDT per l'utilizzo dei client, scegliere tra le attività riportate di seguito:

Procedura

- “Configurazione di un formato binario CCDT” a pagina 42
- V 9.1.2 “Configurazione di un formato JSON CCDT” a pagina 44

- “Ubicazioni per la CCDT” a pagina 51
- “Accesso URL alla CCDT” a pagina 52

Concetti correlati
Cluster uniformi
Client MQI: CCDT (Client Channel Definition Table)

Configurazione di un formato binario CCDT

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 Multiplatforms, una CCDT binaria contenente le impostazioni predefinite viene creata automaticamente quando viene creato il gestore code. Utilizzare il comando **runmqsc** per aggiornare una CCDT binaria.

Prima di iniziare

V 9.1.2 Da IBM MQ 9.1.2, è possibile anche creare una CCDT in formato JSON (JavaScript Object Notation) e l'uso di questo formato alternativo presenta alcuni vantaggi rispetto all'utilizzo di una CCDT binaria. Consultare “Configurazione di un formato JSON CCDT” a pagina 44.

I client su tutte le piattaforme possono visualizzare e utilizzare i CCDT. Tuttavia, il CCDT binario può essere creato e modificato solo in IBM MQ for Multiplatforms.

Informazioni su questa attività

Multi Su Multipiattaforme:

- Un CCDT binario viene creato automaticamente nella directory `@ipcc` sotto la directory dei dati per il gestore code.
- Oltre ad essere creata automaticamente, la CCDT binaria associata ad un gestore code viene mantenuta sincronizzata con le definizioni oggetto. Quando si definisce, si modifica o si elimina un oggetto del canale client, sia la definizione dell'oggetto del gestore code che la voce in CCDT vengono aggiornate come parte della stessa operazione.

  Note:

  – La progettazione del file IBM MQ CCDT è che il file CCDT viene ridotto, solo dopo che tutti i canali di connessione client definiti dall'utente sono stati effettivamente definiti. Quando un canale di connessione client viene eliminato, viene appena contrassegnato come eliminato nel file CCDT, ma non viene fisicamente rimosso.

  – Per forzare la riduzione del file CCDT, dopo aver eliminato uno o più canali di connessione client, immettere il seguente comando:

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

- Utilizzare il comando **runmqsc** per modificare l'ubicazione e il contenuto della CCDT binaria.

I client su tutte le piattaforme possono visualizzare e utilizzare una CCDT binaria.

Procedura

- Multi
  Creare un CCDT binario predefinito.

  Su Multipiattaforme, viene creata una CCDT binaria predefinita denominata `AMQCLCHL.TAB` quando si crea un gestore code.

  Per impostazione predefinita, AMQCLCHL.TAB si trova nella seguente directory su un server:

– IBM i Su IBM i, nell'IFS:

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

– Linux UNIX 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

dove *MQ_INSTALLATION_PATH* rappresenta la directory di alto livello in cui è installato IBM 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.

- Individuare la CCDT:
  – Sul computer client
  – In una posizione condivisa da più di un cliente
  – Sul server come file condiviso

  Consultare “Ubicazioni per la CCDT” a pagina 51.

  a) Creare un CCDT binario direttamente su una macchina client.
     – Utilizzare il comando runmqsc con il parametro **-n** .
     – La CCDT viene creata nell'ubicazione indicata da **MQCHLLIB**e con il nome file indicato da **MQCHLTAB**, che è AMQCLCHL.TAB per default.
     – **Importante:** se si specifica il parametro **-n** , non è necessario specificare altri parametri.

  b) Modificare l'ubicazione.

     È possibile modificare il percorso della CCDT impostando **MQCHLLIB**. Tenere presente che, se si dispone di più gestori code sullo stesso server, essi condividono la stessa ubicazione CCDT.

- Accedi alla CCDT

  È possibile accedere alla CCDT:

  – In remoto da un file, ftp o URL http, definendo la variabile di ambiente **MQCCDTURL** .
  – Localmente impostando le variabili di ambiente **MQCHLLIB** e **MQCHLTAB** .
  – Localmente definendo gli attributi **ChannelDefinitionDirectory** e **ChannelDefinitionFile** della stanza CHANNELS nel file di configurazione del client.

  Consultare “Ubicazioni per la CCDT” a pagina 51 per vari esempi.

- Visualizzare o modificare il contenuto CCDT.

  È possibile visualizzare il contenuto CCDT con il comando **runmqsc** :

  1. Impostare le variabili di ambiente su Accesso a CCDT
  2. Esegui il comando runmqsc -n
  3. Eseguire il comando DISPLAY CHANNEL (*), ad esempio

  Multi Su Multipiattaforme, è anche possibile modificare il contenuto CCDT binario utilizzando il comando **runmqsc** . 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** . Per ulteriori esempi di utilizzo del comando, consultare **runmqsc** .

- Fornire ai client le informazioni di autenticazione per controllare la revoca del certificato TLS.
  a) Definire un elenco nomi contenente gli oggetti delle informazioni di autenticazione.
  b) Nel CCDT, impostare l'attributo del gestore code **SSLCRLNL** sul nome dell'elenco nomi.

Concetti correlati

Utilizzo dei certificati revocati

Attività correlate

"Configurazione di un formato JSON CCDT" a pagina 44

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. Si utilizza un editor di testo per creare e aggiornare un JSON (JavaScript Object Notation) CCDT.

V 9.1.2 *Configurazione di un formato JSON CCDT*

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. Si utilizza un editor di testo per creare e aggiornare un JSON (JavaScript Object Notation) CCDT.

Prima di iniziare

Multi Se si utilizza IBM MQ for Multiplatforms, è possibile utilizzare invece la CCDT binaria che viene creata automaticamente quando si crea un gestore code. Consultare "Configurazione di un formato binario CCDT" a pagina 42.

Informazioni su questa attività

Il nome file dello schema CCDT per il formato JSON è:

Linux

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

Windows

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

Non esiste alcuna CCDT JSON predefinita e IBM MQ non fornisce strumenti per creare o modificare CCDT in formato JSON. Tuttavia, hai più opzioni di configurazione quando sviluppi manualmente una CCDT JSON rispetto a quando utilizzi il comando **runmqsc** per lavorare con una CCDT binaria:

- Non è necessario utilizzare IBM MQ for Multiplatforms per creare e modificare un file CCDT JSON.
- Utilizzando il formato JSON, è possibile definire definizioni di canale duplicate con lo stesso nome. Quando si distribuisce IBM MQ sul cloud, è possibile utilizzarlo per rendere la distribuzione scalabile e altamente disponibile.
- Il file JSON è leggibile, che può semplificare la configurazione del gestore code.
- Un formato di file flat può essere integrato con:
  - Strumenti di controllo della versione per tenere traccia della cronologia CCDT
  - Strumenti di automazione nella fornitura continua
- Non sono necessari strumenti specifici per gestire il file CCDT.
- Il file è più piccolo.
- Questo formato fornisce compatibilità con le versioni precedenti e successive.

Note:

1. Lo standard JSON vede le chiavi duplicate come valide, tuttavia, il programma di analisi JSON prende solo l'ultimo valore di lettura delle chiavi duplicate durante l'assegnazione degli attributi. Pertanto,

quando si definiscono canali duplicati, ogni canale deve essere un elemento di un valore di array assegnato alla chiave '`channel`'.

2. I CCDT JSON non supportano la memorizzazione delle ubicazioni del server LDAP (Lightweight Directory Access Protocol) per le informazioni sull'ubicazione del responder CRL (Certificate Revocation Lists) e OCSP (Online Certificate Status Protocol).

Tabella 7. Requisiti di codifica per piattaforma

Piattaforma	Codifica client JMS	Codifica client C
ULW Piattaforme UNIX , Linuxe Windows	ASCII	ASCII
z/OS z/OS	ASCII o EBCDIC	Non applicabile

Attenzione: Quando fornisci una definizione per un canale tramite una CCDT JSON (inclusa una *sparse* che non include tutti gli attributi), viene creata una definizione di canale completa con tutti gli attributi definiti, utilizzando i valori predefiniti per tutto ciò che non è specificato nel JSON.

Pertanto, è necessario fornire valori specifici per ogni attributo per cui non si desidera il valore predefinito.

Procedura

- Crea una CCDT JSON
  a) Creare un file flat con estensione `.json` con un editor di testo generico.
  b) Definire una CCDT.

  Consultare "Esempi CCDT JSON" a pagina 48 e "Attributi di canale supportati da JSON CCDT" a pagina 46.
- Individuare la CCDT:
  - Sul computer client
  - In una posizione condivisa da più di un cliente
  - Sul server come file condiviso

  Consultare "Ubicazioni per la CCDT" a pagina 51.
- Convalida una CCDT JSON

  Convalida CCDT rispetto allo schema con un linter JSON.

  Vedi Come convalidare un file IBM MQ CCDT JSON file rispetto allo schema per informazioni su come creare un file CCDT con due canali e convalidarne il funzionamento.

  Lo schema CCDT è incluso con i package del prodotto e del client:

  - UNIX Su sistemi UNIX :

    `$MQ_INSTALLATION_PATH/lib` e `/lib` rispettivamente nei package del prodotto e client.
  - Windows Su Windows:

    `%MQ_INSTALLATION_PATH%\bin` e `\bin` rispettivamente nei package del prodotto e client.

  Note:
  - I linters JSON sono disponibili online.
  - Lo schema definisce gli attributi obbligatori con la chiave '`required`'.
  - Lo schema definisce i tipi di dati attributo con la chiave '`type`'.
- Accedi alla CCDT

  È possibile accedere alla CCDT:

- In remoto da un file, ftp o URL http, definendo la variabile di ambiente **MQCCDTURL** .
- Localmente impostando le variabili di ambiente **MQCHLLIB** e **MQCHLTAB** .
- Localmente definendo gli attributi **ChannelDefinitionDirectory** e **ChannelDefinitionFile** della stanza CHANNELS nel file di configurazione del client.

Consultare "Ubicazioni per la CCDT" a pagina 51 per vari esempi.

- Visualizzare o modificare il contenuto CCDT

  Ogni voce di una CCDT rappresenta una connessione client a un gestore code specifico. È possibile visualizzare o modificare il contenuto CCDT con un editor di testo.

  Se si desidera visualizzare solo la CCDT, è anche possibile eseguire questa operazione utilizzando il comando **runmqsc** come riportato di seguito:

  1. Impostare le variabili di ambiente per fornire l'accesso alla CCDT, come descritto nel passo precedente.
  2. Eseguire il comando `runmqsc -n` . Per ulteriori informazioni, consultare runmqsc.
  3. Eseguire il comando **DISPLAY CHANNEL**. Ad esempio, eseguire `DISPLAY CHANNEL(*)`.

Concetti correlati

Cluster uniformi

Utilizzo dei certificati revocati

Attività correlate

"Configurazione di un formato binario CCDT" a pagina 42

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 Multiplatforms, una CCDT binaria contenente le impostazioni predefinite viene creata automaticamente quando viene creato il gestore code. Utilizzare il comando **runmqsc** per aggiornare una CCDT binaria.

V 9.1.2 *Attributi di canale supportati da JSON CCDT*

Un elenco degli attributi del canale di connessione client supportati dalla CCDT JSON. Questo elenco è un sottoinsieme degli attributi supportati dal CCDT binario.

Associazione attributo

Questi attributi vengono inseriti nel seguente oggetto canale:

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

dove `$CHANNEL_X_KEY_VALUE_LIST` è un elenco separato da virgole degli attributi elencati nella seguente tabella.

Per i casi di utilizzo di base, consultare "Esempi CCDT JSON" a pagina 48 .

Per un elenco completo degli attributi disponibili e dei relativi possibili valori, consultare Attributi del canale in ordine alfabetico.

La seguente tabella riporta l'oggetto JSON, la chiave e il tipo di dati, insieme alla corrispondente definizione di attributo del canale binario.

Attenzione: Gli attributi richiesti sono il canale **name** e il canale **type**. Se si definisce anche **portRange**, sono richiesti anche gli attributi *basso* e *alto* .

Oggetto JSON	Chiave JSON	Tipo di dati JSON	Definizione attributo binario
canale (array)	nome	Stringa	CHANNEL
canale (array)	tipo	Stringa	CHLTYPE

Oggetto JSON	Chiave JSON	Tipo di dati JSON	Definizione attributo binario
channel.clientConnection	queueManager	Stringa	QMNAME
channel.clientConnection.connection (array)	host	Stringa	CONNAME
channel.clientConnection.connection	porta	INT	CONNAME
channel.compression.header (array)	intestazione	Stringa	COMPHDR
channel.compression.message (array)	Messaggio	Stringa	COMPMSG
channel.connectionManagement	affinità	Stringa	AFFINITÀ
channel.connectionManagement	clientWeight	INT	CLNTWGHT
channel.connectionManagement	defaultReconnect	Stringa	DEFRECON
channel.connectionManagement	disconnectInterval	INT	DISCINT
channel.connectionManagement	heartInterval	INT	HBINT
channel.connectionManagement	KeepAliveInterval	INT	KAINT
channel.connectionManagement	sharingConversations	INT	SHARECNV
channel.connectionManagement.localAddress (array)	host	Stringa	LOCLADDR
channel.connectionManagement.localAddress (array)	porta	INT	LOCLADDR
channel.connectionManagement.localAddress.portRange	elevata	INT	LOCLADDR
channel.connectionManagement.localAddress.portRange	bassa	INT	LOCLADDR
channel.exits.receive (array)	nome	Stringa	RCVEXIT
channel.exits.receive (array)	userData	Stringa	RCVDATA
channel.exits.security	nome	Stringa	SCYEXIT
channel.exits.security	userData	Stringa	SCYDATA
channel.exits.send (array)	nome	Stringa	SENDEXIT
channel.exits.send (array)	userData	Stringa	SENDDATA
channel.general	descrizione	Stringa	DESCR
channel.general	maximumMessageLunghezza	INT	MAXMSGL
channel.timestamps	Modificato	Stringa	ALTDATE e ALTTIME
channel.transmissionSecurity	certificateLabel	Stringa	CERTLABL
channel.transmissionSecurity	Nome certificatePeer	Stringa	SSLPEER
channel.transmissionSecurity	cipherSpecification	Stringa	SSLCIPH

Note:

- `channel.connectionManagement.localAddress` può essere definito come una delle seguenti combinazioni di chiavi:
  - Host e porta
  - host e portRange
  - porta
  - portRange
- La chiave JSON `channel.timestamps altered` è facoltativa e, se non è definita, il valore predefinito è l'ora dell'ultima modifica del file CCDT JSON. Tuttavia, se l'ambiente è configurato per recuperare il CCDT da un URL, il valore predefinito è l'ora in cui il file è stato scaricato l'ultima volta.
- `channel.clientConnection.connection` deve includere entrambe le chiavi host e porta.
- La chiave modificata è una singola stringa che incapsula entrambi gli attributi ALTDATE e ALTTIME.
- Il tipo di trasporto può essere solo TCP, quindi i seguenti attributi non sono definiti nello schema:
  - **TRPTYPE**
  - **USERID**
  - **PASSWORD**
  - **MODENAME**
  - **TPNAME**

Riferimenti correlati
Attributi del canale per i tipi di canale

V 9.1.2 *Esempi CCDT JSON*
Utilizzare gli esempi elencati in questo argomento come base per i propri requisiti.

Aprire un editor di testo generico e copiare uno dei seguenti esempi:

- “Definire una connessione client semplice” a pagina 48
- “Definire un canale e un gestore code utilizzando TLS” a pagina 49
- “Definire un canale e un gestore code che non utilizzano TLS” a pagina 49
- “Definire due canali con lo stesso nome” a pagina 49
- “Elenco completo di definizioni di attributi di canale CCDT” a pagina 50

Definire una connessione client semplice

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

Definire un canale e un gestore code utilizzando TLS

```
{
  "channel": [
    {
      "name": "SSL.SVRCONN",
      "clientConnection": {
        "connection": [
          {
            "host": "aztlan1.fyre.ibm.com",
            "port": 1419
          }
        ],
        "queueManager": "QM92TLS"
      },
      "transmissionSecurity":
      {
        "cipherSpecification": "TLS_AES_128_GCM_SHA256",
        "certificateLabel": "ibmwebspheremqadministrator",
      },
      "type": "clientConnection"
    }
  ]
}
```

Definire un canale e un gestore code che non utilizzano TLS

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

Definire due canali con lo stesso nome

Ogni canale si connette a due gestori code distinti:

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

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

Elenco completo di definizioni di attributi di canale CCDT

```
{
  "channel":
  [
    {
      "compression":
      {
        "header": [ "system" ],
        "message": [ "zlibfast" ]
      },
      "connectionManagement":
      {
        "sharingConversations": 10,
        "clientWeight": 1,
        "affinity": "none",
        "defaultReconnect": "yes",
        "disconnectInterval": 6000,
        "heartbeatInterval": 600,
        "keepAliveInterval": -1,
        "localAddress":
        [
          {
            "portRange":
            {
              "low": 2020,
              "high": 3030
            }
          }
        ]
      },
      "exits":
      {
        "receive":
        [
          {
          "name": "",
          "userData": ""
          }
        ],
        "security":
        {
          "name": "",
          "userData": ""
        },
        "send":
        [
           {
             "name": "",
             "userData": ""
           }
        ]
      },
      "general":
      {
        "description": "First channel",
        "maximumMessageLength": 4194304
      },
      "name": "the_channel",
      "clientConnection":
```

```
      {
        "connection":
        [
          {
            "host": "localhost",
            "port": 1414
          }
        ],
        "queueManager": "QM1"
      },
      "timestamps":
      {
        "altered": "2018-12-04T15:37:22.000Z"
      },
      "transmissionSecurity":
      {
        "cipherSpecification": "",
        "certificateLabel": "",
        "certificatePeerName": ""
      },
      "type": "clientConnection"
    }
  ]
}
```

Riferimenti correlati

Attributi del canale per i tipi di canale

Attributi del canale in ordine alfabetico

Ubicazioni per la CCDT

IBM MQ supporta il richiamo di una CCDT da un file, FTP o URL HTTP. È possibile rendere il CCDT accessibile per il client come un file condiviso, mentre rimane sul server. In alternativa è possibile distribuire la CCDT, copiando la CCDT su singoli computer client o copiando la CCDT in una posizione condivisa da più di un client.

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.

Da IBM MQ 9.0, la CCDT può essere ospitata in un'ubicazione centralizzata accessibile tramite un URL, eliminando la necessità di aggiornare singolarmente la CCDT per ogni client distribuito. IBM MQ 9.0 ha aggiunto la capacità per le applicazioni .NET native (C/C + +, COBOL e RPG) e non gestite di estrarre la CCDT da un URL, che si tratti di un file locale, di una risorsa FTP o HTTP.

Il comportamento di memorizzazione nella cache predefinito dei client IBM MQ è che un file CCDT viene estratto solo se l'ora di modifica del file è diversa dall'ultima volta che è stato richiamato. Come con la maggior parte delle opzioni di configurazione del client, ci sono diversi modi in cui è possibile fornire l'ubicazione dell'URL:

- **CCDTUrlPtr** e **CCDTUrlOffset** tramite la struttura MQCNO trasmessa nella chiamata MQI MQCONNX
- **MQCCDTURL** variabile di ambiente
- Attributo **ChannelDefinitionDirectory** nella stanza Channels di `mqclient.ini`

Sono supportati sia URL autenticati che non autenticati. Di seguito sono riportati alcuni esempi:

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

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

Se si desidera utilizzare questo supporto con FTP o HTTP, è ancora necessario ospitare il file CCDT su un server, ma con il supporto aggiunto in IBM MQ 9.0, tutte le applicazioni client possono automaticamente acquisire le modifiche alle definizioni dei canali senza eseguire manualmente il push degli aggiornamenti o la necessità di montare un file system di rete su ciascun client. Per ulteriori informazioni, consultare “Accesso URL alla CCDT” a pagina 52.

Come specificare l'ubicazione della CCDT sul client

Su un sistema client, è possibile specificare l'ubicazione della CCDT nei seguenti 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.
- Fornendo un URL (file, FTP o HTTP) per una CCDT che si trova in una posizione centrale come descritto in precedenza.

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.

Se si utilizza un URL per fornire l'ubicazione della CCDT, l'ordine di precedenza per un'applicazione del client nativo per trovare la definizione del canale client è come descritto in "Accesso URL alla CCDT" a pagina 52.

Accesso URL alla CCDT

È possibile ospitare una CCDT (client channel definition table) in un'ubicazione centrale a cui è possibile accedere tramite un URL, eliminando la necessità di aggiornare singolarmente la CCDT per ciascun client distribuito.

Da IBM MQ 9.0, una tabella di definizione del canale client può essere individuata tramite un URL in uno dei seguenti modi:

- Programmando utilizzando MQCNO
- Utilizzando le variabili di ambiente

  Attenzione: È possibile utilizzare l'opzione della variabile di ambiente solo per i programmi nativi che si collegano come client, ovvero applicazioni C, COBOL o C++. Le variabili di ambiente non hanno effetto per le applicazioni Java, JMS o .NET gestite.

  IBM MQ supporta il richiamo di una CCDT da un file, ftp o URL http.
- Utilizzando la stanza CHANNELS del file `mqclient.ini` .

La variabile di ambiente **MQCCDTURL** consente di fornire un URL di file, ftp o http come un singolo valore da cui è possibile ottenere una tabella di definizione del canale client.

È anche possibile utilizzare il percorso di directory specificato dalla variabile di ambiente **MQCHLLIB** (o il percorso specificato dall'attributo **ChannelDefinitionDirectory** in "Stanza CHANNELS del file di configurazione client" a pagina 160) per individuare un file CCDT, tramite file, ftp o URL http, in aggiunta alla directory del file system locale esistente, ovvero `/var/mqm`). Si noti che un valore **MQCHLLIB** è una radice della directory e funziona in combinazione con **MQCHLTAB** per derivare l'URL completo.

L'autenticazione di base sulle connessioni è supportata tramite le credenziali codificate nell'URL:

Connessioni autenticate

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

Connessioni non autenticate

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

Nota: Se si desidera utilizzare connessioni autenticate, è necessario, come con JMS, fornire il nome utente e la password codificati nell'URL.

L'ordine di precedenza, per un'applicazione client nativa, per trovare una definizione di canale client è ora:

1. MQCD fornito da **ClientConnOffset** e **ClientConnPtr** in MQCNO.
2. URL fornito da **CCDTUrlOffset** e **CCDTUrlPtr** in MQCNO.
3. Variabile di ambiente MQSERVER .
4. Se un file `mqclient.ini` è definito e contiene un parametro ServerConnection, viene utilizzato il canale definito. Per ulteriori informazioni, consultare “IBM MQ MQI client file di configurazione, mqclient.ini” a pagina 146 e “Stanza CHANNELS del file di configurazione client” a pagina 160.
5. **MQCCDTURL** variabile di ambiente.
6. **MQCHLLIB** e **MQCHLTAB** variabile di ambiente.
7. **ChannelDefinitionDirectory** e **ChannelDefinitionFile** in “Stanza CHANNELS del file di configurazione client” a pagina 160.

Importante: L'accesso a un file CCDT mediante un URL apre sempre una copia di sola lettura del file, anche quando viene utilizzato il protocollo `file://` .

Il tentativo di aprire un file CCDT per l'accesso in scrittura, ad esempio quando si utilizza il comando **runmqsc** DEFINE CHANNEL da un client, restituisce un errore che indica che non è stato possibile aprire il file per l'accesso in scrittura.

Tuttavia, è possibile leggere le definizioni delle informazioni di autenticazione e del canale utilizzando **runmqsc**.

Attività correlate

“Accesso alle definizioni del canale di connessione client” a pagina 55
È possibile rendere la tabella di definizione del canale client (CCDT) disponibile per le applicazioni client copiandola o condividendolo, quindi specificarne l'ubicazione e il nome sul computer client. Da IBM MQ 9.0, IBM MQ fornisce anche la possibilità di individuare una CCDT (client channel definition table) tramite un URL.

“Configurazione di un formato binario CCDT” a pagina 42
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 Multiplatforms, una CCDT binaria contenente le impostazioni predefinite viene creata automaticamente quando viene creato il gestore code. Utilizzare il comando **runmqsc** per aggiornare una CCDT binaria.

Utilizzo di CCDT con IBM MQ classes for JMS

Riferimenti correlati

CCDTURL
MQCNO - Opzioni di connessione
URL CCDT WMQ_XMSC

Windows Canali di connessione client in Active Directory

Sui sistemi Windows che supportano Active Directory, IBM MQ pubblica i canali di connessione client in Active Directory per fornire il binding 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 MQ li pubblica anche in Active Directory. Quando il client IBM 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 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) oggetto TLS. Per ulteriori informazioni, consultare Record di autenticazione di canale

   Questa definizione di canale è associata al gestore code in esecuzione sul server.

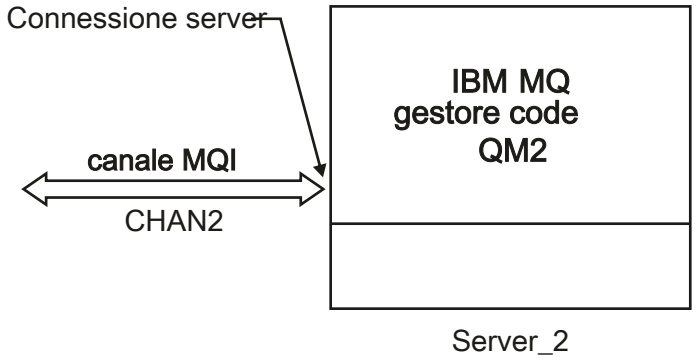


Figura 2. Definizione del canale di connessione server

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 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) oggetto TLS. Per ulteriori informazioni, consultare Record di autenticazione di canale

Risultati

Multi Su Multipiattaforme, questa definizione di canale viene 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 definizione del canale client e per le informazioni corrispondenti su come le definizioni del canale di connessione client sono memorizzate su z/OS, consultare “Configurazione di un formato binario CCDT” a pagina 42.

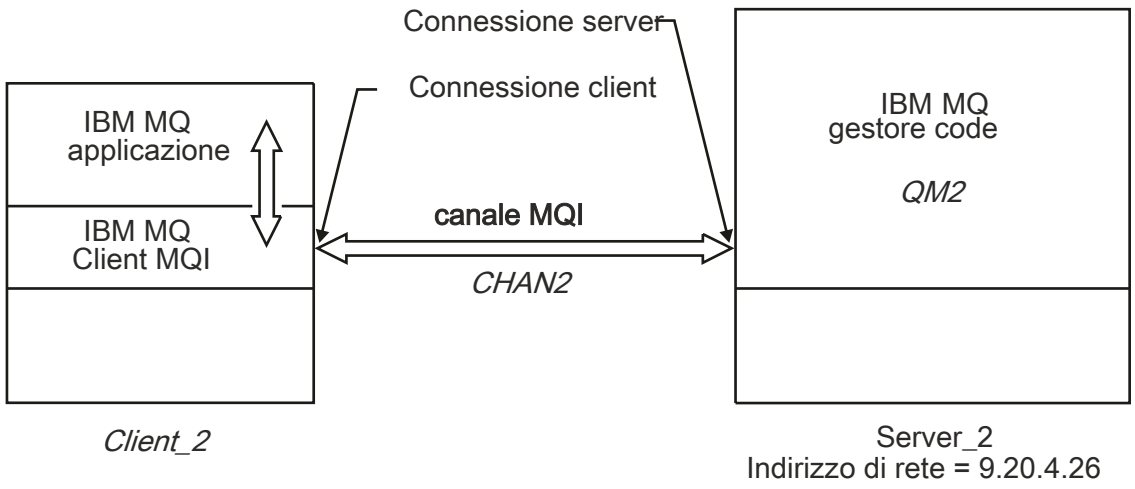


Figura 3. Definizione del canale di connessione client

Accesso alle definizioni del canale di connessione client

È possibile rendere la tabella di definizione del canale client (CCDT) disponibile per le applicazioni client copiandola o condividendolo, quindi specificarne l'ubicazione e il nome sul computer client. Da IBM MQ

9.0, IBM MQ fornisce anche la possibilità di individuare una CCDT (client channel definition table) tramite un URL.

Prima di iniziare

Questa attività presuppone che siano stati definiti, in una CCDT, i canali di connessione client necessari. Consultare "Configurazione delle tabelle di definizione del canale client" a pagina 41.

Informazioni su questa attività

Affinché un'applicazione client utilizzi la CCDT (client channel definition table), è necessario renderla disponibile e specificarne l'ubicazione e il nome. Esistono diversi modi per eseguire questa operazione:

- È possibile copiare CCDT 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.

Da IBM MQ 9.0, IBM MQ, le applicazioni native (C/C + +, COBOL e RPG) e .NET non gestite possono estrarre la CCDT ospitata in una posizione centrale da un URL, sia che si tratti di un file locale, di una risorsa ftp o http.

Procedura

1. Rendere CCDT disponibile per le applicazioni client in uno dei 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.
   d) Opzionale: Definire un file locale, un URL ftp o http per un CCDT ospitato in un'ubicazione centrale in modo che le applicazioni native (C/C + +, COBOL e RPG) e .NET non gestite possano estrarre il CCDT da questo URL.

   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, consultare "Stanza CHANNELS del file di configurazione client" a pagina 160.
   b) Opzionale: Utilizzare le variabili di ambiente MQCHLLIB e MQCHLTAB.

      Ad esempio, è possibile impostare le variabili di ambiente immettendo:

      - Su sistemi UNIX and Linux :

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

      - IBM i Su IBM i:

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

      dove *MQ_INSTALLATION_PATH* rappresenta la directory di alto livello in cui è installato IBM MQ .
   c) Opzionale: Solo su Windows , utilizzare il comando di controllo **setmqscp** per pubblicare le definizioni di canale di connessione client in Active Directory.
   d) Fornire l'ubicazione di una CCDT ospitata centralmente tramite un URL, programmando utilizzando MQCNO, utilizzando le variabili di ambiente o utilizzando le stanze del file `mqclient.ini` . Per ulteriori informazioni, consultare "Ubicazioni per la CCDT" a pagina 51 e "Accesso URL alla CCDT" a pagina 52.

Se la variabile di ambiente MQSERVER è impostata, un client IBM MQ utilizza la definizione del canale di connessione client specificata da MQSERVER come preferenza per qualsiasi definizione nella tabella di definizione del canale client.

Concetti correlati

“Accesso URL alla CCDT” a pagina 52
È possibile ospitare una CCDT (client channel definition table) in un'ubicazione centrale a cui è possibile accedere tramite un URL, eliminando la necessità di aggiornare singolarmente la CCDT per ciascun client distribuito.

Client MQI: CCDT (Client Channel Definition Table)

Attività correlate

“Configurazione di un formato binario CCDT” a pagina 42
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 Multiplatforms, una CCDT binaria contenente le impostazioni predefinite viene creata automaticamente quando viene creato il gestore code. Utilizzare il comando **runmqsc** per aggiornare una CCDT binaria.

ULW Programmi di uscita canale per canali MQI

Sono disponibili tre tipi di uscita canale per l'ambiente IBM MQ MQI client su UNIX, Linux, and 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 viene fornita come parte di IBM MQ, ma è possibile utilizzare una tecnica di compressione differente)
- Crittografia e decrittografia dei dati utente (questa funzionalità viene fornita come parte di IBM 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 sicurezza per garantire che il server e client IBM 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 58
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 IBM MQ

Attività correlate

Estensione delle funzioni del gestore code

Riferimenti correlati

“Percorso delle uscite” a pagina 58
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 60
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.

ULW 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, and Windows , un file di configurazione client viene aggiunto al sistema durante l'installazione di IBM MQ MQI client. 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 ricercato il file di configurazione del client. La stanza ClientExitPath viene letta e vengono caricate tutte le uscite del canale specificate nella definizione del canale.

ULW 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 4 a pagina 59 illustra l'utilizzo delle uscite di sicurezza in una connessione client, utilizzando il gestore autorizzazioni oggetto IBM 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.

L'indirizzo di memoria restituito dal campo MQCXP SecurityParms deve rimanere indirizzabile e non modificato fino a MQXR_TERM. Un'uscita non deve invalidare o liberare nuovamente la memoria sul sistema prima che l'uscita venga richiamata per MQXR_TERM.

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 4. 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 del rilascio di IBM WebSphere MQ 7.1 potrebbero richiedere l'aggiornamento. Per ulteriori informazioni, consultare Programmi di uscita di sicurezza del canale.

ULW 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 8. Identificazione delle chiamate API

Chiamata API	**Valore del byte 10 per la richiesta**	**Valore del byte 10 per la risposta**
MQCONN “1” a pagina 61, “2” a pagina 61	X'81 '	'91'
MQDISC “1” a pagina 61	X'82 '	X' 92 '
MQOPEN “3” a pagina 61	X'83 '	X' 93 '
MQCLOSE	84 '	'94'
MQGET “4” a pagina 61	X'85 '	X' 95 '
MQPUT “4” a pagina 61	X'86 '	X' 96 '
MQPUT1 richiesta “4” a pagina 61	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.

z/OS 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.

Informazioni su questa attività

Un gruppo di condivisione code è formato da un insieme di gestori code che possono accedere allo stesso insieme di code condivise. Per ulteriori informazioni sulle code condivise, consultare Code condivise e gruppi di condivisione code.

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 a un gestore code specifico all'interno del gruppo di condivisione code.

L'interfaccia generica può essere un indirizzo VIPA del distributore Sysplex o un nome risorsa generico VTAM oppure un'altra interfaccia comune per il gruppo di condivisione code. Per ulteriori dettagli sull'impostazione di un'interfaccia generica, consultare Impostazione della comunicazione per IBM MQ for z/OS utilizzando i gruppi di condivisione code.

Procedura

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. A tale scopo, è necessario disporre delle stesse definizioni su ciascun gestore code del gruppo.

1. Definire il canale SVRCONN come mostrato nel seguente esempio:

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

   Le definizioni di canale sul server sono memorizzate in un repository Db2 condiviso. Ciascun gestore code nel gruppo di condivisione code effettua una copia locale della definizione, assicurandosi di connettersi sempre al canale di connessione server corretto quando si emette una chiamata MQCONN o MQCONNX.
2. Definire il canale CLNTCONN come mostrato nel seguente esempio:

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

Risultati

Poiché l'interfaccia generica del gruppo di condivisione code è memorizzata nel campo CONNAME nel canale di collegamento client, è ora possibile connettersi a qualsiasi gestore code del gruppo e inserirlo nelle code condivise di proprietà di tale gruppo.

Utilizzo delle variabili d'ambiente IBM MQ

È possibile utilizzare i comandi per visualizzare le impostazioni correnti o per reimpostare i valori delle variabili di ambiente IBM MQ .

Informazioni su questa attività

È possibile utilizzare le variabili di ambiente nei modi seguenti:

- Per impostare le variabili nel proprio profilo di sistema per effettuare una modifica permanente
- Per immettere un comando dalla riga comandi per effettuare 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

Per ogni variabile di ambiente, è possibile utilizzare i comandi per visualizzare l'impostazione corrente o per reimpostare il valore della variabile. Questi comandi sono disponibili su tutte le piattaforme IBM MQ MQI client , se non diversamente specificato. Il formato del comando dipende dalla piattaforma. Ad esempio:

- Linux UNIX Su UNIX and Linux:

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

- Windows Su Windows:

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

- IBM i Su IBM i:

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

Dove applicabile, IBM MQ utilizza i valori predefiniti per le variabili che non sono state impostate.

Nota: z/OS IBM MQ for z/OS non supporta alcuna variabile di ambiente IBM MQ . Se si utilizza questa piattaforma come server, consultare Tabella di definizione del canale client per informazioni su come viene generata la tabella di definizione del canale client su z/OS. Puoi ancora usare le variabili di ambiente IBM MQ sulla tua piattaforma client.

Procedura

- Windows
  Su Windows, per ogni variabile di ambiente, utilizzare i seguenti comandi per visualizzare l'impostazione corrente o per reimpostare il valore di una variabile:
  - Per eliminare il valore di una variabile di ambiente, utilizzare il comando seguente:

    ```
    SET MQSERVER=
    ```

  - Per visualizzare l'impostazione corrente di una variabile di ambiente, utilizzare il comando seguente:

    ```
    SET MQSERVER
    ```

  - Per visualizzare tutte le variabili di ambiente per la sessione, utilizzare il seguente comando:

```
set
```

- Linux UNIX
  Su UNIX and Linux, per ogni variabile di ambiente, utilizzare i seguenti comandi per visualizzare l'impostazione corrente o per reimpostare il valore di una variabile:
  - Per eliminare il valore di una variabile di ambiente, utilizzare il comando seguente:
    ```
    unset MQSERVER
    ```
  - Per visualizzare l'impostazione corrente di una variabile di ambiente, utilizzare il comando seguente:
    ```
    echo $MQSERVER
    ```
  - Per visualizzare tutte le variabili di ambiente per la sessione, utilizzare il seguente comando:
    ```
    set
    ```

Attività correlate

Impostazione delle variabili di ambiente per IBM MQ classes for JMS

Variabili di ambiente relative a IBM MQ classes for Java

Definizione di variabili di ambiente aggiuntive nel file service.env

“Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms” a pagina 83
È possibile modificare il comportamento di IBM MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione modificando le informazioni nei file di configurazione (`.ini`). È anche possibile modificare le opzioni di configurazione per IBM MQ MQI clients.

Riferimenti correlati

Utilizzo delle variabili di ambiente nelle proprietà MFT

Descrizioni delle variabili di ambiente

Descrizioni delle variabili di ambiente server e client destinate all'utilizzo da parte del cliente.

Esempi di utilizzo

- Linux UNIX Su sistemi UNIX and Linux , utilizzare questo formato: `export [environment variable]=value`.
- Windows Su sistemi Windows , utilizzare questo formato: `Set [environment variable]=value`.
- IBM i Su sistemi IBM i , utilizzare questo formato: `ADDENVVAR ENVVAR(environment variable) VALUE(xx)`.
- MQ Appliance Per IBM MQ Appliance, vedi Configuring environment variables on IBM MQ Appliance nella documentazione IBM MQ Appliance .

AMQ_ALLOWED_CIPHERS

V 9.1.1 Multi

Da IBM MQ 9.1.1, puoi utilizzare la variabile di ambiente **AMQ_ALLOWED_CIPHERS** per specificare un elenco personalizzato di CipherSpecs abilitati per l'utilizzo con i canali IBM MQ su Multiplatforms. La variabile di ambiente assume gli stessi valori dell'attributo della stanza **AllowedCipherSpecs** SSL del file `.ini` :

- Un singolo nome CipherSpec oppure
- Un elenco separato da virgole di nomi IBM MQ CipherSpec da riabilitare o
- Il valore speciale di ALL, che rappresenta tutte le CipherSpecs (non consigliato).

Nota: L'abilitazione di **ALL** CipherSpecs non è consigliata poiché abiliterà i protocolli SSL 3.0 e TLS 1.0 e un numero elevato di algoritmi crittografici deboli.

Per ulteriori informazioni, vedi Fornisci un elenco personalizzato di CipherSpecs abilitati su Multiplatforms nell'ordine CipherSpec nell'handshake TLS.

FDCS _DATA_BAD_AMQ_

La variabile di ambiente **AMQ_BAD_COMMS_DATA_FDCS** è valida quando è impostata su qualsiasi valore.

Se i dati che IBM MQ riceve da un host su TCP/IP sono in un formato non corretto, ad esempio perché un client di rete si è connesso a una porta del listener IBM MQ e ha tentato di comunicare con un protocollo di applicazione non supportato, il gestore code scrive un messaggio di errore AMQ9207E nei log di errori del gestore code. I listener IBM MQ supportano le connessioni TCP/IP da MCA (message channel agent) del gestore code e da applicazioni client MQI, JMS e XMS .

Nota: I listener IBM MQ non supportano il protocollo dell'applicazione utilizzato dai client AMQP e MQTT, questi client devono invece connettersi alle porte di rete configurate nel canale AMQP o nel servizio di telemetria MQXR applicabile.

Potrebbe essere scritto anche un record FDC (failure data capture) contenente i dati non validi ricevuti da IBM MQ . Tuttavia, un file FFST non viene generato se questo è l'inizio di una conversazione con il lato remoto e il formato è un semplice formato noto come una richiesta GET da un browser Web HTTP . Se si desidera sovrascrivere questo valore per far sì che i file FFST vengano scritti per qualsiasi dato non valido, inclusi i semplici formati noti, è possibile impostare la variabile di ambiente **AMQ_BAD_COMMS_DATA_FDCS** su qualsiasi valore (ad esempio, TRUE) e riavviare il gestore code.

AMQ_TRASPORTBCDICNEWLINE

Multi V 9.1.2 V 9.1.0.2

Da IBM MQ 9.1.0 Fix Pack 2 e IBM MQ 9.1.2, è possibile utilizzare la variabile di ambiente **AMQ_CONVEBCDICNEWLINE** per specificare come IBM MQ deve convertire un carattere EBCDIC NL in formato ASCII. La variabile di ambiente assume gli stessi valori dell'attributo **ConvEBCDICNewline** di `mqs.ini`, ovvero, `NL_TO_LF`, `TABLE`o `ISO` (vedere “Stanza AllQueueManagers del file mqs.ini” a pagina 89). È possibile, ad esempio, utilizzare la variabile di ambiente **AMQ_CONVEBCDICNEWLINE** invece dell'attributo della stanza **ConvEBCDICNewline** per fornire la funzionalità **ConvEBCDICNewline** sul lato client in situazioni in cui non è possibile utilizzare il file `mqs.ini` . Se sono impostati sia l'attributo stanza che la variabile di ambiente, l'attributo stanza ha la precedenza.

Per ulteriori informazioni, consultare Conversione dei dati tra serie di caratteri codificati .

AMQ_DIAGNOSTIC_MSG_SEVERITY

V 9.1.0

Da IBM MQ 9.1, se la variabile di ambiente **AMQ_DIAGNOSTIC_MSG_SEVERITY** è impostata su 1 per un processo IBM MQ , la severità del messaggio viene accodata al numero del messaggio come un singolo carattere alfabetico maiuscolo quando il processo IBM MQ scrive un messaggio in un log degli errori o nella console.

Il comportamento abilitato da **AMQ_DIAGNOSTIC_MSG_SEVERITY** è impostato per impostazione predefinita. Puoi disattivare questo comportamento impostando la variabile di ambiente su `0`.

Per ulteriori informazioni, vedi Utilizzo dei log degli errori.

AMQ_DISABLE_CLIENT_AMS

È possibile utilizzare la variabile di ambiente **AMQ_DISABLE_CLIENT_AMS** per disabilitare IBM MQ Advanced Message Security (AMS) sul client se viene riportato un errore 2085 `(MQRC_UNKNOWN_OBJECT_NAME)` quando si tenta di connettersi a un gestore code da una versione precedente del prodotto e si sta utilizzando uno dei seguenti client:

- Un Java runtime environment (JRE) diverso da IBM Java runtime environment (JRE)
- Un client IBM MQ IBM MQ classes for JMS o IBM MQ classes for Java .

Nota: Non è possibile utilizzare la variabile di ambiente **AMQ_DISABLE_CLIENT_AMS** per client C. È necessario utilizzare la variabile di ambiente **MQS_DISABLE_ALL_INTERCEPT** .

Per ulteriori informazioni, consultare Disabilitazione di Advanced Message Security sul client.

AMQ_DMPMQCFG_QSGDISP_DEFAULT

V 9.1.5 V 9.1.0.5

Da IBM MQ 9.1.0 Fix Pack 5 e IBM MQ 9.1.5, le richieste sulla disposizione di un gestore code utilizzate dal comando **dmpmqcfg** richiedono solo le definizioni QSGDISP (QMGR) per impostazione predefinita. È possibile richiedere ulteriori definizioni utilizzando la variabile di ambiente **AMQ_DMPMQCFG_QSGDISP_DEFAULT** , che può essere impostata su uno dei seguenti valori:

ATTIVO
Includere solo gli oggetti definiti con QSGDISP (QMGR) o QSGDISP (COPY).

TUTTO
Includere gli oggetti definiti con QSGDISP (QMGR) e QSGDISP (COPY). Se il gestore code è membro di un gruppo di condivisione code, vengono inclusi anche QSGDISP (GROUP) e QSGDISP (SHARED).

Copia
Includi solo, oggetti definiti con QSGDISP (COPY)

GRUPPO
Includere solo oggetti definiti con QSGDISP (GROUP); il gestore code di destinazione deve essere un membro di un gruppo di condivisione code.

QMGR
Includere solo gli oggetti definiti con QSGDISP (QMGR). Questo è il comportamento predefinito se si utilizza questa variabile di ambiente, per corrispondere al comportamento esistente di **dmpmqcfg**.

PRIVATO
Includere solo gli oggetti definiti con QSGDISP (QMGR) o QSGDISP (COPY).

CONDIVISO
Includere solo gli oggetti definiti con QSGDISP (SHARED).

METRICA_LICENZA_AMQ

V 9.1.1 Multi

Da IBM MQ 9.1.1, l'impostazione della variabile di ambiente **AMQ_LICENSING_METRIC=VPCMonthlyPeak** fa in modo che il gestore code carichi i dati relativi ai tipi di licenze VPC mensili, invece del comportamento predefinito di caricamento dei dati relativi a licenze basate su contenitore orarie.

Per ulteriori informazioni sulla configurazione di IBM MQ per l'utilizzo con il servizio di misurazione IBM Cloud Private , consultare IBM Cloud Private servizio di misurazione nella documentazione di IBM Cloud Private .

TRACCIA AMQ_LDAP_

V 9.1.0.4 V 9.1.4

Da IBM MQ 9.1.0 Fix Pack 4 e IBM MQ 9.1.4, se la variabile di ambiente **AMQ_LDAP_TRACE** è impostata su un valore non null, è possibile attivare e disattivare la traccia del client LDAP senza arrestare o avviare anche il gestore code.

Per ulteriori informazioni, consultare Abilitazione della traccia dinamica del codice della libreria client LDAP.

MQ_MQS_INI_LOCATION

Su sistemi UNIX and Linux , è possibile modificare l'ubicazione utilizzata per il file `mqs.ini` impostando l'ubicazione del file `mqs.ini` nella variabile di ambiente **AMQ_MQS_INI_LOCATION** . Questa variabile di ambiente deve essere impostata a livello di sistema.

Per ulteriori informazioni sul file `mqs.ini` , incluse le ubicazioni delle directory, consultare "File di configurazione IBM MQ , mqs.ini" a pagina 84.

FDCS - NO_AMQ_BAD_COMMS_DATA_

La variabile di ambiente **AMQ_NO_BAD_COMMS_DATA_FDCS** è valida quando è impostata su qualsiasi valore.

Se IBM MQ non riconosce la trasmissione iniziale dei dati durante il tentativo di connessione di un client nonIBM MQ a un listener TCP/IP IBM MQ , il gestore code scriverà un messaggio di errore AMQ9207E nei log di errori del gestore code. Viene scritto anche un record FDC (failure data capture). È possibile sopprimere la generazione di questi file diagnostici con la variabile di ambiente **AMQ_NO_BAD_COMMS_DATA_FDCS** . Quando **AMQ_NO_BAD_COMMS_DATA_FDCS** è impostato su un valore (ad esempio, TRUE), questo indica a IBM MQ di non generare FFST quando si riportano i messaggi di errore AMQ9207E sul flusso di comunicazioni iniziale. Per essere efficace, la variabile di ambiente deve essere impostata prima di avviare i processi del gestore code e del listener.

L'FDC continua ad essere generato nel caso in cui un client invii flussi di protocollo IBM MQ validi al gestore code e quindi invii dati non validi, poiché ciò è indicativo di un problema del client che richiede ulteriori indagini.

AMQ_NO_IPV6

La variabile di ambiente **AMQ_NO_IPV6** è valida quando è impostata su qualsiasi valore. Quando questa variabile di ambiente è impostata, disabilita l'utilizzo di IPv6 durante il tentativo di connessione.

ORDINE_ANNULLAMENTO_COMMIT

La variabile di ambiente **AMQ_REVERSE_COMMIT_ORDER** configura un gestore code in modo che in una transazione XA venga eseguito il commit della modifica del gestore code IBM MQ una volta completato l'aggiornamento del corrispondente database. Le applicazioni che leggono i messaggi dalle code visualizzano un messaggio solo dopo che è stato completato l'aggiornamento del database corrispondente.

Nota: Non impostare **AMQ_REVERSE_COMMIT_ORDER** senza leggere e comprendere lo scenario descritto in Livello di isolamento.

AMQ_SSL_ALLOW_DEFAULT_CERT

Da IBM MQ 9.0.0 Fix Pack 1 e IBM MQ 9.0.2, se la variabile d'ambiente **AMQ_SSL_ALLOW_DEFAULT_CERT** non è impostata, un'applicazione può connettersi a un gestore code con un certificato personale nel keystore del client solo quando il certificato include il nome etichetta `ibmwebspheremq`*`userid`*. Quando la variabile di ambiente **AMQ_SSL_ALLOW_DEFAULT_CERT** è impostata, il certificato non richiede il nome etichetta `ibmwebspheremq`*`userid`*. In altre parole, il certificato utilizzato per connettersi a un gestore code può essere un certificato predefinito, purché sia presente un certificato predefinito nel repository delle chiavi e il repository delle chiavi non contenga un certificato personale con prefisso `ibmwebspheremq`*`userid`*.

Un valore di 1 abilita l'utilizzo di un certificato predefinito.

Invece di utilizzare la variabile di ambiente **AMQ_SSL_ALLOW_DEFAULT_CERT** , un'applicazione può utilizzare l'impostazione **CertificateLabel** della stanza SSL nel file `mqclient.ini` . Per ulteriori

informazioni, vedi Etichette di certificati digitali, che comprendono i requisiti e “Stanza SSL del file di configurazione client” a pagina 168.

AMQ_SSL_LDAP_SERVER_VERSION

La variabile di ambiente **AMQ_SSL_LDAP_SERVER_VERSION** può essere utilizzata per garantire che LDAP v2 o LDAP v3 venga utilizzato dai componenti crittografici IBM MQ nei casi in cui i server CRL richiedono l'utilizzo di una versione specifica del protocollo LDAP.

Impostare la variabile di ambiente sul valore appropriato nell'ambiente utilizzato per avviare il gestore code o il canale:

- Per richiedere l'utilizzo di LDAP v2 , impostare `AMQ_SSL_LDAP_SERVER_VERSION=2`.
- Per richiedere l'utilizzo di LDAP v3 , impostare `AMQ_SSL_LDAP_SERVER_VERSION=3`.

Questa variabile di ambiente non influisce sulle connessioni LDAP stabilite dal gestore code IBM MQ per l'autenticazione utente o l'autorizzazione utente.

MQ_GMQ_LIB

Quando il server IBM MQ MQI client e IBM MQ sono installati sul sistema, le classi di automazione IBM MQ per le applicazioni ActiveX (MQAX) vengono eseguite sul server per impostazione predefinita. Per eseguire MQAX sul client, la libreria di bind client deve essere specificata nella variabile di ambiente **GMQ_MQ_LIB** , ad esempio, impostare `GMQ_MQ_LIB=mqic.dll`. Per un'installazione solo client, non è necessario impostare la variabile di ambiente **GMQ_MQ_LIB** . Quando questa variabile di ambiente non è impostata, IBM MQ tenta di caricare `amqzst.dll`. Se questa DLL non è presente (come nel caso di un'installazione solo client), IBM MQ tenta di caricare `mqic.dll`.

HOME

IBM i Linux UNIX

In UNIX, Linux e IBM i, la variabile di ambiente **HOME** specifica il nome della directory in cui viene ricercato il file `mqclient.ini` . Questo file contiene informazioni di configurazione utilizzate da IBM MQ MQI clients.

Per ulteriori informazioni, consultare “IBM MQ MQI client file di configurazione, mqclient.ini” a pagina 146 e “Ubicazione del file di configurazione client” a pagina 148.

HOMEDRIVE e HOMEPATH

Windows

Per essere utilizzate, devono essere impostate sia le variabili di ambiente **HOMEDRIVE** che **HOMEPATH** . Vengono utilizzati su sistemi Windows per specificare il nome della directory in cui viene ricercato il file `mqclient.ini` . Questo file contiene informazioni di configurazione utilizzate da IBM MQ MQI clients.

Per ulteriori informazioni, consultare “IBM MQ MQI client file di configurazione, mqclient.ini” a pagina 146 e “Ubicazione del file di configurazione client” a pagina 148.

LDAP_BASEDN

LDAP_BASEDN è la variabile di ambiente richiesta per l'esecuzione di un programma di esempio LDAP. Specifica il DN (Distinguished Name) di base per la ricerca nell'indirizzario.

HOST_LDAP

LDAP_HOST è una variabile di ambiente facoltativa per l'esecuzione di un programma di esempio LDAP. Specifica il nome dell'host su cui è in esecuzione il server LDAP; se non viene specificato, viene utilizzato per impostazione predefinita l'host locale.

VERSIONE LDAP

LDAP_VERSION è una variabile di ambiente facoltativa per l'esecuzione di un programma di esempio LDAP. Specifica la versione del protocollo LDAP da utilizzare e può essere 2 o 3. La maggior parte dei server LDAP ora supporta la versione 3 del protocollo; tutti supportano la versione precedente 2. Questo esempio funziona ugualmente bene con entrambe le versioni del protocollo e, se non viene specificato, il valore predefinito è la versione 2.

INTERVALLO_ELIMINAZIONE_CANALE_MQ

La variabile di ambiente **MQ_CHANNEL_SUPPRESS_INTERVAL** specifica l'intervallo di tempo, in secondi, durante il quale i messaggi definiti con **MQ_CHANNEL_SUPPRESS_MSGS** devono essere eliminati dalla scrittura nel log degli errori, insieme al numero di volte in cui un messaggio può verificarsi durante l'intervallo di tempo specificato prima di essere eliminato. Il valore predefinito è 60,5, il che significa che ogni ulteriore ricorrenza di un determinato messaggio viene soppressa dopo le prime cinque ricorrenze di tale messaggio in un intervallo di 60 secondi. Per ulteriori informazioni, consultare Soppressione dei messaggi di errore del canale dai log degli errori su Multiplatforms.

La variabile di ambiente **MQ_CHANNEL_SUPPRESS_INTERVAL** è paragonabile a SuppressInterval nel file “File di configurazione del gestore code, qm.ini” a pagina 97 .

MQ_CHANNEL_SUPPRESS_MSGS

La variabile di ambiente **MQ_CHANNEL_SUPPRESS_MSGS** elimina i messaggi di errore del canale nel log degli errori. È possibile specificare un elenco di messaggi eliminati. **MQ_CHANNEL_SUPPRESS_MSGS** viene utilizzato insieme a **MQ_CHANNEL_SUPPRESS_INTERVAL**, che specifica il numero di volte in cui ogni messaggio viene visualizzato prima di essere eliminato e l'intervallo di tempo per cui i messaggi vengono eliminati. Per ulteriori informazioni, consultare Soppressione dei messaggi di errore del canale dai log degli errori su Multiplatforms.

La variabile di ambiente **MQ_CHANNEL_SUPPRESS_MSGS** è paragonabile a SuppressMessage nel file “File di configurazione del gestore code, qm.ini” a pagina 97 , ad eccezione del fatto che è possibile eliminare qualsiasi messaggio del canale utilizzando la variabile di ambiente, mentre esiste un elenco restrittivo per il metodo `qm.ini` .

TIPO_MQ_CONNECT_

Su Multiplatforms, è possibile utilizzare la variabile d'ambiente **MQ_CONNECT_TYPE** in combinazione con il tipo di collegamento specificato nel campo Opzioni della struttura MQCNO utilizzata su una chiamata MQCONNX. **MQ_CONNECT_TYPE** ha effetto solo per i bind STANDARD. Per altri bind, **MQ_CONNECT_TYPE** viene ignorato.

Per ulteriori informazioni, consultare Utilizzo delle opzioni di chiamata MQCONNX con MQ_CONNECT_TYPE.

MQ_CROSS_QUEUE_ORDER_ALL

Quando si imposta la variabile di ambiente **MQ_CROSS_QUEUE_ORDER_ALL** su un valore diverso da zero, l'ordine di inserimento del messaggio viene conservato in un'unità di lavoro. Ciò significa che, se i messaggi in una UOW (Unit of Work) (UoW) vengono inseriti in più code (ad esempio, Q1, quindi Q2), quando viene emesso un MQCMIT, i messaggi vengono consegnati e resi disponibili nello stesso ordine della coda in cui erano PUT.

In un ambiente con più gestori code, **MQ_CROSS_QUEUE_ORDER_ALL** deve esistere e avere un valore non vuoto sia sul lato di invio che su quello di ricezione prima che ogni gestore code venga avviato.

MQ_EPHEMER_PREFIX

La variabile di ambiente **MQ_EPHEMERAL_PREFIX** specifica il percorso della directory temporanea del gestore code, all'interno della quale vengono conservati i dati del gestore code temporaneo, mentre il gestore code è in esecuzione.

Come alternativa alla modifica del prefisso temporaneo modificando l'attributo **EphemeralPrefix** nell'attributo **DefaultEphemeralPrefix** della stanza AllQueueManagers del file `mqs.ini` , è possibile utilizzare la variabile d'ambiente **MQ_EPHEMERAL_PREFIX** per sovrascrivere **EphemeralPrefix** per il comando **crtmqm** . Per ulteriori informazioni, consultare “Directory effimera configurabile” a pagina 10.

PERCORSO MQ_FILE

Windows

La variabile di ambiente **MQ_FILE_PATH** viene configurata durante l'installazione del pacchetti di runtime sulla piattaforma Windows . Questa variabile di ambiente contiene gli stessi dati della seguente chiave nel registro Windows :

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

Per ulteriori informazioni, consultare setmqenv (set IBM MQ environment) e crtmqenv (create IBM MQ environment).

MQ_JAVA_DATA_PATH

La variabile di ambiente **MQ_JAVA_DATA_PATH** specifica la directory per l'output di log e traccia per IBM MQ classes for JMS e IBM MQ classes for Java. Viene utilizzato dagli script forniti con IBM MQ classes for JMS e IBM MQ classes for Java.

Per ulteriori informazioni, consultare Impostazione delle variabili di ambiente per IBM MQ classes for JMS e Variabili di ambiente relative alle classi IBM MQ per Java.

PERCORSO_INSTALL_JAVA_MQ_

La variabile di ambiente **MQ_JAVA_INSTALL_PATH** specifica la directory in cui sono installati IBM MQ classes for JMS come mostrato in Elementi installati per le classi IBM MQ per JMSe IBM MQ classes for Java come mostrato in Directory di installazione IBM MQ classes for Java .

Per ulteriori informazioni, consultare Impostazione delle variabili di ambiente per IBM MQ classes for JMS e Variabili di ambiente relative alle classi IBM MQ per Java.

MQ_JAVA_LIB_PATH

La variabile di ambiente **MQ_JAVA_LIB_PATH** specifica la directory in cui sono memorizzate le librerie IBM MQ classes for JMSe IBM MQ classes for Java . Alcuni script, ad esempio IVTRun, forniti con IBM MQ classes for JMS o IBM MQ classes for Java utilizzano questa variabile di ambiente.

Per ulteriori informazioni, consultare Impostazione delle variabili di ambiente per IBM MQ classes for JMS e Variabili di ambiente relative alle classi IBM MQ per Java.

MQ_SET_NODELAYACK

AIX

La variabile di ambiente **MQ_SET_NODELAYACK** disattiva il riconoscimento ritardato TCP su AIX.

Quando si imposta questa variabile di ambiente, l'impostazione disattiva la ricezione ritardata TCP richiamando la chiamata setsockopt del sistema operativo con l'opzione TCP_NODELAYACK . Solo AIX supporta questa funzione, quindi la variabile di ambiente **MQ_SET_NODELAYACK** ha effetto solo su AIX.

LOGFILE MQAPI_TRACE_

Il programma di uscita API di esempio genera una traccia MQI per un file specificato dall'utente con un prefisso che è definito nella variabile di ambiente **MQAPI_TRACE_LOGFILE** .

Per ulteriori informazioni, consultare Il programma di esempio dell'uscita API.

NOME MQAPPL

ULW V 9.1.2

Se il nome dell'applicazione non è stato ancora scelto, è possibile utilizzare la variabile di ambiente **MQAPPLNAME** come nome da utilizzare per identificare la connessione a un gestore code. Vengono utilizzati solo i primi 28 caratteri e non devono essere tutti spazi o valori null.

Per ulteriori informazioni, consultare Utilizzo del nome applicazione nei linguaggi di programmazione supportati.

MQCCSID

La variabile di ambiente **MQCCSID** specifica il numero della serie di caratteri codificati da utilizzare e sostituisce il valore CCSID con cui è stato configurato il server. **MQCCSID** può essere utilizzato per sovrascrivere il CCSID nativo di un'applicazione e specificare il numero della serie di caratteri codificati da utilizzare, ad esempio se il CCSID nativo è un CCSID non supportato o non è il CCSID richiesto.

Per impostare **MQCCSID**, utilizzare uno dei seguenti comandi:

- Linux UNIX Su UNIX and Linux:

```
export MQCCSID=number
```

- Windows Su Windows:

```
SET MQCCSID=number
```

- IBM i Su IBM i:

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

Per ulteriori informazioni, consultare Scelta del CCSID del client o del server.

URL MQCCDT

La variabile di ambiente **MQCCDTURL** fornisce la capacità equivalente di impostare una combinazione delle variabili di ambiente **MQCHLLIB** e **MQCHLTAB** . Consente di fornire un file, ftp o http URL come un singolo valore da cui è possibile ottenere una tabella di definizione del canale client per i programmi nativi che si collegano come client, ovvero applicazioni C, COBOL o C + +.

Nota: L'utilizzo delle variabili di ambiente per fornire l' URL non ha alcun effetto per le applicazioni Java, JMS o .NET gestite.

IBM MQ supporta il richiamo di una CCDT da un file, ftp o http URL. Tuttavia, **MQCCDTURL** accetta solo un valore URL . Non accetta il formato indirizzario del file system locale esistente.

Per utilizzare **MQCCDTURL** al posto di **MQCHLLIB** e **MQCHLTAB** con un file locale, puoi utilizzare un protocollo `'file://'` . Pertanto, come mostrato in questo esempio per AIX e Linux:

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

equivale a:

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

Puoi specificare anche un file JSON come mostrato in questo esempio per Windows:

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

equivale a:

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

Per ulteriori informazioni, consultare "Accesso URL alla CCDT" a pagina 52.

MQCERTLABL

La variabile di ambiente di **MQCERTLABL** definisce l'etichetta del certificato di una definizione di canale che IBM MQ deve utilizzare per individuare un certificato personale inviato durante un handshake TLS.

Per ulteriori informazioni, consultare Etichette di certificati digitali, che comprendono i requisiti.

MQCERTVPOL

La variabile di ambiente **MQCERTVPOL** specifica il tipo di politica di convalida del certificato da utilizzare. Questa variabile di ambiente sovrascrive l'attributo **CertificateValPolicy** nella stanza SSL del file di configurazione client.

MQCERTVPOL può essere impostato su uno dei seguenti due valori:

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.

Per impostare **MQCERTVPOL**, utilizzare uno dei seguenti comandi:

- Linux UNIX Per sistemi UNIX and Linux :

  ```
  export MQCERTVPOL= value
  ```

- Windows Per sistemi Windows :

  ```
  SET MQCERTVPOL= value
  ```

- IBM i Per sistemi IBM i :

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

Per ulteriori informazioni, consulta Certificate validation policies in IBM MQ e Configuring certificate validation policies in IBM MQ.

MQCHLLIB

La variabile di ambiente **MQCHLLIB** specifica il percorso di directory del file che contiene la CCDT (client channel definition table). Il file viene creato sul server, ma può essere copiato sulla workstation IBM MQ MQI client .

Per impostare **MQCHLLIB**, utilizzare uno dei seguenti comandi:

- Windows Su Windows:

```
SET MQCHLLIB=pathname
```

  Ad esempio:

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

- Linux UNIX Per sistemi UNIX and Linux :

```
export MQCHLLIB=pathname
```

- IBM i Per IBM i:

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

Se **MQCHLLIB** non è impostato, il percorso per il client assume il valore predefinito:

- Linux UNIX Su UNIX and Linux: `/var/mqm/`
- Windows Su Windows: *MQ_INSTALLATION_PATH*
- IBM i Su IBM i: `/QIBM/UserData/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 valore predefinito del percorso è uno della prima serie. Se *datapath* non è impostato, il percorso assume il valore predefinito di uno della seconda serie.

- Linux UNIX Su UNIX and Linux: *datapath*`/@ipcc`
- Windows Su Windows: *datapath*`\@ipcc`
- IBM i Su IBM i: *datapath*`/&ipcc`

Oppure:

- Linux UNIX Su UNIX and Linux: `/prefix/qmgrs/`*qmgrname*`/@ipcc`
- Windows Su Windows: *MQ_INSTALLATION_PATH*`\data\qmgrs\`*qmgrname*`\@ipcc`
- IBM i Su IBM i: `/`*prefix*`/qmgrs/`*qmgrname*`/&ipcc`

dove:

- *MQ_INSTALLATION_PATH* rappresenta la directory di alto livello in cui è installato IBM 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 di solito uno dei seguenti valori:
  - Linux UNIX `/var/mqm` su sistemi UNIX and Linux .
  - IBM i `/QIBM/UserData/mqm/` su IBM i.
- *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 posizione in cui è definita la sezione del gestore code dipende dalla piattaforma:
  - IBM i Linux UNIX Nel file `mqs.ini` su IBM i, UNIX and Linux.

– Windows Nel registro su Windows.

Note:

1. z/OS Se si utilizza IBM MQ for z/OS come server, il file deve essere conservato sulla workstation client IBM MQ .
2. Se impostato, MQCHLLIB sovrascrive il percorso utilizzato per individuare la CCDT.
3. MQCHLLIB può contenere un URL che funziona in combinazione con la variabile di ambiente MQCHLTAB (consultare “Accesso URL alla CCDT” a pagina 52).
4. 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.
5. 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** .
6. 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 definizione precedente, le modifiche vengono perse. Per questo motivo, è necessario considerare la ricerca di alternative all'impostazione di **MQCHLLIB** come variabile di ambiente a livello di sistema sul server.
7. 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.
8. Il comando **rcrmqobj** `-t clchltab` elimina e ricrea il file CCDT. Il file viene ricreato solo con le definizioni di connessioni client create sul gestore code su cui è in esecuzione il comando.
9. 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.
10. Il percorso per **MQCHLLIB** non necessita di virgolette.

Per ulteriori informazioni, consultare “Ubicazioni per la CCDT” a pagina 51, “Accesso URL alla CCDT” a pagina 52e Connessione delle applicazioni client ai gestori code utilizzando le variabili di ambiente.

MQCHLTAB

La variabile di ambiente **MQCHLTAB** specifica il nome del file che contiene la CCDT (client channel definition table). Il nome file predefinito è AMQCLCHL.TAB.

Per impostare **MQCHLTAB**, utilizzare uno dei seguenti comandi:

- Linux UNIX Su UNIX and Linux:

```
export MQCHLTAB=filename
```

- Windows Su Windows:

```
SET MQCHLTAB=filename
```

- IBM i Su IBM i:

```
ADDENVVAR ENVVAR(MQCHLTAB) VALUE(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.

Per ulteriori informazioni, consultare “Ubicazioni per la CCDT” a pagina 51, “Accesso URL alla CCDT” a pagina 52e Connessione delle applicazioni client ai gestori code utilizzando le variabili di ambiente.

MQCLNTCF

La variabile di ambiente **MQCLNTCF** specifica l'ubicazione del file di configurazione IBM MQ MQI client . Questo file contiene informazioni di configurazione utilizzate da IBM MQ MQI clients.

È possibile utilizzare la variabile di ambiente **MQCLNTCF** per modificare il percorso del file `mqclient.ini` .

Il formato di questa variabile di ambiente è un URLcompleto. Ciò significa che il nome file potrebbe non essere necessariamente `mqclient.ini`, il che facilita l'inserimento del file su un file system collegato in rete. Per ulteriori informazioni, consultare “IBM MQ MQI client file di configurazione, mqclient.ini” a pagina 146 e “Ubicazione del file di configurazione client” a pagina 148.

TRACE_MQDOTNET_ATTIVO

La variabile di ambiente **MQDOTNET_TRACE_ON** viene utilizzata per abilitare la traccia per client IBM MQ .NET ridistribuibili. I valori uguali e inferiori a 0 non abilitano la traccia, 1 abilita la traccia predefinita e i valori superiori a 1 abilitano la traccia dei dettagli.

Per ulteriori informazioni, consultare Installazione di IBM MQ classes for .NET Standard.

MQIPADRV

La variabile di ambiente **MQIPADDRV** specifica quale protocollo IP utilizzare per una connessione del canale. Ha i valori stringa possibili di `"MQIPADDR_IPV4"` o `"MQIPADDR_IPV6"`. Questi valori hanno lo stesso significato di IPv4 e IPv6 in **ALTER QMGR IPADDRV** e l'attributo **IPAddressVersion** della stanza TCP del file di configurazione client. Se la variabile di ambiente non è impostata, viene utilizzato `"MQIPADDR_IPV4"` .

Per impostare **MQIPADDRV**, utilizzare uno dei seguenti comandi:

- Linux UNIX Su UNIX and Linux:

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

- Windows Su Windows:

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

- IBM i Su IBM i:

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

MQLICENSE

V 9.1.5 Linux

Sui sistemi Linux , è possibile utilizzare la variabile di ambiente **MQLICENSE** per accettare o visualizzare una licenza IBM MQ dopo aver installato il prodotto.

Per ulteriori informazioni sul motivo per cui è possibile o necessario eseguire questa operazione, consultare Accettazione della licenza su IBM MQ per Linux

La variabile di ambiente **MQLICENSE** può essere impostata su uno dei due seguenti valori:

accetta
Accettare la licenza post - installazione.

vista
Visualizzare la licenza, se la licenza è stata accettata.

Per accettare la post - installazione della licenza, utilizzare questo comando:

```
export MQLICENSE=accept
```

Per visualizzare la licenza, utilizzare questo comando:

```
export MQLICENSE=view
```

Nota: È inoltre possibile utilizzare i seguenti comandi per accettare e visualizzare la licenza:

- mqlicense (accetta la licenza dopo l'installazione)
- dspmqlic (visualizza licenza IBM MQ)

DIMENSIONE MQMAXERRORLOGSIZE

Multi

La variabile di ambiente **MQMAXERRORLOGSIZE** specifica la dimensione del file di log degli errori del gestore code copiato nel backup.

Per ulteriori informazioni, vedi Utilizzo dei log degli errori.

NOME

Windows

La variabile di ambiente **MQNAME** specifica il nome NetBIOS locale che i processi IBM MQ possono utilizzare. Una connessione NetBIOS si applica solo a un client e a un server su cui è in esecuzione Windows.

Per impostare **MQNAME**, utilizzare questo comando:

```
SET MQNAME=Your_env_Name
```

Ad esempio:

```
SET MQNAME=CLIENT1
```

Alcune implementazioni NetBIOS richiedono un nome univoco, impostato da **MQNAME**, per ogni applicazione se si eseguono più applicazioni IBM MQ contemporaneamente su IBM MQ MQI client.

Per ulteriori informazioni, consultare “Definizione del nome IBM MQ locale NetBIOS” a pagina 244.

MQNOREMPOOL

Quando si imposta la variabile di ambiente **MQNOREMPOOL** , si disattiva il pool di canali e i canali vengono eseguiti come thread del listener.

Per ulteriori informazioni, fare riferimento a MCATYPE (Message channel agent type).

LOGFILE MQPSE_TRACE_

Si utilizza la variabile di ambiente **MQPSE_TRACE_LOGFILE** quando si esegue il programma di esempio di uscita di pubblicazione AMQSPSE0, che è un esempio di programma C di un'uscita per intercettare una pubblicazione prima che venga consegnata a un sottoscrittore. Nel processo dell'applicazione da tracciare, questa variabile di ambiente descrive dove devono essere scritti i file di traccia.

Per ulteriori informazioni, consultare Programma di esempio Pubblica uscita.

MQS_AMSCRED_XX_ENCODE_CASE_ONE file_chiave

È possibile utilizzare la variabile di ambiente **MQS_AMSCRED_KEYFILE** per sovrascrivere o fornire il file di chiavi iniziale da utilizzare al runtime delle applicazioni IBM MQ Advanced Message Security (AMS) o quando si sta proteggendo un file di configurazione keystore utilizzando il comando **runamscred** .

Per ulteriori informazioni, consultare Utilizzo di keystore e certificati con AMS e Protezione delle password nei file di configurazione del componente IBM MQ.

MQS_DISABLE_ALL_INTERCEPT

È possibile utilizzare la variabile di ambiente **MQS_DISABLE_ALL_INTERCEPT** per disabilitare IBM MQ Advanced Message Security (AMS) se viene riportato un errore 2085 (MQRC_UNKNOWN_OBJECT_NAME) quando si tenta di connettersi a un gestore code da una versione precedente del prodotto e si utilizza IBM MQ con client C nativi.

Nota: È possibile utilizzare la variabile di ambiente **MQS_DISABLE_ALL_INTERCEPT** solo per i client C. Per client Java , è necessario utilizzare invece la variabile di ambiente **AMQ_DISABLE_CLIENT_AMS** .

Per ulteriori informazioni, consultare Disabilitazione di Advanced Message Security sul client.

HOST IP_MQS

Poiché gli oggetti del file system IPC devono essere distinti dal sistema, una sottodirectory per ciascun sistema su cui viene eseguito il gestore code viene aggiunta al percorso della directory. Se il valore generato del nome host crea un problema, è possibile impostare il nome host utilizzando la variabile di ambiente **MQS_IPC_HOST** .

Per ulteriori informazioni, consultare Condivisione dei file IBM MQ su Multiplatforms.

MQS_KEYSTORE_CONF

La variabile di ambiente **MQS_KEYSTORE_CONF** specifica l'ubicazione del file di configurazione del keystore per IBM MQ Advanced Message Security (AMS), se il file non si trova nell'ubicazione predefinita di *home_directory*/.mqs/keystore.conf.

Per ulteriori informazioni, consultare Utilizzo di keystore e certificati con AMS.

Se si verificano problemi su Managed File Transfer, consultare Cosa fare se MFT non legge le proprietà del keystore dal file di configurazione del keystore in AMS.

MQS_TRACE_OPZIONI

AIX

Per la traccia selettiva dei componenti su AIX, utilizzare la variabile d'ambiente **MQS_TRACE_OPTIONS** per attivare singolarmente le funzioni di traccia dei parametri e dei dettagli.

Nota: Impostare la variabile di ambiente **MQS_TRACE_OPTIONS** solo se è stato richiesto dal supporto IBM .

Per ulteriori informazioni, vedi Traccia su UNIX and Linux.

SERVER MQT

La variabile di ambiente **MQSERVER** viene utilizzata per definire un canale minimo. **MQSERVER** specifica l'ubicazione del server IBM MQ e il metodo di comunicazione da utilizzare.

Nota: Non puoi utilizzare **MQSERVER** per definire un canale TLS o un canale con uscite canale. Per ulteriori informazioni su come definire un canale TLS, vedi Protezione dei canali con TLS.

I seguenti esempi mostrano come impostare **MQSERVER**:

- Linux UNIX Su UNIX and Linux:

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

- Windows Su Windows:

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

- IBM i Su IBM i:

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

Nota:

- Il nome del canale non può contenere il carattere barra (/) poiché questo carattere viene utilizzato per separare il nome del canale, il tipo di trasporto e il nome della connessione. Quando si utilizza la variabile di ambiente **MQSERVER** per definire un canale 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.
- Il tipo di trasporto può essere uno tra LU62 , TCP , NETBIOS, SPX, a seconda della piattaforma client IBM MQ .
- Il nome della connessione deve essere un nome di rete completo. ad esempio AMACHINE.ACOMPANY.COM(1414).
- Il nome connessione può essere un elenco separato da virgole di nomi connessione. I nomi di connessione nell'elenco vengono utilizzati in modo simile a più connessioni in una tabella di connessioni client. L'elenco dei nomi delle connessioni potrebbe essere utilizzato come alternativa ai gruppi di gestori code per specificare più collegamenti per il client da provare. Se si sta configurando un gestore code a più istanze, è possibile utilizzare un elenco di nomi di connessione per specificare diverse istanze del gestore code.

Se si utilizza la variabile di ambiente **MQSERVER** per definire il canale tra la macchina IBM MQ MQI client e una macchina server, questo è l'unico canale disponibile per l'applicazione e non viene fatto alcun riferimento alla CCDT (client channel definition table).

Per ulteriori informazioni, consultare “Creazione di un canale di connessione client su IBM MQ MQI client utilizzando MQSERVER” a pagina 36.

MQSNOAUT

Quando si imposta la variabile di ambiente **MQSNOAUT** su qualsiasi valore, disabilita OAM (object authority manager) e impedisce qualsiasi controllo di sicurezza. Potrebbe essere adatto per un ambiente di test.

La variabile di ambiente **MQSNOAUT** ha effetto solo quando viene creato un gestore code.

Avvertenza: Per abilitare OAM, è necessario eliminare il gestore code, eliminare la variabile di ambiente e ricreare il gestore code senza specificare **MQSNOAUT**.

Per ulteriori informazioni, consultare Prevenzione dei controlli di accesso di sicurezza sui sistemi AIX, Linuxe Windows.

MQSPREFIX

In alternativa alla modifica del prefisso predefinito, è possibile utilizzare la variabile di ambiente **MQSPREFIX** per sovrascrivere il **DefaultPrefix** per il comando **crtmqm** .

Per ulteriori informazioni, fare riferimento a IBM MQ nomi file e alla stanza AllQueueManagers del file mqs.ini.

CCRYMQSSL

ULW

La variabile di ambiente **MQSSLCRYP** contiene una stringa di parametro che è possibile utilizzare per configurare l'hardware crittografico presente nel sistema. I valori consentiti sono gli stessi del parametro **SSLCRYP** del comando **ALTER QMGR** .

Per impostare **MQSSLCRYP**, utilizzare uno dei seguenti comandi:

- Linux UNIX Su sistemi UNIX and Linux:

```
export MQSSLCRYP=string
```

- Windows Su sistemi Windows:

```
SET MQSSLCRYP=string
```

Per ulteriori informazioni, consultare Configurazione per l'hardware di crittografia su UNIX, Linux, and Windows.

FIPS MQSSL

La variabile di ambiente **MQSSLFIPS** specifica se devono essere utilizzati solo algoritmi certificati FIPS se la crittografia viene eseguita in IBM MQ. È possibile impostare questa variabile di ambiente su YES o NO Il valore predefinito è NO. Questi valori sono gli stessi del parametro **SSLFIPS** del comando **ALTER QMGR** .

Per impostare **MQSSLFIPS**, utilizzare uno dei seguenti comandi:

- Linux UNIX Su sistemi UNIX and Linux:

```
export MQSSLFIPS=YES|NO
```

- Windows Su sistemi Windows:

```
SET MQSSLFIPS=YES|NO
```

- IBM i Su IBM i:

```
ADDENVVAR ENVVAR(MQSSLFIPS) VALUE(YES|NO)
```

L'uso di algoritmi certificati FIPS è influenzato dall'uso di hardware crittografico. Per ulteriori informazioni, consultare Specifica che solo le CipherSpecs certificate FIPS vengono utilizzate al runtime sul client MQI.

MQSSLKEYR

La variabile di ambiente **MQSSLKEYR** specifica l'ubicazione del repository delle chiavi che contiene il certificato digitale appartenente all'utente, in formato radice. Il formato stem indica che include il percorso completo e il nome file senza un'estensione.

Per impostare **MQSSLKEYR**, utilizzare uno dei seguenti comandi:

- Linux UNIX Su sistemi UNIX and Linux:

```
export MQSSLKEYR=pathname
```

- Windows Su sistemi Windows:

```
SET MQSSLKEYR=pathname
```

- IBM i Su IBM i:

```
ADDENVVAR ENVVAR(MQSSLKEYR) VALUE(pathname)
```

Non esiste alcun valore predefinito per questa variabile di ambiente.

Per ulteriori informazioni, consultare il parametro **SSLKEYR** del comando **ALTER QMGR** .

MQSSLPROX

La variabile di ambiente **MQSSLPROXY** specifica il nome host e il numero di porta del server proxy HTTP che deve essere utilizzato da GSKit per i controlli OCSP.

Per impostare **MQSSLPROXY**, utilizzare uno dei seguenti comandi:

- Linux UNIX Su sistemi UNIX and Linux:

```
export MQSSLPROXY="string"
```

- Windows Su sistemi Windows:

```
SET MQSSLPROXY= string
```

La stringa specificata con **MQSSLPROXY** può essere 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).

Linux UNIX 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"
```

Per ulteriori informazioni, consultare Utilizzo di OCSP (Online Certificate Status Protocol).

RESET MQSSL

La variabile di ambiente **MQSSLRESET** specifica il numero di byte non codificati inviati e ricevuti su un canale TLS prima che la chiave segreta TLS venga rinegoziata. Può essere impostato su un numero 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 TLS compreso nell'intervallo tra 1 byte e 32 KB, i canali TLS utilizzano un conteggio di reimpostazione della chiave segreta di 32 KB. Questo conteggio di reimpostazioni segrete evita un numero eccessivo di reimpostazioni di chiavi che si verificherebbe per valori di reimpostazione di chiavi segrete TLS di piccole dimensioni.

Per impostare **MQSSLRESET**, utilizzare uno dei seguenti comandi:

- Linux UNIX Su sistemi UNIX and Linux:

```
export MQSSLRESET=integer
```

- Windows Su sistemi Windows:

```
SET MQSSLRESET=integer
```

- IBM i Su IBM i:

```
ADDENVVAR ENVVAR(MQSSLRESET) VALUE(integer)
```

Per ulteriori informazioni, vedi Reimpostazione delle chiavi segrete SSL e TLS.

MQSUITEB

ULW

Puoi configurare IBM MQ per operare in conformità con lo standard NSA Suite B su piattaforme UNIX, Linux, and Windows .

La variabile di ambiente **MQSUITEB** specifica se deve essere utilizzata la crittografia conforme a Suite B. Se deve essere utilizzata la crittografia Suite B, è possibile specificare la potenza della crittografia impostando **MQSUITEB** su uno dei seguenti valori:

- Nessuna
- 128_BIT, 192_BIT
- 128_BIT
- 192_BIT

È possibile specificare più valori utilizzando un elenco separato da virgole. L'utilizzo del valore NONE con qualsiasi altro valore non è valido.

Per ulteriori informazioni, vedi Configurazione di IBM MQ per Suite B.

MQTCPTIMEOUT

La variabile di ambiente **MQTCPTIMEOUT** specifica per quanto tempo IBM MQ attende una chiamata di connessione TCP.

ODQ_MSG

Se si utilizza un gestore code di messaggi non recapitabili diverso da quello di **runmqdlq**, l'origine dell'esempio, `amqsdlq`, è disponibile per l'utilizzo come base. L'esempio è simile al gestore di lettere non recapitate fornito all'interno del prodotto, ma la traccia e la notifica degli errori sono differenti. Utilizzare la variabile di ambiente **ODQ_MSG** per impostare il nome del file contenente i messaggi di errore e di informazioni. Il file fornito è denominato `amqsdlq.msg`.

Per ulteriori informazioni, vedere Esempio di gestore code di messaggi non instradabili.

TRACCIA_ODQ

Se si utilizza un gestore code di messaggi non recapitabili diverso da quello di **runmqdlq**, l'origine dell'esempio, amqsdlq, è disponibile per l'utilizzo come base. L'esempio è simile al gestore di lettere non recapitate fornito all'interno del prodotto, ma la traccia e la notifica degli errori sono differenti. Per abilitare la traccia, impostare la variabile di ambiente **ODQ_TRACE** su YES o yes.

Per ulteriori informazioni, vedere Esempio di gestore code di messaggi non instradabili.

ID_PERCORSO

La variabile di ambiente **OMQ_PATH** specifica dove è possibile trovare il report Sintomo primo errore se le classi di automazione IBM MQ per lo script ActiveX hanno esito negativo.

TRACCIA QUERY

Le classi di automazione IBM MQ per ActiveX (MQAX) includono una funzione di traccia che consente al supporto IBM di identificare cosa accade quando si verifica un problema. Mostra i percorsi presi quando si esegue lo script MQAX. A meno che non si abbia un problema, eseguire l'esecuzione con la traccia disattivata per evitare un uso non necessario delle risorse di sistema. **OMQ_TRACE** è una delle tre variabili di ambiente impostate per controllare la traccia. La specifica di qualsiasi valore per **OMQ_TRACE** attiva la funzione di traccia. Anche se si imposta **OMQ_TRACE** su OFF, la funzione di traccia è ancora attiva.

Per ulteriori informazioni, consultare Controllo della traccia per le classi di automazione IBM MQ per ActiveX.

LIVELLO_TRACCIA_OMQ_

OMQ_TRACE_LEVEL è una delle tre variabili di ambiente impostate per controllare la traccia per le classi di automazione IBM MQ per ActiveX. Imposta il livello di traccia richiesto. I valori maggiori di 9 non producono ulteriori informazioni nel file di traccia.

Per ulteriori informazioni, consultare Controllo della traccia per le classi di automazione IBM MQ per ActiveX.

PERCORSO_TRACCIA_OMQ

OMQ_TRACE_PATH è una delle tre variabili di ambiente impostate per controllare la traccia per le classi di automazione IBM MQ per ActiveX. Imposta la directory di traccia in cui viene scritto il file di traccia.

Per ulteriori informazioni, consultare Controllo della traccia per le classi di automazione IBM MQ per ActiveX.

ONCONFIG

La variabile di ambiente di **ONCONFIG** specifica il nome del file di configurazione del server Informix . Ad esempio, sui sistemi UNIX and Linux , utilizzare:

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

Sui sistemi Windows , utilizzare quanto segue:

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

Per ulteriori informazioni, vedi Configurazione di Informix.

WCF_TRACE_ON

Sono disponibili due diversi metodi di traccia per il canale personalizzato WCF. Questi due metodi di traccia vengono attivati indipendentemente o insieme. Ogni metodo produce il proprio file di traccia, quindi quando entrambi i metodi di traccia sono stati attivati, vengono generati due file di output di traccia. Esistono quattro combinazioni per abilitare e disabilitare i due diversi metodi di traccia. Oltre a queste combinazioni per abilitare la traccia WCF, la traccia XMS .NET può essere abilitata utilizzando la variabile di ambiente **WCF_TRACE_ON** .

Per ulteriori informazioni, vedi Traccia del canale personalizzato WCF per IBM MQ.

HOME WMQSOAP

La variabile di ambiente **WMQSOAP_HOME** viene utilizzata quando si completano ulteriori operazioni di configurazione dopo che l'ambiente di hosting del servizio .NET SOAP over JMS è stato installato e configurato correttamente in IBM MQ. È accessibile da un gestore code locale.

Per ulteriori informazioni, vedi Client WCF a un servizio .NET ospitato dall'esempio IBM MQ e Client WCF a un servizio Axis Java ospitato dall'esempio IBM MQ.

XMS_TRACE_ON, XMS_TRACE_FILE_PATH, XMS_TRACE_FORMAT e XMS_TRACE_SPECIFICATION

Se si utilizza IBM MQ classes for XMS .NET Framework, è possibile configurare la traccia da un file di configurazione dell'applicazione e dalle variabili di ambiente XMS .

V 9.1.1 Se si utilizza IBM MQ classes for XMS .NET Standard, è necessario configurare la traccia dalle variabili di ambiente XMS . La traccia viene normalmente utilizzata sotto la guida del supporto IBM .

Per abilitare e configurare la traccia per un'applicazione XMS .NET , impostare le seguenti variabili di ambiente prima di eseguire l'applicazione:

TRACE_XMS ON
: Se la variabile di ambiente **XMS_TRACE_ON** è impostata, tutta la traccia è abilitata per impostazione predefinita.

PERCORSO_FILE_TRACCIA_X
: La variabile di ambiente **XMS_TRACE_FILE_PATH** specifica il nome percorso completo della directory in cui vengono scritti i record FFDC e di traccia, se si desidera che tali record vengano scritti in un'ubicazione alternativa dalla directory di lavoro corrente.

FORMATO_TRACCIA_XMS
: La variabile di ambiente **XMS_TRACE_FORMAT** specifica il formato di traccia richiesto, che può essere `BASIC` o `ADVANCED`.

SPECIFICA_TRACCIA_XMS
: La variabile di ambiente **XMS_TRACE_SPECIFICATION** sostituisce le impostazioni di traccia definite nella sezione Traccia di un file di configurazione dell'applicazione. **XMS_TRACE_SPECIFICATION** si applica solo a IBM MQ classes for XMS .NET Framework .

Per ulteriori informazioni, vedi Traccia delle applicazioni XMS .NET e Traccia delle applicazioni XMS .NET utilizzando le XMS variabili di ambiente.

Attività correlate

“Utilizzo delle variabili d'ambiente IBM MQ” a pagina 62
È possibile utilizzare i comandi per visualizzare le impostazioni correnti o per reimpostare i valori delle variabili di ambiente IBM MQ .

Multi Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms

È possibile modificare il comportamento di IBM MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione modificando le informazioni nei file di configurazione (`.ini`). È anche possibile modificare le opzioni di configurazione per IBM MQ MQI clients.

Informazioni su questa attività

È possibile modificare le informazioni di configurazione di IBM MQ a livello del nodo o del gestore code modificando i valori specificati in una serie di attributi di configurazione (o parametri) che gestiscono IBM MQ.

Un file di configurazione (o file di 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. È possibile modificare gli attributi di configurazione IBM MQ nei seguenti file di configurazione:

IBM MQ file di configurazione, `mqs.ini`
Il file `mqs.ini` influenza le modifiche sul nodo nel suo insieme. Esiste un file `mqs.ini` per ogni installazione di IBM MQ .

Poiché il file di configurazione IBM 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 MQ .

File di configurazione del gestore code, `qm.ini`
Il file `qm.ini` influisce sulle modifiche per specifici gestori code. È presente un file `qm.ini` per ogni gestore code sul nodo.

IBM MQ MQI client file di configurazione, mqclient.ini
Le opzioni di configurazione per il IBM MQ MQI clients vengono conservate separatamente, nel file di configurazione del client, generalmente denominato `mqclient.ini`.

File di configurazione della traccia attività, mqat.ini
Il file `mqat.ini` viene utilizzato per configurare il comportamento della traccia dell'attività.

Potrebbe essere necessario modificare un file di configurazione se, ad esempio:

- Si perde un file di configurazione. (Recuperarlo dal backup, se possibile.)
- È necessario spostare uno o più gestori code in una nuova directory.
- È necessario modificare il gestore code predefinito. Ciò può verificarsi se si elimina accidentalmente il gestore code esistente.
- Si consiglia di farlo dal supporto IBM .

Importante: Le modifiche apportate a un file di configurazione di solito non diventano effettive fino al successivo avvio del gestore code.

Punti da notare sulla modifica dei file di configurazione:

- I valori degli attributi di un file di configurazione sono impostati in base alla seguente priorità:
  - I parametri immessi sulla riga comandi 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` .
- Dopo l'installazione, è possibile modificare i valori predefiniti nei file di configurazione IBM MQ .
- Quando si esegue il backup di un gestore code, ricordarsi di includere sia il relativo file di configurazione (`qm.ini`) che il file di configurazione centrale IBM MQ (`mqs.ini`).

- Se si imposta un valore non corretto su un attributo del file di configurazione, l'effetto è lo stesso di perdere completamente l'attributo. Il valore viene ignorato e viene emesso un messaggio operatore per indicare il problema.
- IBM i Su IBM i, i file `.ini` sono file di flusso residenti in IFS.
- Esistono diverse regole di sintassi per il formato del file `mqat.ini` . Per ulteriori informazioni, consultare la traccia delle attività dell'applicazione Configurazione del comportamento della traccia delle attività utilizzando `mqat.ini`.

ULW Su UNIX o Linux, il file di configurazione dell'installazione, `mqinst.ini`, contiene informazioni su tutte le installazioni IBM MQ . Il file `mqinst.ini` non deve essere modificato o a cui si fa riferimento direttamente poiché il formato non è fisso e potrebbe essere modificato. Invece, è necessario modificarlo utilizzando i comandi. Per ulteriori informazioni, consultare “File di configurazione dell'installazione, mqinst.ini” a pagina 145.

Procedura

1. Prima di modificare un file di configurazione, eseguirne il backup in modo da disporre di una copia a cui è possibile tornare, se necessario.
2. Modificare il file di configurazione `.ini` in uno dei seguenti modi:
   - Manualmente utilizzando un editor di testo standard. 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 "\" . Il carattere viene quindi utilizzato come parte dei dati di configurazione.
   - Automaticamente, utilizzando i comandi che modificano la configurazione dei gestori code sul nodo. Per ulteriori informazioni, consultare Riferimento comandi.

     Windows Ad esempio, il Windows comando specifico **amqmdain** aggiornerà automaticamente una serie secondaria delle proprietà `qm.ini` . Per ulteriori informazioni, consultare amqmdain.
   - Linux Windows Su Linux (x86 e x86-64) e su Windows, è possibile aggiornare un sottoinsieme delle proprietà `qm.ini` utilizzando IBM MQ Explorer. Per ulteriori informazioni, fare riferimento a Configurazione di IBM MQ utilizzando MQ Explorer.

     Nota: Poiché ci sono implicazioni significative per la modifica dei servizi installabili e dei loro componenti, i servizi installabili sono di sola lettura in IBM MQ Explorer. Pertanto, è necessario apportare eventuali modifiche ai servizi installabili modificando il file `qm.ini` . Per ulteriori informazioni, consultare “Stanza di servizio del file qm.ini” a pagina 131.

Attività correlate

AmministrazioneIBM MQ

Multi File di configurazione IBM MQ , mqs.ini

Il file di configurazione IBM MQ , `mqs.ini`, contiene informazioni relative a tutti i gestori code sul nodo. Viene creato automaticamente durante l'installazione.

Nota: Per ulteriori informazioni su come e quando modificare il file `mqs.ini` e su quando le modifiche apportate al file diventano effettive, consultare “Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms” a pagina 83.

Percorsi di directory

Linux UNIX Su UNIX and Linux, la directory di dati e la directory di log sono sempre `/var/mqm` e `/var/mqm/log` rispettivamente.

Windows Sui sistemi Windows , l'ubicazione della directory di dati `mqs.ini`e l'ubicazione della directory di log sono memorizzate nel registro, poiché la loro ubicazione può variare. Le informazioni di configurazione dell'installazione, contenute in sistemi `mqinst.ini` su UNIX and Linux , si trovano anche nel Registro di sistema, poiché non vi è alcun file `mqinst.ini` in Windows (consultare "File di configurazione dell'installazione, mqinst.ini" a pagina 145).

Windows Il file `mqs.ini` per i sistemi Windows viene fornito dal WorkPath specificato nella chiave `HKLM\SOFTWARE\IBM\IBM MQ` . Contiene:

- I nomi dei gestori code
- Il nome del gestore code predefinito
- L'ubicazione dei file associati a ciascuno di essi

IBM i Su IBM i, il file `mqs.ini` è memorizzato in `/QIBM/UserData/mqm`. Il file contiene:

- I nomi dei gestori code.
- Il nome del gestore code predefinito.
- L'ubicazione dei file associati a ciascun gestore code.
- Informazioni che identificano le uscite API (per ulteriori informazioni, consultare Configurazione delle uscite API).

In particolare, il file `mqs.ini` viene utilizzato per individuare i dati associati a ciascun gestore code.

File `mqs.ini` di esempio per UNIX and Linux

Linux UNIX

```
#********************************************************************#
#* Module Name: mqs.ini                                             *#
#* Type       : IBM MQ Machine-wide Configuration File              *#
#* Function   : Define IBM MQ resources for an entire machine       *#
#********************************************************************#
#* Notes      :                                                     *#
#* 1) This is the installation time default configuration           *#
#*                                                                  *#
#********************************************************************#
AllQueueManagers:
#********************************************************************#
#* The path to the qmgrs directory, below which queue manager data  *#
#* is stored                                                        *#
#********************************************************************#
DefaultPrefix=/var/mqm

LogDefaults:
   LogPrimaryFiles=3
   LogSecondaryFiles=2
   LogFilePages=4096
   LogType=CIRCULAR
   LogBufferPages=0
   LogDefaultPath=/var/mqm/log

QueueManager:
   Name=saturn.queue.manager
   Prefix=/var/mqm
   Directory=saturn!queue!manager
   InstallationName=Installation1

QueueManager:
   Name=pluto.queue.manager
   Prefix=/var/mqm
   Directory=pluto!queue!manager
   InstallationName=Installation2

DefaultQueueManager:
   Name=saturn.queue.manager

ApiExitTemplate:
   Name=OurPayrollQueueAuditor
   Sequence=2
```

```
   Function=EntryPoint
   Module=/usr/ABC/auditor
   Data=123

ApiExitCommon:
   Name=MQPoliceman
   Sequence=1
   Function=EntryPoint
   Module=/usr/MQPolice/tmqp
   Data=CheckEverything
```

File `mqs.ini` di esempio per Windows

Windows

```
#********************************************************************#
#* Module Name: mqs.ini                                             *#
#* Type       : IBM MQ Machine-wide Configuration File              *#
#* Function   : Define IBM MQ resources for an entire machine       *#
#********************************************************************#
#* Notes      :                                                     *#
#* 1) This is the installation time default configuration           *#
#*                                                                  *#
#********************************************************************#
AllQueueManagers:
#********************************************************************#
#* The path to the qmgrs directory, below which queue manager data  *#
#* is stored                                                        *#
#********************************************************************#
DefaultPrefix=C:\ProgramData\IBM\MQ

LogDefaults:
   LogPrimaryFiles=3
   LogSecondaryFiles=2
   LogFilePages=4096
   LogType=CIRCULAR
   LogBufferPages=0
   LogDefaultPath=C:\ProgramData\IBM\MQ\log

QueueManager:
   Name=saturn.queue.manager
   Prefix=C:\ProgramData\IBM\MQ
   Directory=saturn!queue!manager
   InstallationName=Installation1

QueueManager:
   Name=pluto.queue.manager
   Prefix=C:\ProgramData\IBM\MQ
   Directory=pluto!queue!manager
   InstallationName=Installation2

DefaultQueueManager:
   Name=saturn.queue.manager

ApiExitTemplate:
   Name=OurPayrollQueueAuditor
   Sequence=2
   Function=EntryPoint
   Module=C:\usr\ABC\auditor
   Data=123

ApiExitCommon:
   Name=MQPoliceman
   Sequence=1
   Function=EntryPoint
   Module=C:\usr\MQPolice\tmpq
   Data=CheckEverything
```

File `mqs.ini` di esempio per IBM i

IBM i

```
#********************************************************************#
#* Module Name: mqs.ini                                             *#
```

```
#* Type       : IBM MQ Configuration File                                *#
#* Function   : Define IBM MQ resources for the node                     *#
#*                                                                       *#
#************************************************************************#
#* Notes      :                                                          *#
#* 1) This is an example IBM MQ configuration file                       *#
#*                                                                       *#
#************************************************************************#
AllQueueManagers:
#************************************************************************#
#* The path to the qmgrs directory, within which queue manager data     *#
#* is stored                                                            *#
#************************************************************************#
DefaultPrefix=/QIBM/UserData/mqm

QueueManager:
Name=saturn.queue.manager
Prefix=/QIBM/UserData/mqm
Library=QMSATURN.Q
Directory=saturn!queue!manager

QueueManager:
Name=pluto.queue.manager
Prefix=/QIBM/UserData/mqm
Library=QMPLUTO.QU
Directory=pluto!queue!manager

DefaultQueueManager:
Name=saturn.queue.manager
```

Note:

1. IBM MQ sul nodo utilizza le ubicazioni predefinite per i gestori code e i journal.
2. Il gestore code saturn.queue.manager è il gestore code predefinito per il nodo. La directory per i file associati a questo gestore code è stata automaticamente trasformata in un nome file valido per il filesystem.
3. Poiché il file di configurazione IBM 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 IBM MQ . Inoltre, le applicazioni non possono connettersi a un gestore code che non è definito nel file di configurazione IBM MQ .

stanze `mqs.ini`

Attenzione: Questo argomento si collega a ulteriori informazioni sulle stanze nel file `mqs.ini` . Ogni stanza contiene informazioni sui parametri in quella stanza.

Multi Riepilogo delle stanze e degli attributi del file mqs.ini

Un riepilogo degli attributi delle stanze del IBM MQ file di configurazione, `mqs.ini`, con link a ulteriori informazioni.

Tabella 9. Stanze del file mqs.ini	
Stanza e attributi	**Descrizione degli attributi**
Stanza AllQueueManagers	
DefaultPrefix	Il percorso della directory `qmgrs` , all'interno della quale vengono conservati i dati del gestore code.
ULW V 9.1.3 DefaultEphemeralpredefinito	Il percorso della directory in cui vengono conservati i dati effimeri del gestore code.
Multi ConvEBCDICNewline	Come IBM MQ deve convertire il carattere EBCDIC NL in formato ASCII
ApiExitStanza comune e stanza ApiExitTemplate	

Tabella 9. Stanze del file mqs.ini (Continua)	
Stanza e attributi	**Descrizione degli attributi**
Nome	Il nome descrittivo dell'uscita API inoltrato nel campo Nome ExitInfodella struttura MQAXP.
funzione	Il nome del punto di ingresso della funzione nel modulo contenente il codice di uscita API.
Modulo	Il modulo contenente il codice di uscita API.
Dati	I dati da passare all'uscita API nel campo ExitData della struttura MQAXP.
Sequenza	La sequenza in cui questa uscita API viene richiamata rispetto ad altre uscite API.
Stanza del gestoreDefaultQueue	
Nome	Il nome del gestore code che elabora i comandi per cui un nome gestore code non è specificato esplicitamente.
Stanza ExitProperties	
CLWLMode	Indica se l'uscita CLWL (cluster workloac) viene eseguita in modalità FAST o SAFE.
Stanza LogDefaults	
LogPrimaryFiles	I file di log assegnati quando viene creato il gestore code.
LogSecondaryFiles	I file di log assegnati quando i file primari sono esauriti.
LogFilePages	Il numero di pagine del file di log. (La dimensione del file di log è specificata in unità di pagine da 4 KB.)
LogType	Il tipo di registrazione che deve essere utilizzato dal gestore code (circolare o lineare).
LogBufferPages	La quantità di memoria assegnata ai record buffer per la scrittura, specificando la dimensione dei buffer in unità di pagine da 4 KB.
LogDefaultPath	La directory in cui risiedono i file di log per un gestore code.
LogWriteIntegrity	Il metodo utilizzato dal programma di registrazione per scrivere in modo affidabile i record di log.
StanzaQueueManager	
Nome	Il nome del gestore code.
prefisso	La posizione in cui sono memorizzati i file del gestore code.
Directory	Il nome della sottodirectory nella directory `prefix\QMGRS` in cui sono memorizzati i file del gestore code.
DataPath	Un percorso dati esplicito fornito quando è stato creato il gestore code, sostituisce Prefisso e Directory come percorso dei dati del gestore code.
InstallationName	Il nome dell'installazione IBM MQ associato a questo gestore code.

Tabella 9. Stanze del file mqs.ini (Continua)	
Stanza e attributi	**Descrizione degli attributi**
V 9.1.3 EphemeralPrefix	Dove vengono memorizzati i dati effimeri del gestore code.
HA	Presente per i gestori code HA e DR/HA replicati, il valore è `Replicated`. L''attributo viene aggiunto quando il gestore code viene creato e non deve essere modificato.
DR	Presente per gestori code di dati replicati DR/HA, il valore è `Replicated`. L''attributo viene aggiunto quando il gestore code viene creato e non deve essere modificato.
Ruolo DRR	Presente per gestori code di dati replicati DR e indica il ruolo DR corrente del gestore code. L'attributo viene aggiunto quando il gestore code viene creato e aggiornato da IBM MQ. Non deve essere modificato manualmente.

Multi Stanza AllQueueManagers del file mqs.ini

La stanza AllQueueManagers può specificare il percorso della directory `qmgrs` in cui sono memorizzati i file associati a un gestore code, il percorso della libreria eseguibile e il metodo di conversione dei dati in formato EBCDIC in formato ASCII.

Utilizzare la stanza AllQueueManagers nel file `mqs.ini` per specificare le informazioni su tutti i gestori code.

Linux Windows In alternativa, in Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà IBM MQ Explorer `General` e `Extended` IBM MQ .

DefaultPrefix= *nome_directory*
Questo attributo specifica il percorso della directory `qmgrs` , in cui 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 IBM MQ prima di modificare il prefisso predefinito e riavviare IBM MQ solo dopo aver spostato le strutture nella nuova posizione e aver modificato il prefisso predefinito.

Nota: ULW Non eliminare la directory `/var/mqm/errors` su sistemi UNIX and Linux o la directory `\errors` su 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.

ULW V 9.1.3 **DefaultEphemeralPrefisso = *nome_directory***
Questo attributo specifica il percorso della directory, all'interno della quale vengono conservati i dati temporanei del gestore code, come i socket IPC, e viene utilizzato solo per impostare il `EphemeralPrefix` di un gestore code quando viene creato un gestore code. Inoltre, è necessario creare la directory se si modifica il valore predefinito.

È necessario creare la directory di dati effimeri con le autorizzazioni che consentono al gruppo IBM MQ di accedere alla scrittura in tale directory.

Come alternativa alla modifica del file `mqs.ini` , è possibile utilizzare la variabile di ambiente **`MQ_EPHEMERAL_PREFIX`** per sovrascrivere **`DefaultEphemeralPrefix`** per il comando **`crtmqm`** .

A causa delle limitazioni del sistema operativo, il prefisso temporaneo predefinito è limitato a 12 caratteri su UNIX and Linux piattaforme.

`DefaultEphemeralPrefix` non è supportato su IBM MQ Appliance o su IBM i.

Multi **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 IBM MQ deve convertire il carattere EBCDIC NL in formato ASCII.

IBM i Su IBM MQ for IBM i, CCSID 1253 viene considerato come un CCSID ISO e NL_TO_LF influisce sulle conversioni ISO e ASCII.

z/OS L'attributo **`ConvEBCDICNewline`** non è disponibile su z/OS. Il comportamento su z/OS equivale a `ConvEBCDICNewline=TABLE`. Notare che il valore predefinito su altre piattaforme potrebbe essere diverso.

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 sono mostrati in Tabella 10 a pagina 90.

Tabella 10. 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
1051	roman8

Se il CCSID ASCII non è un sottoinsieme ISO, **ConvEBCDICNewline** assume il valore predefinito NL_TO_LF.

V 9.1.2 V 9.1.0.2 Da IBM MQ 9.1.0 Fix Pack 2 e IBM MQ 9.1.2, è possibile utilizzare la variabile di ambiente **AMQ_CONVEBCDICNEWLINE** invece dell'attributo della stanza **ConvEBCDICNewline** , ad esempio per fornire la funzionalità **ConvEBCDICNewline** sul lato client in situazioni in cui non è possibile utilizzare il file mqs.ini . La variabile di ambiente assume gli stessi valori (NL_TO_LF, TABLEo ISO) dell'attributo **ConvEBCDICNewline** . L'attributo stanza ha la precedenza se sono impostati sia l'attributo che la variabile di ambiente.

Multi Stanze del modello ApiExitCommon e ApiExitdel file mqs.ini

Il modello ApiExite le stanze comuni ApiExitidentificano le routine di uscita API per tutti i gestori code.

Utilizzare il modello ApiExite le stanze comuni ApiExitnel file mqs.ini per identificare le routine di uscita API per tutti i gestori code. (Per identificare le routine di uscita API per singoli gestori code, utilizzare la stanza ApiExitlocale, come descritto in “ApiExitStanza locale del file qm.ini” a pagina 108.)

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà di IBM MQ Explorer Exits IBM MQ .

Windows Su Windows, è anche possibile utilizzare il comando **amqmdain** per modificare le voci per le uscite API.

Per ulteriori informazioni sull'utilizzo di questi attributi, consultare Configurazione delle uscite API.

Nome=ApiExit_name
Il nome descrittivo dell'uscita API inoltrato nel campo Nome ExitInfodella struttura MQAXP.

Questo nome deve essere univoco, non deve superare i 48 caratteri e contenere solo caratteri validi per i nomi degli oggetti IBM MQ (ad esempio, nomi coda).

Funzione=nome_funzione
Il nome del punto di ingresso della funzione nel modulo contenente il codice di uscita API. Questo punto di ingresso è la funzione MQ_INIT_EXIT.

La lunghezza di questo campo è limitata a MQ_EXIT_NAME_LENGTH.

Modulo=nome_modulo
Il modulo contenente il codice di uscita API.

Se questo campo contiene il percorso completo del modulo, questo verrà visualizzato così come è. Se questo campo contiene solo il nome del modulo, il modulo si trova utilizzando l'attributo **ExitsDefaultPath** nella stanza ExitPath del file qm.ini .

Su piattaforme che supportano librerie separate, è necessario fornire sia una versione non con thread che una versione con thread del modulo di uscita API. La versione con thread deve avere un suffisso _r . La versione con thread dello stub dell'applicazione IBM MQ accoda implicitamente _r al nome modulo fornito prima che venga caricato.

La lunghezza di questo campo è limitata alla lunghezza massima del percorso supportata dalla piattaforma.

Dati=nome_dati
I dati da passare all'uscita API nel campo ExitData della struttura MQAXP.

Se si include questo attributo, vengono rimossi gli spazi iniziali e finali, la stringa rimanente viene troncata a 32 caratteri e il risultato viene passato all'uscita. Se si omette questo attributo, il valore predefinito di 32 spazi viene passato all'uscita.

La lunghezza massima di questo campo è 32 caratteri.

Sequenza=numero_sequenza
La sequenza in cui questa uscita API viene richiamata rispetto ad altre uscite API. Un'uscita con un numero di sequenza basso viene richiamata prima di un'uscita con un numero di sequenza più alto. Non è necessario che la numerazione di sequenza delle uscite sia contigua. Una sequenza di 1, 2, 3 ha lo stesso risultato di una sequenza di 7, 42, 1096. Se due uscite hanno lo stesso

numero di sequenza, il gestore code decide quale richiamare per primo. È possibile determinare quale elemento è stato richiamato dopo l'evento inserendo l'ora o un indicatore nell'area ExitChainindicata da ExitChainAreaPtr in MQAXP oppure scrivendo il proprio file di log.

Questo attributo è un valore numerico senza segno.

Multi Stanza del gestore DefaultQueuedel file mqs.ini

La stanza DefaultQueueManager specifica il gestore code predefinito per il nodo.

Utilizzare la stanza Gestore DefaultQueuenel file `mqs.ini` per specificare il gestore code predefinito.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la IBM MQ Explorer pagina delle proprietà `General` IBM MQ .

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`** .

Multi Stanza ExitProperties del file mqs.ini

La stanza ExitProperties specifica le opzioni di configurazione utilizzate dai programmi di uscita del gestore code.

Utilizzare la stanza ExitProperties nel file `mqs.ini` per specificare opzioni di configurazione utilizzate dai programmi di uscita del gestore code.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà di IBM MQ Explorer `Extended` IBM MQ .

CLWLMode= SAFE (predefinito) | FAST

L'uscita del carico di lavoro cluster (CLWL) consente di specificare quale coda cluster nel cluster aprire in risposta 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 cluster viene eseguita in modalità SAFE.

SICURA

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 potrebbe 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.

Multi Stanza LogDefaults del file mqs.ini

La stanza LogDefaults specifica le informazioni sui valori predefiniti di log per tutti i gestori code.

Utilizzare la stanza LogDefaults nel file `mqs.ini` per specificare le informazioni sui valori predefiniti di log per tutti i gestori code.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà di IBM MQ Explorer `Default log settings` IBM MQ .

Se la stanza non esiste, vengono utilizzati i valori predefiniti IBM 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** . Per ulteriori informazioni su questo comando, consultare **crtmqm**.

Una volta creato un gestore code, gli attributi di log per tale gestore code vengono ricavati dalle impostazioni descritte in “Stanza di log del file qm.ini” a pagina 125.

Nota: La stanza LogDefaults fornita per una nuova installazione IBM 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 per la stanza LogDefaults sono riportati in “File mqs.ini di esempio per UNIX and Linux” a pagina 85 e “File mqs.ini di esempio per Windows” a pagina 86. Un valore zero per l'attributo `LogBufferPages` indica 512.

Il prefisso predefinito, specificato in “Stanza AllQueueManagers del file mqs.ini” a pagina 89, e il percorso di log specificato per il particolare gestore code, specificato in “Stanza di log del file qm.ini” a pagina 125, consentono al gestore code e al relativo log di trovarsi su 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 599.

Nota: I limiti forniti nel seguente elenco di parametri sono limiti impostati da IBM MQ. I limiti del sistema operativo potrebbero ridurre la dimensione massima possibile del log.

LogPrimaryFiles = 3 (predefinito) |*2-254* (Windows) |*2 - 510* (UNIX 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 numero massimo è 254 su Windowso 510 su 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 UNIX and Linuxe 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 (predefinito) |*1-253* (Windows) |*1-509* (UNIX 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 numero massimo è 253 su Windowso 509 su 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 UNIX and Linuxe 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.

LogFilePagine = *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 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 (valore predefinito) | LINEAR
Il tipo di log da utilizzare. Il valore predefinito è `CIRCULAR`.

CIRCOLARE
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 594 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 594 per una spiegazione più completa della registrazione lineare.

Se si desidera modificare il valore predefinito, è possibile modificare l'attributo LogType oppure specificare la registrazione lineare utilizzando il comando **crtmqm** .

V 9.1.0 Da IBM MQ 9.1.0, è possibile modificare il metodo di registrazione dopo che è stato creato un gestore code. Per ulteriori informazioni, consultare migmqlog.

LogBufferPagine = 0 (valore predefinito) |*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 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:

- Windows *DefaultPrefix*\log per IBM MQ for Windows dove *DefaultPrefix* è il valore specificato nell'attributo DefaultPrefix nella pagina delle proprietà di All Queue Managers IBM MQ . Questo valore è impostato al momento dell'installazione.
- Linux UNIX /var/mqm/log per sistemi UNIX e 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 (predefinito)
Il metodo utilizzato dal programma di registrazione per scrivere in modo affidabile i record di log.

TripleWrite (predefinito)
È il metodo predefinito.

Nota: è possibile selezionare **DoubleWrite** ma, in tal caso, il sistema l'interpreta come **TripleWrite**.

SingleWrite
Si consiglia di utilizzare **SingleWrite**, solo se il file - system e il dispositivo che ospita il log di recupero IBM MQ garantiscono esplicitamente l'atomicità delle scritture 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.

Nota: Se è presente una simultaneità sufficiente nel tuo carico di lavoro persistente, c'è un vantaggio potenziale minimo nell'impostazione di un valore diverso da quello predefinito, **TripleWrite**.

Per ulteriori informazioni, consultare “LogWriteIntegrity - utilizzando SingleWrite o TripleWrite” a pagina 128.

Multi Stanza QueueManager del file mqs.ini

La stanza QueueManager specifica l'ubicazione della directory del gestore code.

Esiste una stanza QueueManager per ogni gestore code. Gli attributi di questa stanza 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. Per ulteriori informazioni sulla trasformazione dei nomi, consultare Informazioni sui nomi file IBM MQ.

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 uguale al valore specificato nell'attributo **DefaultPrefix** della sezione Tutti i gestori code nel file `mqs.ini` .

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 al momento della creazione del gestore code, sovrascrive **Prefix** e **Directory** come percorso dei dati del gestore code.

InstallationName= *nome*
Il nome dell'installazione IBM MQ associato a questo gestore code. I comandi da questa installazione devono essere utilizzati quando si interagisce con questo gestore code.

IBM i **Libreria = *nome***
Il nome della libreria in cui sono memorizzati gli oggetti IBM i pertinenti a questo gestore code, ad esempio i giornali e i ricevitori di journal. 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 libreria valido.

ULW V 9.1.3 **EphemeralPrefix= *nome***

Dove vengono memorizzati i dati effimeri del gestore code.

Per impostazione predefinita, questo valore non è presente, il che significa che i dati vengono memorizzati nell'ubicazione Prefisso.

Il valore viene impostato dal valore della variabile di ambiente **MQ_EPHEMERAL_PREFIX** o dall'attributo **DefaultEphemeralPrefix** della stanza AllQueueManagers nel file `mqs.ini` , quando il gestore code viene creato.

Attività correlate

“Associazione di un gestore code a un'installazione” a pagina 432

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** .

Windows API (Advanced Configuration and Power Interface)

Windows supporta lo standard ACPI (Advanced Configuration and Power Interface). Ciò consente agli utenti Windows con hardware abilitato ACPI di arrestare e riavviare i canali quando il sistema entra e riprende dalla modalità di sospensione.

Utilizzare la pagina delle proprietà di ACPI IBM MQ da IBM MQ Explorer, per specificare il modo in cui IBM MQ deve comportarsi quando il sistema riceve una richiesta di sospensione.

Tenere presente che le impostazioni specificate nella pagina delle proprietà di ACPI IBM 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 (vedere 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 finestra di 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.

Multi File di configurazione del gestore code, qm.ini

Un file di configurazione del gestore code, `qm.ini`, contiene informazioni relative a uno specifico 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.

Nota: Per ulteriori informazioni su come e quando modificare un file `qm.ini` e su quando le modifiche apportate al file diventano effettive, consultare “Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms” a pagina 83.

Da IBM MQ 9.0.4 e IBM MQ 9.0.0 Fix Pack 2, 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 vedere cosa non è corretto e correggerlo rapidamente se **strmqm** rileva che il file `qm.ini` contiene errori. Per ulteriori informazioni, vedere strmqm.

Ubicazione dei file `qm.ini`

Linux UNIX Sui sistemi UNIX and Linux , un file di `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
```

Windows Su sistemi Windows , l'ubicazione del file `qm.ini` viene fornita dal WorkPath specificato nella chiave `HKLM\SOFTWARE\IBM\WebSphere MQ` . Ad esempio, il percorso e il nome per un file di configurazione per un gestore code denominato QMNAME è il seguente:

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

IBM i Un file `qm.ini` viene conservato in *mqmdata directory*`/`*QMNAME*`/qm.ini`, dove *mqmdata directory* è `/QIBM/UserData/mqm` per impostazione predefinita e *QMNAME* è il nome del gestore code a cui si applica il file di inizializzazione.

Nota: È possibile modificare *mqmdata directory* nel file `mqs.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 IBM MQ file names e Object names on IBM i.

stanze qm.ini

Attenzione:

- Questo argomento si collega a ulteriori informazioni sulle stanze nel file qm.ini . Ogni stanza contiene informazioni sui parametri presenti in quella stanza, incluso un esempio dove appropriato.
- Ogni stanza mostra la piattaforma, o le piattaforme, di IBM MQ for Multiplatforms a cui si applica tale stanza.

Multi V 9.1.4 Configurazione automatica di qm.ini all'avvio

Da IBM MQ 9.1.4, è possibile configurare il proprio gestore code per applicare automaticamente il contenuto di un file o di una serie di file, contenenti le sovrascritture qm.ini , ad ogni avvio del gestore code.

È possibile utilizzarlo per avere una configurazione che può essere modificata e riprodotta automaticamente al successivo riavvio del gestore code. Ad esempio, se le sovrascritture di qm.ini si trovano su un'unità montata, è possibile disporre di una configurazione centralizzata in cui l'ultima versione viene applicata a ogni gestore code all'avvio.

È possibile utilizzare questa funzionalità per semplificare la creazione di un cluster uniforme, utilizzando la funzionalità cluster automatica. Per un esempio, consultare Creazione di un cluster uniforme da IBM MQ 9.1.4.

Nota: Queste sovrascritture vengono applicate solo all'avvio del gestore code e non possono influenzare la creazione del gestore code. Ad esempio, non è possibile impostare il numero di file di log primari con questa funzione.

Prima di iniziare

È possibile utilizzare:

1. Un singolo file e creare un file di testo contenente le modifiche al file qm.ini .
2. Un insieme di file di formato qm.ini :
   - Per identificare una directory in cui esisteranno le configurazioni e
   - In tale directory, creare i file, ognuno con estensione .ini, ad esempio qminisettings.ini.

Il file, o i file, devono contenere solo la sezione e le impostazioni **attribute**=*value* per gli elementi che vengono modificati. Ad esempio, per aggiornare l'attributo **MaxChannels** nella stanza Channels, il file potrebbe contenere:

```
Channels:
 MaxChannels=1234
```

Tenere presente che nei file di sovrascrittura qm.ini , qualsiasi riga con prefisso # viene considerata come un commento.

Abilitazione della configurazione automatica degli attributi del file qm.ini

È possibile configurare un nuovo gestore code utilizzando l'indicatore **-ii** per il comando **crtmqm** e puntando a un file specifico o a una directory. Il valore fornito viene memorizzato nel file qm.ini nella stanza AutoConfig , come attributo **IniConfig**.

È possibile configurare un gestore code esistente per abilitare la configurazione MQSC automatica, aggiungendo l'attributo della stanza AutoConfig **IniConfig**, che punta a un file o a una directory validi. Ad esempio:

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

Come funziona la configurazione automatica?

Durante l'avvio del gestore code, la configurazione identificata dall'attributo della stanza AutoConfig **IniConfig** viene convalidata per garantire una sintassi valida, quindi memorizzata nella struttura ad albero dei dati del gestore code nella directory `autocfg` come un singolo file `cached.ini` .

Quando vengono elaborati più file da una directory, vengono elaborati in ordine alfabetico.

Durante il primo avvio del gestore code, l'impossibilità di leggere il file o la directory impedisce l'avvio del gestore code, con un messaggio di errore appropriato sia per la console che per il log degli errori del gestore code.

Al successivo riavvio, se il file o la directory a cui si fa riferimento non è leggibile, viene utilizzato il file precedentemente memorizzato nella cache e un messaggio scritto nel log degli errori del gestore code lo evidenzia.

Quando si utilizza il comando **strmqm** , il contenuto del file `cached.ini` viene applicato al file `qm.ini` come sovrascritture prima che venga richiamato il gestore code.

Ciò significa che per un gestore code in standby, le impostazioni vengono lette quando il comando **strmqm** viene elaborato, non quando il gestore code diventa attivo.

Come viene creato il file di sostituzione qm.ini ?

La prima volta che viene configurata la configurazione dell'inizializzazione automatica e il gestore code viene avviato, una copia del file `qm.ini` corrente viene copiata nella sottodirectory `autoconfig` all'interno della directory di dati del gestore code come `base_qm.ini`. Questa è considerata la linea di base da qui in poi.

Ad ogni avvio del gestore code, ossia all'ora **strmqm** , il file `qm.ini` attualmente attivo viene eliminato e sostituito con una copia di `base_qm.ini`. Quindi, la configurazione dal file `cached.ini` viene applicata a questo file.

Una volta che un gestore code è sotto il controllo della configurazione automatica, tutte le modifiche al file `qm.ini` devono essere eseguite tramite il file o i file a cui si fa riferimento utilizzando l'attributo **IniConfig** nella stanza AutoConfig .

Poiché il file `qm.ini` esistente viene rimosso all'avvio del gestore code, solo la configurazione nel file `qm.ini` fornito utilizzando l'attributo **IniConfig** viene applicata alla riga di base del gestore code.

Se una stanza o un attributo sono stati modificati tramite la configurazione di inizializzazione automatica nei precedenti avvii del gestore code, tali modifiche vengono rimosse a meno che non siano ancora identificate nel file o nei file identificati dall'attributo **IniConfig** .

A causa della ricreazione del file `qm.ini` all'avvio del gestore code, tutte le modifiche manuali al file `qm.ini` andranno perse. Se è necessario apportare una modifica persistente e non è possibile utilizzare l'attributo **IniConfig** per apportare tale modifica, è possibile effettuare una delle seguenti operazioni:

- Apportare la modifica al file `base_qm.ini` .
- Eliminare il file `base_qm.ini` .

  Se si elimina questo file, `base_qm.ini` viene ricreato al successivo avvio del gestore code, in base al contenuto corrente del file `qm.ini` . Questo *rarisce* tutte le modifiche correnti man mano che inizia la nuova baseline per il futuro.

Multi Riepilogo delle stanze e degli attributi del file qm.ini

Un riepilogo degli attributi delle stanze del file di configurazione del gestore code, `qmi.ini`, con link a ulteriori informazioni.

Tabella 11. Stanze del file qm.ini	
Stanza e attributi	**Descrizione degli attributi**
Windows **StanzaAccessMode**	
Windows gruppo di accesso [1]	Un gruppo di protezione Windows , i cui membri avranno accesso completo a tutti i file di dati del gestore code.
ApiExitStanza locale	
Nome	Il nome descrittivo dell'uscita API inoltrato nel campo Nome ExitInfodella struttura MQAXP.
funzione	Il nome del punto di ingresso della funzione nel modulo contenente il codice di uscita API.
Modulo	Il modulo contenente il codice di uscita API.
Dati	I dati da passare all'uscita API nel campo ExitData della struttura MQAXP.
Sequenza	La sequenza in cui questa uscita API viene richiamata rispetto ad altre uscite API.
V 9.1.4 **StanzaAutoCluster**	
V 9.1.4 Tipo	Il tipo di cluster automatico. L'unica opzione valida è Uniform, che rappresenta un cluster uniforme.
V 9.1.4 ClusterName	Il nome del cluster automatico.
V 9.1.4 RepositoryName1	Il nome del gestore code del primo repository completo nel cluster automatico.
V 9.1.4 Repository1Conname	Il valore del nome connessione (CONNAME) per il modo in cui i membri del cluster automatico devono connettersi al gestore code.
V 9.1.4 RepositoryName2	Il nome del gestore code per il secondo repository completo nel cluster automatico.
V 9.1.4 Repository2Conname	Il valore del nome connessione (CONNAME) per il modo in cui i membri del cluster automatico devono connettersi al gestore code.
V 9.1.4 **StanzaAutoConfig**	
V 9.1.4 Configurazione MQSC	Un percorso file completo o un percorso a una directory, in cui tutti i file `*.mqsc` vengono applicati al gestore code ad ogni avvio del gestore code.
V 9.1.4 IniConfig	Un percorso file completo o un percorso a una directory, in cui tutti i file `*.ini` vengono applicati al file `qm.ini` ad ogni avvio del gestore code.
Stanza Canali	
MaxChannels	Il numero massimo di canali correnti consentiti.

Tabella 11. Stanze del file qm.ini (Continua)	
Stanza e attributi	**Descrizione degli attributi**
MaxActiveChannels	Il numero massimo di canali che possono essere attivi in qualsiasi momento.
MaxInitiators	Il numero massimo di iniziatori.
MQIBindType	Il binding per le applicazioni.
PipeLineLength	Il numero massimo di thread simultanei che un canale utilizzerà.
AdoptNewMCA	Quali tipi di canali possono avere l'istanza del canale esistente arrestata in modo che una nuova istanza del canale possa essere avviata quando IBM MQ riceve una richiesta di avviare un canale, ma rileva che un'istanza del canale è già in esecuzione.
AdoptNewMCATimeout	La quantità di tempo, in secondi, per cui la nuova istanza del canale attende la fine della vecchia.
AdoptNewMCACheck	Il tipo di controllo richiesto quando si abilita l'attributo **AdoptNewMCA** .
V 9.1.0 ChlauthEarlyAdotta	L'ordine in cui vengono elaborate le regole di autenticazione della connessione e di autenticazione del canale.
PasswordProtection	Impostare le password protette nella struttura MQCSP, piuttosto che utilizzare TLS.
V 9.1.0 IgnoreSeqNumberMismatch	Controlla come il gestore code gestisce una mancata corrispondenza di numeri di sequenza durante l'avvio del canale.
Stanza Connessione	
DefaultBindDefaultBind	Se le applicazioni e il gestore code, che vengono eseguiti in processi separati, condividono alcune risorse o nessuna risorsa tra loro.
Stanza DiagnosticMessages	
Nome	Nome di una stanza.
Servizio	Un servizio che viene abilitato da questa sezione.
ExcludeMessage	I messaggi che non devono essere scritti nel log degli errori del gestore code.
SuppressMessage	Messaggi che devono essere scritti nel log degli errori del gestore code una sola volta in un intervallo di tempo specificato.
IBM i SuppressInterval	L'intervallo di tempo, in secondi, in cui i messaggi specificati in **SuppressMessage** vengono scritti una sola volta nel log degli errori del gestore code.
Gravità	Un elenco separato da virgole di livelli di severità.
FilePath	Il percorso in cui vengono scritti i file di log. (Supportato solo quando l'attributo Servizio è impostato su File.)

Tabella 11. Stanze del file qm.ini (Continua)	
Stanza e attributi	**Descrizione degli attributi**
FilePrefix	Il prefisso dei file di log. (Supportato solo quando l'attributo Servizio è impostato su File.)
FileSize	La dimensione alla quale il log esegue il rollover. (Supportato solo quando l'attributo Servizio è impostato su File.)
formato	Il formato del file. (Supportato solo quando l'attributo Servizio è impostato su File.)
Linux UNIX Syslog	Il servizio Syslog che invia tutti i messaggi non filtrati a syslog utilizzando la specifica dei messaggi di diagnostica formato JSON .
Linux UNIX Rientro	Il valore ident associato alle voci syslog. Supportato solo quando l'attributo Servizio è impostato su Syslog.
Stanza ExitPath	
ExitsDefaultPath	Il percorso per i programmi di uscita utente sul sistema del gestore code (32 bit).
ExitsDefaultPath64	Il percorso per i programmi di uscita utente sul sistema del gestore code (64 bit).
ExitPropertiesstanza locale	
CLWLMode	Indica se l'uscita CLWL (cluster workloac) viene eseguita in modalità FAST o SAFE.
IBM i Linux UNIX **Stanza del file system**	
IBM i Linux UNIX ValidateAuth	Consentire agli utenti che non sono membri del gruppo `mqm` di accedere a file e directory di errori.
Stanza di log	
LogPrimaryFiles	I file di log assegnati quando viene creato il gestore code.
LogSecondaryFiles	I file di log assegnati quando i file primari sono esauriti.
LogFilePages	Il numero di pagine del file di log. (La dimensione del file di log è specificata in unità di pagine da 4 KB.)
LogType	Il tipo di registrazione che deve essere utilizzato dal gestore code (circolare o lineare).
LogBufferPages	La quantità di memoria assegnata ai record buffer per la scrittura, specificando la dimensione dei buffer in unità di pagine da 4 KB.
LogPath	La directory in cui risiedono i file di log per un gestore code.
LogWriteIntegrity	Il metodo utilizzato dal programma di registrazione per scrivere in modo affidabile i record di log.
V 9.1.0 LogManagement	Il metodo utilizzato per gestire le estensioni di log, manualmente o dal gestore code.
Windows **StanzaLU62**	

Tabella 11. Stanze del file qm.ini (Continua)	
Stanza e attributi	**Descrizione degli attributi**
Windows Nome TP	Il nome TP da avviare sul sito remoto.
Windows Library1	Il nome della DLL APPC.
Windows Library2	Lo stesso di Library1, utilizzato se il codice è memorizzato in due librerie separate.
Windows **Stanza NETBIOS**	
Windows LocalName	Il nome con cui questa macchina è nota sulla LAN.
Windows AdapterNum	Il numero dell'adattatore LAN.
Windows NumSess	Il numero di sessioni da assegnare.
Windows NumCmds	Il numero di comandi da assegnare.
Windows NumNames	Il numero di nomi da assegnare.
Windows Library1	Il nome della DLL NetBIOS.
Stanza QMErrorLog	
DimensioneErrorLog	Specifica la dimensione del log degli errori del gestore code copiato nel backup.
ExcludeMessage	Specifica i messaggi che non devono essere scritti nel log degli errori del gestore code.
SuppressMessage	Specifica i messaggi scritti nel log degli errori del gestore code una sola volta in un intervallo di tempo specificato.
SuppressInterval	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.
Linux UNIX **Stanza Modalità limitata** [2]	
Linux UNIX ApplicationGroup	Il nome della coda di trasmissione locale in cui vengono inseriti i messaggi remoti se una coda di trasmissione non è esplicitamente definita per la relativa destinazione.
Stanza di protezione	
ClusterQueueAccessControl	Controllare il controllo degli accessi delle code cluster o delle code complete ospitate sui gestori code cluster.
Windows GroupModel	Se OAM (Object Authority Manager) controlla i gruppi globali quando determina l'appartenenza al gruppo di un utente su Windows.
Stanza di servizio	
Nome	Il nome del servizio richiesto.
EntryPoints	Il numero di punti di entrata definiti per il servizio.
Windows SecurityPolicy	Su Windows, la politica di sicurezza per ciascun gestore code

Tabella 11. Stanze del file qm.ini (Continua)	
Stanza e attributi	**Descrizione degli attributi**
Linux UNIX SecurityPolicy	Su UNIX and Linux, se il gestore code utilizza l'autorizzazione basata sull'utente o sul gruppo.
SharedBindingsUserId	Solo per i binding condivisi, se il campo UserIdentifier nella struttura IdentityContext , dalla funzione MQZ_AUTHENTICATE_USER, è l'ID utente effettivo o l'ID utente reale.
FastpathBindingsUserId	Solo per i collegamenti fastpath, se il campo UserIdentifier nella struttura IdentityContext , dalla funzione MQZ_AUTHENTICATE_USER, è l'ID utente effettivo o l'ID utente reale.
IsolatedBindingsUserId	Solo per bind isolati, se il campo UserIdentifier nella struttura IdentityContext , dalla funzione MQZ_AUTHENTICATE_USER, è l'ID utente effettivo o l'ID utente effettivo.
Stanza ServiceComponent	
Servizio	Il nome del servizio richiesto.
Nome	Il nome descrittivo del componente servizio.
Modulo	Il nome del modulo che deve contenere il codice per questo componente.
ComponentDataComponentData	La dimensione, in byte, dell'area dati del componente passata al componente su ciascuna chiamata.
Windows **Stanza SPX**	
Windows Socket	Il numero di socket SPX in notazione esadecimale.
Windows BoardNum	Il numero dell'adattatore LAN.
Windows KeepAlive	Attivare o disattivare la funzione KeepAlive .
Windows Library1	Il nome della DLL SPX.
Windows Library2	Lo stesso di LibraryName1, utilizzato se il codice è memorizzato in due librerie separate.
Windows ListenerBacklog	Sovrascrivere il numero predefinito di richieste in sospeso per il listener SPX.
Stanza SSL	
AllowOutboundAllowOutbound	Specifica se i client con capacità SNI imposteranno SNI sul nome canale IBM MQ di destinazione sul sistema remoto quando si avvia una connessione TLS.
V 9.1.1 AllowedCipher	Specifica un elenco personalizzato di CipherSpecs abilitati per l'utilizzo con i canali IBM MQ su Multiplatforms.
V 9.1.4 AllowTLSV13	Se un gestore code è in grado di utilizzare TLS 1.3 CipherSpecs.

Tabella 11. Stanze del file qm.ini (Continua)	
Stanza e attributi	**Descrizione degli attributi**
CDPCheckExtensions	Se i canali TLS su questo gestore code tentano di controllare i server CDP denominati nelle estensioni del certificato del punto CrlDistribution.
V 9.1.4 MinimumRSAKeyDimensione	Specifica la dimensione chiave minima che i certificati RSA devono avere per essere accettati.
OCSPAuthentication	L'azione da intraprendere quando uno stato di revoca non può essere determinato da un server OCSP.
OCSPCheckExtensions	Indica se i canali TLS su questo gestore code tentano di controllare i server OCSP denominati nelle estensioni certificato di accesso AuthorityInfo.
V 9.1.5 V 9.1.5 OCSPTimeout	Il numero di secondi di attesa per un responder OCSP durante l'esecuzione di una verifica di revoca.
SSLHTTPProxyName	Il nome host o l'indirizzo di rete del server proxy HTTP che deve essere utilizzato da GSKit per i controlli OCSP.
V 9.1.5 V 9.1.5 SSLHTTPConnectTimeout	Il numero di secondi di attesa per stabilire correttamente una connessione di rete a un server HTTP durante l'esecuzione di un controllo di revoca.
Stanza del pool secondario "3" a pagina 107	Questa stanza è creata da IBM MQ. Non modificarla.
ShortSubpoolShortSubpool "3" a pagina 107	Un nome corrispondente a una directory e a un collegamento simbolico creato all'interno della directory /var/mqm/sockets , che IBM MQ utilizza per le comunicazioni interne tra i propri processi in esecuzione.
Windows **Stanza TCP**	
PORT	Il numero di porta predefinito, in notazione decimale, per le sessioni TCP/IP.
Windows Library1	Il nome della DLL socket TCP/IP.
KeepAlive	Attivare o disattivare la funzione KeepAlive .
ListenerBacklog	Sovrascrivere il numero predefinito di richieste in sospeso per il listener TCP/IP.
Timeout connessione	Il numero di secondi prima del timeout di un tentativo di connessione del socket.
SndBuffSndBuff	La dimensione in byte del buffer di invio TCP/IP utilizzato dalla fine di invio dei canali.
RcvBuff	La dimensione in byte del buffer di ricezione TCP/IP utilizzato dall'estremità di ricezione dei canali.
RcvSndBuffSize	La dimensione in byte del buffer di invio TCP/IP utilizzato dall'estremità mittente di un canale ricevente.
RcvRcvBuffSize	La dimensione in byte del buffer di ricezione TCP/IP utilizzato dall'estremità di ricezione di un canale ricevente.

Tabella 11. Stanze del file qm.ini (Continua)	
Stanza e attributi	**Descrizione degli attributi**
SvrSndBuffSize	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	La dimensione in byte del buffer di ricezione TCP/IP utilizzato dall'estremità server di un canale di connessione server di connessione client.
V 9.1.0 **Stanza dei parametri di ottimizzazione**	
SuppressDspAuthFail	Se il gestore code elimina la generazione di eventi di autorizzazione e la scrittura di messaggi di errore AMQ8077 nel log degli errori quando un controllo di autorizzazione non riesce, se la connessione non dispone dell'autorizzazione + dsp per un oggetto.
ImplSyncOpenOutput	Il numero minimo di applicazioni che hanno la coda aperta per l'inserimento, prima che un punto di sincronizzazione implicito possa essere abilitato per un'operazione di inserimento permanente, al di fuori del punto di sincronizzazione.
V 9.1.2 UniformClusterUniformCluster	Il nome del cluster di IBM MQ che si sta utilizzando come cluster uniforme.
V 9.1.0.9 OAMLdapConnectOAMLdapConnect	Il tempo massimo, in secondi, che il client LDAP attenderà per stabilire una connessione TCP al server.
V 9.1.0.9 OAMLdapQueryTimeLimit	Il tempo massimo, in secondi, che il client LDAP attende per ricevere una risposta a una richiesta LDAP dal server.
V 9.1.0.15 OAMLdapResponseWarningTime	Se una connessione a un server LDAP ha impiegato più tempo del numero di soglia di secondi specificato dal parametro **OAMLdapResponseWarningTime** , un messaggio AMQ5544W verrà scritto nel log degli errori.
ExpiryInterval	Indica la frequenza con cui il gestore code esegue la scansione delle code alla ricerca di messaggi scaduti che non sono stati già ripuliti da altre attività della coda. Si tratta di un intervallo di tempo in secondi.
V 9.1.4 **Stanza variabili**	
V 9.1.4 *attributo=valore*	Un nome e un valore associato da utilizzare come inserimento durante le definizioni MQSC.
Stanza XAResourceManager	
Nome	L'istanza del gestore risorse.
SwitchFile	Il nome completo del file di caricamento contenente la struttura dello switch XA del gestore risorse.
XAOpenString	La stringa di dati da passare al punto di ingresso xa_open del gestore risorse.
XACloseString	La stringa di dati da trasmettere al punto di ingresso xa_close del gestore risorse.

Tabella 11. Stanze del file qm.ini (Continua)	
Stanza e attributi	**Descrizione degli attributi**
ThreadOfControl	Il valore che il gestore code utilizza per la serializzazione quando deve richiamare il gestore risorse da uno dei propri processi a più thread. Obbligatorio per Windows.

Note:

1. La stanza AccessMode viene impostata dall'opzione **-a [r]** nel comando **crtmqm** . Non modificare la stanza AccessMode dopo che il gestore code è stato creato.
2. La stanza RestrictedMode è impostata dall'opzione **-g** nel 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` .
3. La stanza Subpool e il nome dell'attributo ShortSubpoolall'interno di tale stanza, vengono scritti automaticamente da IBM MQ quando si crea un gestore code. IBM MQ sceglie un valore per il nome ShortSubpool. Non modificare questo valore.

Windows Stanza AccessMode del file qm.ini

La modalità di accesso si applica solo a server Windows . La stanza AccessMode del file qm.ini è 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 accessi (`-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 si è avviato il gestore code as-a-service, l'ID utente controllato dal sistema Windows è l'ID utente configurato con la procedura guidata **Prepara** IBM 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.

Stanza di esempio

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

Concetti correlati

"Proteggere i file e le directory di log e i dati del gestore code non condivisi su Windows" a pagina 507

"Protezione dei dati del gestore code condiviso e delle directory di log e dei file su Windows" a pagina 504

Attività correlate

"Creazione di un gestore code a più istanze su workstation o server di dominio su Windows" a pagina 479

Riferimenti correlati

crtmqm (crea gestore code)

ApiExitStanza locale del file qm.ini

Per un server, utilizzare la pagina delle proprietà del gestore code `Exits` da IBM MQ Explorero la stanza ApiExitlocale del file `qm.ini` per identificare le routine di uscita API per un gestore code. Per un client, modificare la sezione ApiExitlocale 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 "Stanze del modello ApiExitCommon e ApiExitdel file mqs.ini" a pagina 91.)

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 ulteriori informazioni sull'utilizzo di questi attributi, consultare Configurazione delle uscite API.

Nome=ApiExit_name
Il nome descrittivo dell'uscita API inoltrato nel campo Nome ExitInfodella struttura MQAXP.

Questo nome deve essere univoco, non deve superare i 48 caratteri e contenere solo caratteri validi per i nomi degli oggetti IBM MQ (ad esempio, nomi coda).

Funzione=nome_funzione
Il nome del punto di ingresso della funzione nel modulo contenente il codice di uscita API. Questo punto di ingresso è la funzione MQ_INIT_EXIT.

La lunghezza di questo campo è limitata a MQ_EXIT_NAME_LENGTH.

Modulo=nome_modulo
Il modulo contenente il codice di uscita API.

Se questo campo contiene il percorso completo del modulo, questo verrà visualizzato così come è. Se questo campo contiene solo il nome del modulo, il modulo si trova utilizzando l'attributo **`ExitsDefaultPath`** nella stanza `ExitPath` del file `qm.ini` .

Su piattaforme che supportano librerie separate, è necessario fornire sia una versione non con thread che una versione con thread del modulo di uscita API. La versione con thread deve avere un suffisso `_r` . La versione con thread dello stub dell'applicazione IBM MQ accoda implicitamente `_r` al nome modulo fornito prima che venga caricato.

La lunghezza di questo campo è limitata alla lunghezza massima del percorso supportata dalla piattaforma.

Dati=nome_dati
I dati da passare all'uscita API nel campo ExitData della struttura MQAXP.

Se si include questo attributo, vengono rimossi gli spazi iniziali e finali, la stringa rimanente viene troncata a 32 caratteri e il risultato viene passato all'uscita. Se si omette questo attributo, il valore predefinito di 32 spazi viene passato all'uscita.

La lunghezza massima di questo campo è 32 caratteri.

Sequenza=numero_sequenza
La sequenza in cui questa uscita API viene richiamata rispetto ad altre uscite API. Un'uscita con un numero di sequenza basso viene richiamata prima di un'uscita con un numero di sequenza più alto. Non è necessario che la numerazione di sequenza delle uscite sia contigua. Una sequenza di 1, 2, 3 ha lo stesso risultato di una sequenza di 7, 42, 1096. Se due uscite hanno lo stesso numero di sequenza, il gestore code decide quale richiamare per primo. È possibile determinare quale elemento è stato richiamato dopo l'evento inserendo l'ora o un indicatore nell'area ExitChainindicata da ExitChainAreaPtr in MQAXP oppure scrivendo il proprio file di log.

Questo attributo è un valore numerico senza segno.

Multi V 9.1.4 Stanza AutoCluster del file qm.ini

La stanza AutoCluster viene utilizzata quando il gestore code viene avviato per identificare se il cluster è un membro di un cluster automatico e può identificare i repository completi del cluster.

I seguenti attributi sono obbligatori per la stanza AutoCluster :

Tipo =*Uniforme*
Specifica il tipo di cluster automatico e l'unica opzione valida è *Uniforme*, che rappresenta un cluster uniforme.

ClusterName=*< Stringa>*
Il nome del cluster, ovvero il nome del cluster automatico.

I seguenti attributi sono facoltativi per la stanza AutoCluster , ma è necessario fornirli in coppie:

RepositoryName1 =*< Stringa>*
Questo è il nome del gestore code per il primo repository completo nel cluster automatico. Può essere il nome di questo gestore code o di un altro gestore code.

Repository1Conname=*< Stringa nome connessione>*
Questo è il valore del nome connessione (CONNAME) per il modo in cui i membri del cluster automatico devono connettersi a questo gestore code.

Repository2Name=*< Stringa>*
Questo è il nome del gestore code per il secondo repository completo nel cluster automatico. Può essere il nome di questo gestore code o di un altro gestore code.

Repository2Conname=*< Stringa nome connessione>*
Questo è il valore del nome connessione (CONNAME) per il modo in cui i membri del cluster automatico devono connettersi a questo gestore code.

Stanza di esempio

```
AutoCluster:
        Repository1Name=QM1
        Repository2Name=QM2
        Repository1Conname=127.0.0.1(1414)
        Repository2Conname=127.0.0.1(1415)
        ClusterName=UNIFORMCLUSTER1
        Type=Uniform
```

Concetti correlati

Bilanciamento automatico dell'applicazione

Attività correlate

Creazione di un nuovo cluster uniforme

Utilizzo della configurazione automatica del cluster

Multi V 9.1.4 Stanza AutoConfig del file qm.ini

Gli attributi della stanza AutoConfig vengono utilizzati frequentemente come parte dell'impostazione di cluster uniformi.

Nota: È possibile utilizzare la stanza AutoCluster solo per i cluster uniformi.

MQSCConfig=*< Path>*

Il percorso è un percorso file completo o un percorso a una directory, in cui tutti i file `*.mqsc` vengono applicati al gestore code ad ogni avvio del gestore code.

Per ulteriori informazioni, consultare Configurazione automatica da uno script MQSC all'avvio.

IniConfig=*< Path>*

Il percorso è un percorso file completo o un percorso a una directory, in cui tutti i file `*.ini` vengono applicati al file `qm.ini` ad ogni avvio del gestore code.

Per ulteriori informazioni, consultare “Configurazione automatica di qm.ini all'avvio” a pagina 98.

Stanza di esempio

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

Concetti correlati

Bilanciamento automatico dell'applicazione

Attività correlate

Creazione di un nuovo cluster uniforme

Utilizzo della configurazione automatica del cluster

Multi Stanza dei Canali del file qm.ini

Gli attributi della stanza Channels determinano la configurazione di un canale.

z/OS Queste informazioni non sono applicabili a IBM MQ for z/OS.

Utilizzare la sezione `CHANNELS` del file `qm.ini` per specificare informazioni sui canali.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà del gestore code IBM MQ Explorer `Channels` .

MaxChannels= 100 (valore predefinito) |*numero*

Il numero massimo di canali *correnti* consentiti.

Il valore predefinito è 100.

È possibile impostare **`MaxChannels`** su un valore diverso per limitare il numero massimo di canali correnti, se necessario. Per IBM MQ Appliance, il valore predefinito è 999 999 999 e non deve essere modificato.

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 (valore predefinito) |*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; nessun processo agent.

STANDARD
I canali si collegano utilizzando STANDARD.

PipeLineLength = 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 (valore predefinito) | SVR | SDR | RCVR | CLUSRCVR | ALL | FASTPATH
Se IBM 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 alla scadenza dell'intervallo di attesa **AdoptNewMCATimeout** , il thread o il processo per il precedente server del canale viene terminato.
3. Se il server del canale precedente non è terminato dopo il passo 2 e dopo la scadenza dell'intervallo di attesa **AdoptNewMCATimeout** per una seconda volta, IBM MQ termina il canale con un errore CHANNEL IN USE .

La funzione **AdoptNewMCA** si applica a 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 (valore predefinito) | 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`.

V 9.1.0 **ChlauthEarlyadotta = Y (predefinito) | N**
L'ordine in cui vengono elaborate l'autenticazione della connessione e le regole di autenticazione del canale è un fattore significativo nella determinazione del contesto di sicurezza per connessioni dell'applicazione client IBM MQ .

Attenzione: Il valore predefinito se **`ChlauthEarlyAdopt`** non è presente nel file qm.ini è `N`, tuttavia, da IBM MQ 9.0.4 tutti i gestori code vengono creati con **`ChlauthEarlyAdopt`**=Y aggiunto automaticamente al file qm.ini .

`ChlauthEarlyAdopt` adotta solo gli ID utente forniti a un gestore code per l'autenticazione della connessione, se ADOPTCTX (YES) è impostato sull'oggetto AUTHINFO di autenticazione della connessione sul gestore code.

I valori validi per **`ChlauthEarlyAdopt`** sono i seguenti:

Y
Il canale convalida e adotta le credenziali ID utente e password fornite da un'applicazione che utilizza l'autenticazione della connessione del gestore code prima di applicare le regole di

autenticazione del canale. In questa modalità di funzionamento, le regole di autenticazione del canale corrispondono all'ID utente risultante dai controlli di autenticazione della connessione.

N
Il canale ritarda la convalida di autenticazione della connessione delle credenziali ID utente e password fornite da un'applicazione fino a quando non sono state applicate le regole di autenticazione del canale. Si noti che in questa modalità di operazione, le regole di associazione e di blocco dell'autenticazione del canale non possono considerare i risultati della convalida di ID utente e password.

Ad esempio, l'oggetto delle informazioni di autenticazione predefinito è impostato su **ADOPTCTX(YES)** e l'utente `fred` è collegato. Sono configurate le seguenti due regole CHLAUTH:

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

Il seguente comando viene emesso, con l'intenzione di autenticare il comando come contesto di sicurezza adottato dall'utente bob:

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

Infatti, il gestore code utilizza il contesto di sicurezza di `fred`, non bob, e la connessione non riesce.

Per utilizzare il contesto di sicurezza di bob, **ChlauthEarlyAdopt** deve essere impostato su Y.

PasswordProtection = compatible|always|optional|warn
Da IBM MQ 8.0, impostare le password protette nella struttura MQCSP, piuttosto che utilizzare TLS.

La protezione della password MQCSP è utile per scopi di test e sviluppo in quanto l'utilizzo della protezione della password MQCSP è più semplice rispetto all'impostazione della crittografia TLS, ma non così sicuro.

Per ulteriori informazioni, consultare MQCSP password protection.

V 9.1.0 **IgnoreSeqNumberMismatch = NO (predefinito) | YES**
Gli MCA (Message Channel Agent) alle due estremità di un canale conservano il conteggio del numero di messaggi inviati attraverso il canale per mantenere la sincronizzazione. La sincronizzazione può essere persa, ad esempio se la definizione di canale ad un'estremità viene eliminata e quindi ricreata. In queste circostanze potrebbe essere richiesto un RESET CHANNEL per riconoscere che i dati di sincronizzazione sono stati persi e consentire al canale di continuare l'avvio.

L'attributo **IgnoreSeqNumberMismatch** deve essere impostato sul gestore code del destinatario.

Effettivamente, questo attributo esegue un comando di reimpostazione del canale sul canale ricevente.

Questo attributo controlla il modo in cui il gestore code gestisce una mancata corrispondenza del numero di sequenza durante l'avvio del canale utilizzando i seguenti valori:

NO
I numeri di sequenza del canale vengono controllati durante la risincronizzazione del canale, se i due MCA non concordano sullo stesso numero di sequenza, verrà riportato il messaggio di errore AMQ9526 e il canale non verrà avviato.

SÌ
I numeri di sequenza del canale vengono controllati durante la risincronizzazione del canale, ma se i due MCA non concordano sullo stesso numero di sequenza, verrà notificato il messaggio di avviso AMQ9703 e l'avvio del canale continuerà. Questo valore di attributo non dovrebbe essere necessario in circostanze normali. Quando è noto che i dati di sincronizzazione sono stati persi, ad esempio durante il ripristino di emergenza, questa opzione evita di dover riconoscere manualmente ogni mancata corrispondenza del numero di sequenza. La specifica di questo valore ha un effetto simile a quello di un amministratore che immette automaticamente un **RESET CHANNEL** in risposta a ogni mancata corrispondenza di numeri di sequenza.

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

Consente a un gestore code di rendere il nome utente corrispondente all'interno delle regole CHLAUTH non sensibili al maiuscolo / minuscolo. Questa opzione consente di:

- CLNTUSER nelle regole CHLAUTH TYPE (USERMAP) da mettere in corrispondenza senza distinzione tra maiuscole e minuscole
- USERLIST nelle regole CHLAUTH TYPE (BLOCKUSER) da mettere in corrispondenza in modo insensibile al maiuscolo / minuscolo

I valori validi per **ChlauthIgnoreUserCase** sono i seguenti:

N
Le regole di autenticazione del canale tentano di mettere in corrispondenza l'identificazione dell'utente client con la sensibilità al maiuscolo / minuscolo, ad esempio una regola che specifica CLNTUSER ('Fred') non corrisponderà a 'fred' o 'FRED', ma solo a un identificativo utente di 'Fred '. Questo è il valore predefinito.

Y
Le regole di autenticazione del canale tentano di mettere in corrispondenza l'identificazione utente del client con l'insensibilità al maiuscolo / minuscolo, ad esempio una regola di autenticazione del canale con TYPE (USERMAP) o TYPE (USERBLOCK) che specifica CLNTUSER ('Fred') corrisponderà a qualsiasi variazione di maiuscolo / minuscolo, ad esempio gli identificatori utente 'Fred', 'FRED' e 'fred ' corrispondono tutti.

Tenere presente che, quando si ignorano gli identificativi utente durante la corrispondenza delle regole di autenticazione del canale, è possibile che più di una regola corrisponda. Se ciò si verifica, la regola corrispondente non è definita. Ad esempio, con le seguenti regole, se l'utente 'fred' si connette a un gestore code tramite il canale CLIENT, potrebbe essere associato a 'mquser1' o 'mquser2':

```
SET CHLAUTH('CLIENT') TYPE(USERMAP) CLNTUSER('fred') USERSRC(MAP) MCAUSER('mquser1')
SET CHLAUTH('CLIENT') TYPE(USERMAP) CLNTUSER('FRED') USERSRC(MAP) MCAUSER('mquser2')
```

Per evitare qualsiasi incertezza quando si utilizza `ChlauthIgnoreUserCase=Y`, evitare di definire regole CHLAUTH che si sovrapporrebbero e risulterebbero in un comportamento diverso quando si utilizza una corrispondenza non sensibile al maiuscolo / minuscolo.

ChlauthIssueAvvertenza = y
Impostare questo attributo se si desidera che il messaggio AMQ9787 venga generato quando si imposta l'attributo WARN = YES sul comando **SET CHLAUTH** .

Stanza di esempio

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

Concetti correlati

“Stati del canale” a pagina 208
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.

Multi Stanza di connessione del file qm.ini

La stanza Connection definisce il tipo di binding predefinito.

Utilizzare la stanza Connection nel file `qm.ini` per specificare il tipo di binding predefinito.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà del gestore code IBM MQ Explorer `Extended` .

Nota: È necessario creare una stanza di connessione, se ne è necessaria una.

DefaultBindTipo = SHARED (valore predefinito) |ISOLATO

Se **DefaultBindType** è impostato su `ISOLATO`, le applicazioni e il gestore code vengono eseguiti in processi separati e non viene condivisa alcuna risorsa.

Se **DefaultBindType** è impostato su SHARED, le applicazioni e il gestore code vengono eseguiti in processi separati, ma alcune risorse vengono condivise tra loro.

Il valore predefinito è SHARED.

Attenzione: DefaultBindType si applica a tutte le chiamate MQCONN e a tutte le chiamate MQCONNX con MQCNO_STANDARD_BINDING.

La modifica di **DefaultBindType** potrebbe causare il peggioramento delle prestazioni di alcune applicazioni.

Stanza di esempio

```
Connection:
  DefaultBindType=SHARED
```

Registrazione dei messaggi diagnostici

I log dei messaggi diagnostici di IBM MQ sono un meccanismo che consente ai vari componenti del sistema IBM MQ di notificare i messaggi diagnostici relativi alle modifiche e ai problemi di configurazione e di stato di runtime di IBM MQ .

Questi log sono a volte indicati come IBM MQ *log di errore*, ma contengono sempre IBM MQ informazioni e messaggi di avvertenza, nonché messaggi di errore. I tre componenti principali di IBM MQ che riportano a questi log sono:

- Gestori code
- IBM MQ Client
- Il resto del sistema IBM MQ

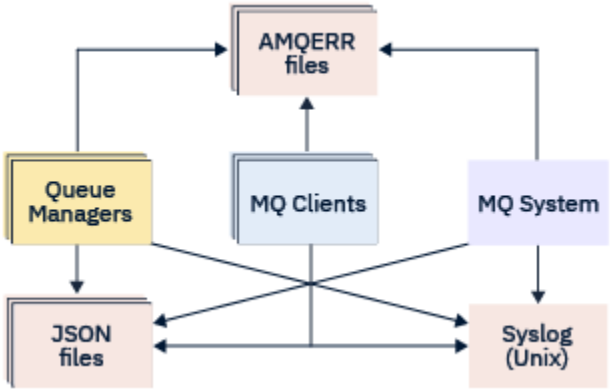
IBM MQ supporta la creazione di report dei messaggi di diagnostica tramite diversi metodi noti come *servizi di messaggi di diagnostica*, consentendo un approccio personalizzato per la registrazione e l'utilizzo di tali informazioni:

- File di log AMQERRnn
- File di log formattati JSON
- UNIX Syslog in formato JSON

L'output JSON di IBM MQ è formattato come oggetti JSON a riga singola, in modo che ogni singola riga del log JSON o del record Syslog, rappresenti un oggetto JSON valido. L'intero log non è incapsulato come un singolo oggetto JSON.

La seguente figura mostra che i gestori code, i client IBM MQ e il sistema IBM MQ possono *tutti* i messaggi di diagnostica utilizzando i metodi descritti.

Figura 5. Come le diverse parti di IBM MQ possono riportare i messaggi diagnostici



Modalità di configurazione dei log di diagnostica IBM MQ :

I log di diagnostica sono definiti e personalizzati utilizzando le stanze all'interno del file `qm.ini` particolare del componente IBM MQ che li richiede. Ogni endpoint di registrazione univoco è definito sotto la propria intestazione di stanza all'interno del file ini, insieme a tutte le personalizzazioni definite al suo interno. Le personalizzazioni possono includere:

- La dimensione dei file di log su cui eseguire il wrap, prima del rollover; non applicabile a Syslog
- Qualsiasi filtro basato sulla severità dei messaggi di log e
- Qualsiasi codice di messaggio specifico da eliminare.

IBM MQ può essere configurato per scrivere in uno o in tutti e tre i tipi di endpoint di registrazione, consentendo a particolari stanze di log di soddisfare particolari ruoli. Allo stesso modo, è possibile definire più servizi file. Ad esempio:

- Il formato JSON semplifica l'analisi tramite strumenti automatizzati in ambienti locali e cloud.
- L'output syslog consente ai componenti IBM MQ di integrare le informazioni di diagnostica in un'ubicazione di registrazione del SO comune in linea con altri prodotti sul sistema.
- Gli endpoint di log filtrati in base alla severità, consentendo a determinati file di log di registrare, ad esempio, solo errori gravi nel sistema.

Indipendentemente dallo stile di registrazione della diagnostica configurato, i file di diagnostica tradizionali contenuti nella directory di log del sistema IBM MQ (`/var/mqm/errors/AMQERRnn.log`) e nella directory di log del gestore code specifico (`/var/mqm/qmgrs/<qmgr_name>/errors/AMQERRnn.log`) vengono sempre scritti, in aggiunta a qualsiasi altra configurazione di registrazione utilizzata.

Solo per i gestori code, la configurazione facoltativa di questi log obbligatori può essere eseguita specificando attributi di “Stanze del servizio messaggi diagnostici” a pagina 118.

Aree di stanza differenti

Le stanze aggiuntive possono essere applicate a diverse aree di IBM MQ.

Gestore code (qm.ini)
Si applica al messaggio di log generato dal gestore code

Sistema (mqs.ini)
Si applica ai messaggi di log generati dal sistema. Questa opzione non è specifica per un gestore code, tranne quando un gestore code non può accedere o scrivere nei propri log.

Modelli (mqs.ini)
Una o più stanze come modelli, che vengono copiate in `qm.ini` quando viene creato un gestore code.

Client (mqclient.ini)
Si applica all'operazione client, ad esempio **runmqsc** in modalità client per un gestore code remoto.

Conversione tra i log formattati JSON e quelli formattati in modo tradizionale

Il comando mqrc è stato migliorato per consentire un numero di conversioni tra JSON e i log formattati in modo tradizionale e tra lingue differenti.

Riferimenti correlati

"Stanze del servizio messaggi diagnostici" a pagina 118
Le opzioni del servizio messaggi di diagnostica disponibili abilitano la personalizzazione della registrazione della diagnostica IBM MQ , in modo che l'output del log possa essere indirizzato a diversi endpoint di log da diversi componenti di IBM MQ.

"stanza QMErrorLog" a pagina 117
Utilizzare la stanza del log degli errori del gestore code QMErrorLog nel file `qm.ini` per adattare l'operazione e il contenuto dei log degli errori IBM MQ .

"Servizi di messaggi diagnostici" a pagina 121
È possibile definire i seguenti servizi di messaggi diagnostici e i relativi attributi specifici del servizio, specificati nelle sezioni DiagnosticSystemMessages, DiagnosticMessages e DiagnosticMessagesTemplate dei file di configurazione:

Multi *stanza QMErrorLog*

Utilizzare la stanza del log degli errori del gestore code QMErrorLog nel file `qm.ini` per adattare l'operazione e il contenuto dei log degli errori IBM MQ .

Il servizio QMErrorLog è il servizio di log di diagnostica IBM MQ tradizionale utilizzato per emettere messaggi di diagnostica relativi al gestore code. Il servizio QMErrorLog viene eseguito continuamente e non può essere disattivato, ma può essere personalizzato in una certa misura.

È possibile utilizzare la sezione QMErrorLog del file `qm.ini` per escludere alcuni messaggi dalla scrittura nel log degli errori del gestore code. È inoltre possibile impedire che i messaggi vengano scritti nel log degli errori per un determinato periodo di tempo.

Linux Windows In alternativa, anziché modificare direttamente il file `qm.ini` , è possibile utilizzare la pagina delle proprietà del gestore code esteso in IBM MQ Explorer per escludere ed eliminare i messaggi con gli attributi **Messaggi esclusi**, **Messaggi soppressi** e **Intervallo messaggi soppressi** .

Attenzione:

- Windows È possibile utilizzare IBM MQ Explorer per apportare le modifiche solo se si sta utilizzando un gestore code locale sulla piattaforma Windows .
- La stanza QMErrorLog non è applicabile al file di configurazione del sistema IBM MQ , `mqs.ini`, o al file di configurazione del client, generalmente denominato `mqclient.ini`.

I seguenti attributi possono essere inclusi nella stanza QMErrorLog :

ErrorLogDimensione = *maxsize*
Specifica la dimensione del log degli errori del gestore code copiato nel backup. **`maxsize`** deve essere compreso tra 32768 e 2147483648 byte. Se **`ErrorLogSize`** non viene specificato, viene utilizzato il valore predefinito di 33554432 byte (32 MB).

È possibile utilizzare questo attributo per ridurre la dimensione massima al valore massimo precedente di 2 MB, se richiesto.

È possibile impostare la dimensione del log utilizzando la variabile di ambiente **`MQMAXERRORLOGSIZE`** .

ExcludeMessage= *msgIds*
Specifica i messaggi che non devono essere scritti nel log degli errori del gestore code.

Per ulteriori informazioni, consultare ExcludeMessage in "Stanze del servizio messaggi diagnostici" a pagina 118 .

SuppressMessage= *msgIds*
Specifica i messaggi scritti nel log degli errori del gestore code una sola volta in un intervallo di tempo specificato. Se lo stesso ID messaggio viene specificato in `SuppressMessage` e `ExcludeMessage`, il messaggio viene escluso.

Questa opzione non è applicabile ai servizi di messaggi di diagnostica definiti in `mqclient.ini`. Per ulteriori informazioni, consultare SuppressMessage in "Stanze del servizio messaggi diagnostici" a pagina 118.

SuppressInterval= *lunghezza*
Specifica l'intervallo di tempo, in secondi, in base al quale i messaggi specificati in `SuppressMessage` vengono scritti nel log degli errori del gestore code una sola volta. *length* deve essere compreso tra 1 e 86400 secondi. Se `SuppressInterval` non viene specificato, viene utilizzato il valore predefinito di 30 secondi.

Stanza di esempio

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

Concetti correlati

"File di configurazione del gestore code, qm.ini" a pagina 97
Un file di configurazione del gestore code, `qm.ini`, contiene informazioni relative a uno specifico gestore code.

Riferimenti correlati

"Stanze del servizio messaggi diagnostici" a pagina 118
Le opzioni del servizio messaggi di diagnostica disponibili abilitano la personalizzazione della registrazione della diagnostica IBM MQ , in modo che l'output del log possa essere indirizzato a diversi endpoint di log da diversi componenti di IBM MQ.

Multi *Stanze del servizio messaggi diagnostici*

Le opzioni del servizio messaggi di diagnostica disponibili abilitano la personalizzazione della registrazione della diagnostica IBM MQ , in modo che l'output del log possa essere indirizzato a diversi endpoint di log da diversi componenti di IBM MQ.

Abilitare ulteriori servizi di messaggi diagnostici, utilizzando una stanza con uno dei seguenti nomi:

- **`DiagnosticSystemMessages`**

  Definisce i servizi utilizzati quando viene generato un messaggio diagnostico che va alla registrazione errori di sistema. Valido nei file `mqs.ini` o `mqclient.ini` .

  Le applicazioni client utilizzano una sezione **`DiagnosticSystemMessages`** nel file mqclient.ini e in mqs.ini, la stanza **`DiagnosticSystemMessages`** controlla i messaggi per un'applicazione server che non dispone di un contesto gestore code.

  È possibile configurare un gestore code e le applicazioni che scrivono ulteriormente tutti i messaggi nel servizio syslog.

- **`DiagnosticMessages`**

  Definisce i servizi utilizzati quando viene generato un messaggio diagnostico che va al log degli errori del gestore code. Valido solo nel file `qm.ini` .

- **`DiagnosticMessagesTemplate`**

  Una stanza copiata dal file `mqs.ini` in **`DiagnosticMessages`** nel file `qm.ini` quando viene creato un gestore code.

Per visualizzare messaggi diagnostici, utilizzare il comando mqrc .

Attributi delle stanze

Attenzione: `Servizio`e un nome di stanza sono obbligatori.

nome= < nomestanza>
Nome di una stanza. Il valore deve essere univoco in un file ini.

Servizio = *tipo di servizio*

Questo attributo definisce un servizio, in cui il nome del servizio non è sensibile al maiuscolo / minuscolo, abilitato da questa stanza.

Ad esempio, per abilitare `syslog` come servizio aggiuntivo, immettere quanto segue:

```
Service=syslog
```

Consultare “Servizi di messaggi diagnostici” a pagina 121 e i relativi attributi specifici disponibili per l'utilizzo con le stanze del servizio messaggi diagnostici.

È possibile aggiungere i seguenti attributi facoltativi alle stanze:

- ExcludeMessage
- SuppressMessage
- SuppressInterval
- “Gravità” a pagina 120

ExcludeMessage= *msgIds*
Specifica i messaggi che non devono essere scritti nel log degli errori del gestore code. Se il sistema IBM MQ è molto 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 della copia cartacea. Il bridge IBM MQ - IMS e il gestore buffer potrebbero anche produrre un numero elevato di messaggi informativi, pertanto l'esclusione dei messaggi impedisce di ricevere un numero elevato di messaggi, se necessario. *msgIds* contiene un elenco separato da virgole di ID messaggio provenienti da:

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
IBM i 7163 - Messaggio avviato dal lavoro (solo IBM i)
7234 - Numero di messaggi caricati
8245 - L'entità non dispone di autorizzazione sufficiente per visualizzare l'oggetto
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
9545 - Intervallo di disconnessione scaduto
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 IBM MQ è molto 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 della copia cartacea. Il bridge IBM MQ - IMS e il gestore buffer potrebbero anche produrre un numero elevato di messaggi informativi, pertanto l'eliminazione dei messaggi impedisce di ricevere un certo numero di messaggi ripetuti, se necessario. L'intervallo di tempo è specificato da `SuppressInterval`. *msgIds* contiene un elenco separato da virgole di identificatori di messaggi 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
IBM i 7163 - Messaggio avviato dal lavoro (solo IBM i)
7234 - Numero di messaggi caricati
8245 - L'entità non dispone di autorizzazione sufficiente per visualizzare l'oggetto
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
9545 - Intervallo di disconnessione scaduto
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 in `SuppressMessage` e `ExcludeMessage`, il messaggio viene escluso.

Questa opzione non è applicabile ai servizi di messaggi di diagnostica definiti in `MQ client.ini`.

SuppressInterval= *lunghezza*
Specifica l'intervallo di tempo, in secondi, in cui i messaggi specificati in **SuppressMessage** vengono scritti una sola volta nel log degli errori del gestore code. *length* deve essere compreso tra 1 e 86400 secondi. Se **SuppressInterval** non viene specificato, viene utilizzato il valore predefinito di 30 secondi.

Gravità
Un elenco separato da virgole di livelli di severità, in cui il nome del livello di severità non è sensibile al maiuscolo / minuscolo. I valori consentiti sono:

- I (o Informazioni o 0)
- W (o Avvertenza o 10)
- E (o Errore o 20 e 30)
- S (o Stop o 40)

- T (o Sistema o 50)

Note:

1. Il valore predefinito è: `all`
2. Solo i messaggi nei livelli di severità selezionati vengono presentati al servizio.

   In alternativa, è possibile utilizzare il carattere più (+) che visualizza il livello di errore specificato e tutti i livelli superiori. Ad esempio, per visualizzare tutti gli errori:

```
Severities=E+
```

Riferimenti correlati

“stanza QMErrorLog” a pagina 117
Utilizzare la stanza del log degli errori del gestore code QMErrorLog nel file `qm.ini` per adattare l'operazione e il contenuto dei log degli errori IBM MQ .

“Servizi di messaggi diagnostici” a pagina 121
È possibile definire i seguenti servizi di messaggi diagnostici e i relativi attributi specifici del servizio, specificati nelle sezioni DiagnosticSystemMessages, DiagnosticMessages e DiagnosticMessagesTemplate dei file di configurazione:

Multi *Servizi di messaggi diagnostici*

È possibile definire i seguenti servizi di messaggi diagnostici e i relativi attributi specifici del servizio, specificati nelle sezioni DiagnosticSystemMessages, DiagnosticMessages e DiagnosticMessagesTemplate dei file di configurazione:

Sono definiti i seguenti servizi di messaggi diagnostici:

File

Questo servizio invia i messaggi non filtrati a un file in modo simile al servizio QMErrorLog . Il formato testuale esistente o il formato JSON specificato viene utilizzato in base al **Format**specificato. Per impostazione predefinita, esistono tre file denominati `AMQERR01.LOG`, `AMQERR02.LOG`e `AMQERR03.LOG` o `AMQERR01.json`, `AMQERR02.json`e `AMQERR03.json`, a seconda della proprietà **Format** e questi rollover si basano sulla dimensione configurata.

I seguenti attributi sono supportati solo in una stanza File:

FilePath

Il percorso in cui vengono scritti i file di log. Il valore predefinito è lo stesso percorso dei file `AMQERR01.log` , ossia il sistema o il gestore code. Il percorso deve essere assoluto, ma può includere inserimenti sostituibili. Ad esempio:

+ MQ_Q_MGR_DATA_PATH +

Il percorso completo dell'elemento principale della directory dei messaggi di diagnostica del gestore code. I valori predefiniti sono:

- UNIX Su piattaforme UNIX and Linux : `/var/mqm/qmgrs/<QM_name>`
- Windows su Windows, `C:\Program Data\IBM\MQ\qmgrs\<QM_name>`

+ MQ_DATA_PATH +

Il percorso completo della directory dei messaggi di diagnostica del sistema. I valori predefiniti sono:

- UNIX Su piattaforme UNIX and Linux :`/var/mqm`
- Windows Su Windows: `C:\Program Data\IBM\MQ`

È necessario creare questo percorso con le autorizzazioni appropriate, se non si utilizza la directory degli errori esistente.

FilePrefix

Il prefisso dei file di log. Il valore predefinito è AMQERR.

FileSize
La dimensione alla quale il log esegue il rollover. Il valore predefinito è 32MB, come con la proprietà **ErrorLogSize** di "stanza QMErrorLog" a pagina 117, che è semanticamente identica.

Nota: La proprietà **ErrorLogSize** si applica solo al servizio di registrazione errori predefinito, non ai servizi di diagnostica personalizzati.

È possibile impostare la dimensione del log utilizzando la variabile di ambiente **MQMAXERRORLOGSIZE** .

Format
Il formato del file. Il valore può essere *text* (per ulteriori servizi di stile QMErrorLog) o *json*, che è il valore predefinito.

Il suffisso del file è `.LOG` o `.json` in base all'impostazione di questo attributo.

Ad esempio, modificare il file `qm.ini` del gestore code e aggiungere la stanza seguente:

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

Dopo il riavvio, il gestore code avrà i file `AMQERR0x.json` nella directory ERRORS.

È possibile definire più servizi File. Ciò consente la configurazione, come mostrato nei seguenti esempi, in cui i messaggi di tag differenti sono suddivisi in diverse serie di log:

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

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

Linux UNIX **Syslog**
Il servizio Syslog non è disponibile su Windows o IBM i

È possibile definire solo un servizio Syslog e il servizio Syslog invia tutti i messaggi non filtrati a syslog utilizzando la specifica dei messaggi diagnostici formato JSON . Le informazioni vengono aggiunte a syslog nell'ordine mostrato nella tabella, iniziando con msgID e inserimenti.

La severità del messaggio è associata al livello syslog nel seguente modo:

Tabella 12. Associazione della severità del messaggio al livello syslog

Gravità	**Livello**
0	LOG_INFO
10	LOG_AVVERTENZA
20	ERR LOGO
30	ERR LOGO
40	LOG_ALERT
50	LOG_ALERT

Il seguente attributo è supportato solo in una stanza syslog:

Ident
Definisce il valore **ident** associato alle entrate syslog. Il valore predefinito è *ibm - mq*.

Il seguente esempio mostra i messaggi di errore inviati al Syslog:

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

Consultare “Stanze del servizio messaggi diagnostici” a pagina 118 per ulteriori informazioni sugli attributi generici della stanza.

Note:

1. Solo per il servizio File, è possibile avere più stanze, ognuna con un nome diverso. Solo la definizione, utilizzando il nome finale nella sequenza, diventa effettiva.
2. Le modifiche al valore di una stanza diventano effettive solo quando il gestore code viene riavviato.

Multi Stanza ExitPath del file qm.ini

La stanza ExitPath specifica il percorso per i programmi di uscita utente sul sistema gestore code.

Utilizzare la stanza `ExitPath` nel file `qm.ini` per specificare il percorso per i programmi di uscita utente sul sistema del gestore code.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà del gestore code IBM MQ Explorer `Exits` .

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

Stanza di esempio

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

Multi ExitPropertiesStanza locale del file qm.ini

La stanza ExitPropertiesLocal specifica le informazioni sulle proprietà di uscita su un gestore code.

Utilizzare la stanza ExitPropertiesLocal nel file `qm.ini` per specificare le informazioni sulle proprietà di uscita su un gestore code.

Linux Windows In alternativa, in Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà del gestore code del cluster IBM MQ Explorer .

Windows In alternativa, su Windows è possibile specificare queste informazioni utilizzando il comando **amqmdain** .

Per impostazione predefinita, questa impostazione viene ereditata dall'attributo **CLWLMode** nella stanza ExitProperties della configurazione della macchina (descritta in “Stanza ExitProperties del file mqs.ini” a pagina 92). 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.

Utilizzare la stanza ExitProperties nel file `mqs.ini` per specificare opzioni di configurazione utilizzate dai programmi di uscita del gestore code.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà di IBM MQ Explorer `Extended` IBM MQ .

CLWLMode= SAFE (predefinito) | FAST
L'uscita del carico di lavoro cluster (CLWL) consente di specificare quale coda cluster nel cluster aprire in risposta 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 cluster viene eseguita in modalità SAFE.

SICURA
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 potrebbe 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.

Stanza di esempio

```
ExitPropertiesLocal:
      CLWLMode=SAFE
```

IBM i Linux UNIX Stanza del file system del file qm.ini

La stanza File system specifica se le autorizzazioni impostate sui log degli errori del gestore code devono rimanere invariate o devono essere nuovamente modificate ai valori predefiniti.

Si prevede che le autorizzazioni predefinite impostate sui file di log degli errori siano utili nella maggior parte dei casi e, pertanto, non è necessario che la maggior parte degli amministratori IBM MQ le modifichino.

Tuttavia, l'amministratore IBM MQ potrebbe voler modificare le autorizzazioni sui propri file di log degli errori, nel qual caso dovrebbe impostare l'opzione della stanza `Filesystem` **ValidateAuth**=*No*, che fa in modo che il gestore code lasci le autorizzazioni inalterate in seguito.

Il funzionamento predefinito (senza **ValidateAuth**=*No*) è che il gestore code controlla le autorizzazioni file dei log degli errori del gestore code e le modifica di nuovo ai valori predefiniti. Questo controllo può verificarsi in qualsiasi momento, anche durante un'operazione di fine o avvio del gestore code.

Stanza di esempio

```
Filesystem:
      ValidateAuth=No
```

Multi Stanza di log del file qm.ini

La stanza Log specifica le informazioni sulla registrazione su un gestore code.

Utilizzare la stanza Log nel file `qm.ini` per specificare le informazioni sulla registrazione su un gestore code.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà del gestore code IBM MQ Explorer Log .

Per impostazione predefinita, queste impostazioni vengono ereditate dalle impostazioni specificate per le impostazioni di log predefinite del gestore code (descritte in “Stanza LogDefaults del file mqs.ini” a pagina 93). 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 599.

Nota: I limiti forniti nel seguente elenco di parametri sono impostati da IBM MQ. I limiti del sistema operativo potrebbero ridurre la dimensione massima possibile del log.

LogPrimaryFiles = 3 (valore predefinito) |*2-254* (Windows) |*2-510* (sistemi UNIX 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 sistemi 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 (predefinito) |*1-253* (Windows) |*1-509* (sistemi UNIX 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 sistemi 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.

LogFilePagine = *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 (valore predefinito) | LINEAR
Il tipo di registrazione che deve essere utilizzato dal gestore code. Il valore predefinito è CIRCULAR. Fare riferimento alla descrizione dell'attributo **LogType** in "Stanza LogDefaults del file mqs.ini" a pagina 93 per informazioni sulla creazione di un gestore code con il tipo di registrazione richiesto.

CIRCOLARE
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 594 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 594 per una spiegazione più completa della registrazione lineare.

Nota: Il **LogType** di un gestore code non può essere modificato modificando questo attributo nel file qm.ini . Per modificare il **LogType** di un gestore code, è necessario utilizzare il comando **migmqlog** .

LogBufferPagine = 0 (valore predefinito) |*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.

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:

- Windows C:\ProgramData\IBM\MQ\log in Windows.
- Linux UNIX /var/mqm/log in sistemi UNIX and Linux .

È possibile specificare il nome di una directory sul 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 .

Nei sistemi IBM MQ for UNIX e 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` (predefinito)
Il metodo utilizzato dal programma di registrazione per scrivere in modo affidabile i record di log.

`TripleWrite` (predefinito)
È il metodo predefinito.

Nota: è possibile selezionare **DoubleWrite** ma, in tal caso, il sistema l'interpreta come **TripleWrite**.

SingleWrite
Si consiglia di utilizzare **SingleWrite**, solo se il file - system e il dispositivo che ospita il log di recupero IBM MQ garantiscono esplicitamente l'atomicità delle scritture 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.

Nota: Se è presente una simultaneità sufficiente nel tuo carico di lavoro persistente, c'è un vantaggio potenziale minimo nell'impostazione di un valore diverso da quello predefinito, **TripleWrite**.

Per ulteriori informazioni, consultare “LogWriteIntegrity - utilizzando SingleWrite o TripleWrite” a pagina 128.

LogManagement= `Manuale` (predefinito) | Automatico | Archivio
Il metodo utilizzato per gestire le estensioni di log, manualmente o dal gestore code. Il valore predefinito è `Manuale`.

L'attributo si applica solo quando **LogType** è `LINEAR`.

Se si modifica il valore **`LogManagement`**, la modifica non ha effetto fino al riavvio del gestore code.

Se viene trovato un valore non riconosciuto per l'attributo, il gestore code non verrà avviato fino a quando il valore non viene corretto.

La proprietà **`LogManagement`** non è valida su IBM i.

`Manuale` (predefinito)
Le estensioni di log vengono gestite manualmente. Specificando questa opzione il gestore code non riutilizza o elimina le estensioni log, anche quando non sono più necessarie per il ripristino.

Automatico
Le estensioni log vengono gestite automaticamente dal gestore code. Specificando questa opzione il gestore code può riutilizzare o eliminare le estensioni log quando non sono più necessarie per il ripristino. Nessuna agevolazione viene effettuata per l'archiviazione.

Archivio
Le estensioni log sono gestite dal gestore code, ma è necessario notificare al gestore code quando l'archiviazione di ciascuna estensione log è completa.

Specificando questa opzione il gestore code è libero di riutilizzare o eliminare un'estensione log esistente, come viene notificato che un'estensione log non è più necessaria per il ripristino essa viene archiviata.

Eseguire questa notifica utilizzando il comando **`RESET QMGR`** MQSC o il comando PCF Reimposta gestore code .

Stanza di esempio

```
Log:
   LogPrimaryFiles=3
```

```
    LogSecondaryFiles=2
    LogFilePages=4096
    LogType=CIRCULAR
    LogBufferPages=0
    LogPath=/var/mqm/log/saturn!queue!manager/
```

Nota: Il valore di zero per `LogBufferPages` fornisce un valore di 512.

LogWriteIntegrity - utilizzando SingleWrite o TripleWrite

L'impostazione dell'opzione **LogWriteIntegrity** , nella stanza Log del file `qm.ini` , determina l'algoritmo utilizzato dal logger in IBM MQ per scrivere i record di log nel log di ripristino. L'impostazione predefinita è *TripleWrite* e questa impostazione è sicura in quasi tutti gli scenari possibili

L'impostazione di **LogWriteIntegrity** ha alcun effetto, solo quando deve essere scritta una pagina di log parziale. Per un gestore code con una quantità ragionevole di attività simultanea, questo scenario si verifica raramente.

SingleWrite

SingleWrite seleziona un algoritmo che, in circostanze molto insolite, può essere eseguito meglio dell'impostazione predefinita *TripleWrite* . L'impostazione *SingleWrite* è sicura, solo se la piattaforma di archiviazione sottostante può garantire in modo assoluto che le pagine 4KB scritte in modo sincrono nel log di ripristino di MQ vengano scritte in modo atomico.

È necessario utilizzare l'impostazione *SingleWrite*, solo se il file - system o la periferica, che ospita il log di recupero IBM MQ , garantisce esplicitamente l'atomicità delle scritture 4KB . Vale a dire, quando una scrittura di una pagina 4KB ha esito negativo per qualsiasi motivo, gli unici due stati possibili devono essere l'immagine precedente o l'immagine successiva e non deve essere possibile alcuno stato intermedio. In tutti gli altri casi, si consiglia *TripleWrite.*

Su un sistema con una simultaneità sufficiente, il gestore code scrive solo pagine complete di dati di log e, se viene raggiunta un'elevata percentuale di pagine complete, non vi è alcuna differenza di prestazioni significativa tra *SingleWrite* e *TripleWrite*.

Su un sistema con poca simultaneità, può essere un vantaggio significativo sulle prestazioni per *SingleWrite*, tuttavia la soluzione preferita è di solito quella di aumentare la simultaneità, piuttosto che utilizzare *SingleWrite*.

Si noti che può essere difficile determinare in modo affidabile l'atomicità delle scritture 4KB e le modifiche al software o all'hardware sottostante potrebbero invalidare tale garanzia.

Se hai il dubbio che la tua infrastruttura di archiviazione offra le garanzie richieste ora e in qualsiasi momento in futuro in tutte le circostanze, dovresti utilizzare *TripleWrite*.

Windows Stanza LU62 del file qm.ini (soloWindows)

La stanza LU62 specifica parametri di configurazione del protocollo SNA LU 6.2 . Questi parametri sovrascrivono gli attributi predefiniti per i canali.

Utilizzare la sezione LU62 del file `qm.ini` per specificare i parametri di configurazione del protocollo SNA LU 6.2 . Sovrascrivono gli attributi predefiniti per i canali.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà del gestore code IBM MQ Explorer LU6.2 .

TPName
Il nome TP da avviare sul sito remoto.

Library1= *NomeDLL 1*
Il nome della DLL APPC.

Il valore predefinito è WCPIC32.

Library2= *DLLName2*
Lo stesso di Library1, utilizzato se il codice è memorizzato in due librerie separate.

Il valore predefinito è WCPIC32.

Windows Stanza NETBIOS del file qm.ini (soloWindows)

La stanza NETBIOS nel file `qm.ini` specifica i parametri di configurazione del protocollo NetBIOS . Questi parametri sovrascrivono gli attributi predefiniti per i canali.

Utilizzare la stanza NETBIOS nel file `qm.ini` per specificare i parametri di configurazione del protocollo NetBIOS . Sovrascrivono gli attributi predefiniti per i canali.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà del gestore code Netbios IBM MQ Explorer .

LocalName= *nome*
Il nome con cui questa macchina è nota sulla LAN.

AdapterNum= `0` (predefinito) | *numero_adattatore*
Il numero dell'adattatore LAN. Il valore predefinito è l'adattatore 0.

NumSess= 1 (valore predefinito) | *numero_di_sessioni*
Il numero di sessioni da assegnare. Il valore predefinito è 1.

NumCmds= 1 (valore predefinito) | *numero_di_comandi*
Il numero di comandi da assegnare. Il valore predefinito è 1.

NumNames= 1 (valore predefinito) | *numero_di_nomi*
Il numero di nomi da assegnare. Il valore predefinito è 1.

Library1= *DLLName1*
Il nome della DLL NetBIOS.

Il valore predefinito è NETAPI32.

Linux UNIX Stanza RestrictedMode del file qm.ini

La stanza RestrictedMode specifica il nome del gruppo che contiene i membri a cui è consentito eseguire le applicazioni MQI, aggiornare tutte le risorse IPCC e modificare il contenuto di alcune directory del gestore code. Questa stanza si applica solo ai sistemi UNIX and Linux .

La stanza RestrictedMode è impostata dall'opzione **`-g`** sul comando **`crtmqm`** . Se non si utilizza l'opzione **`-g`** , la stanza non viene creata nel file `qm.ini` .

Alcune directory in cui le applicazioni IBM 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

- Aggiorna 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 MQ devono essere nel gruppo di applicazioni.

Qualsiasi chiamata MQCONN o MQCONNX emessa da un utente che non si trova nel gruppo di applicazioni ha esito negativo con codice motivo MQRC_Q_MGR_NOT_AVAILABLE.

Importante: Su molti sistemi operativi, affinché l'aggiunta di un utente a un gruppo venga riconosciuta, l'utente in questione deve scollegarsi e ricollegarsi.

La modalità con restrizioni funziona con il servizio di autorizzazione IBM MQ . Pertanto, è necessario concedere agli utenti anche l'autorità di connettersi a IBM MQ e accedere alle risorse richieste utilizzando il servizio di autorizzazione IBM MQ .

ULW Ulteriori informazioni sulla configurazione del servizio di autorizzazione IBM MQ sono disponibili in Impostazione della sicurezza sui sistemi UNIX, Linux, and Windows.

Utilizzare la modalità limitata IBM MQ solo quando il controllo fornito dal servizio di autorizzazione non fornisce un isolamento sufficiente delle risorse del gestore code.

Riferimenti correlati
`crtmqm` (crea gestore code)

Multi Stanza di sicurezza del file qm.ini

La stanza Sicurezza specifica le 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.

Windows **GroupModel=GlobalGroups**
Questo attributo determina se OAM controlla i gruppi globali quando determina l'appartenenza a un gruppo di utenti 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 dei gruppi globali; consultare il parametro **`setmqaut`** `-g` .

Nota: Se si imposta `ClusterQueueAcessControl=RQMName` e si dispone di una implementazione personalizzata del servizio di autorizzazione inferiore a `MQZAS_VERSION_6` , il gestore code non viene avviato. In questa istanza, impostare `ClusterQueueAcessControl=Xmitq` o aggiornare il servizio di autorizzazione personalizzato a `MQZAS_VERSION_6` o superiore.

Stanza di esempio

```
Security:
      ClusterQueueAccessControl=Xmitq
      GroupModel=GlobalGroups
```

Multi Stanza di servizio del file qm.ini

La stanza Service viene utilizzata per apportare modifiche ai servizi installabili. Questa stanza contiene il nome e il numero di punti di ingresso definiti per il servizio.

Nota: Linux Windows La modifica dei servizi installabili e dei relativi componenti ha implicazioni significative. Per questo motivo, i servizi installabili sono di sola lettura in IBM MQ Explorer.

Per ogni componente all'interno di un servizio, è necessario anche specificare nome e percorso del modulo contenente il codice per tale componente. Utilizzare la stanza ServiceComponent per questo.

Le stanze **Service** e **ServiceComponent** possono essere presenti in qualsiasi ordine e le relative chiavi possono essere presenti anche in qualsiasi ordine. Per una di queste stanze, tutte le chiavi della stanza devono essere presenti. Se una chiave di stanza è duplicata, viene utilizzata l'ultima.

All'avvio, il gestore code elabora ciascuna voce del componente del servizio nel file di configurazione a turno. Quindi carica il modulo del componente specificato, richiamando il punto di ingresso del componente (che deve essere il punto di ingresso per l'inizializzazione del componente), passando ad esso un handle di configurazione.

Nome = AuthorizationService (predefinito) |NameService
Il nome del servizio richiesto.

AuthorizationService
Per IBM 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 stanze ServiceComponent .

Linux AIX Le seguenti stanze nel file di configurazione del gestore code definiscono due componenti del servizio di autorizzazione su IBM MQ for AIX. *MQ_INSTALLATION_PATH* rappresenta la directory di livello superiore in cui è installato IBM MQ .

```
 Service:
    Name=AuthorizationService
    EntryPoints=13

 ServiceComponent:
    Service=AuthorizationService
    Name=MQSeries.UNIX.auth.service
Module= MQ_INSTALLATION_PATH/lib/amqzfu
    ComponentDataSize=0

 ServiceComponent:
    Service=AuthorizationService
    Name=user.defined.authorization.service
    Module=/usr/bin/udas01
    ComponentDataSize=96
```

Figura 6. UNIX and Linux stanze del servizio di autorizzazione in qm.ini

Linux AIX La stanza del componente servizio (`MQSeries.UNIX.auth.service`) definisce il componente del servizio di autorizzazione predefinito, OAM. Se si rimuove questa stanza e si riavvia il gestore code, l'OAM viene disabilitato e non viene eseguito alcun controllo di autorizzazione.

Windows È anche possibile aggiungere l'attributo `SecurityPolicy` utilizzando i servizi IBM MQ . L'attributo `SecurityPolicy` si applica solo se il servizio specificato nella stanza *`Service`* è il servizio di autorizzazione, ossia l'OAM predefinito. L'attributo `SecurityPolicy` consente di specificare la politica di sicurezza per ciascun gestore code. I valori possibili sono:

`Default`
Specificare `Default` se si desidera che la politica di sicurezza predefinita abbia effetto. Se un identificativo di sicurezza Windows (SID NT) non viene passato all'OAM per un determinato ID utente, viene effettuato un tentativo di ottenere il SID appropriato ricercando i database di sicurezza pertinenti.

`NTSIDsRequired`
Richiede che un SID NT venga passato a OAM quando si eseguono i controlli di sicurezza.

Windows La stanza del componente del servizio, `MQSeries.WindowsNT.auth.service` definisce il componente del servizio di autorizzazione predefinito, OAM. Se si rimuove questa stanza e si riavvia il gestore code, l'OAM viene disabilitato e non viene eseguito alcun controllo di autorizzazione.

NameService
Per impostazione predefinita, non viene fornito alcun servizio nomi. Se si richiede un servizio nomi, è necessario aggiungere manualmente la stanza `NameService` .

Linux AIX I seguenti esempi di stanze del file di configurazione UNIX and Linux per il servizio nomi specificano un componente servizio nomi fornito dalla società ABC (fittizia).

```
# Stanza for name service
 Service:
    Name=NameService
    EntryPoints=5

# Stanza for name service component, provided by ABC
 ServiceComponent:
    Service=NameService
    Name=ABC.Name.Service
    Module=/usr/lib/abcname
    ComponentDataSize=1024
```

Figura 7. Stanze del servizio dei nomi in qm.ini (per sistemi UNIX and Linux)

EntryPoints= *numero di voci*
Il numero di punti di entrata definiti per il servizio.

Ciò include i punti di ingresso di inizializzazione e terminazione.

Windows **SecurityPolicy= Predefinito |NTSIDsRequired**
Sui sistemi Windows , l'attributo **`SecurityPolicy`** si applica solo se il servizio specificato è il servizio di autorizzazione predefinito, ossia OAM. L'attributo **`SecurityPolicy`** consente di specificare la politica di sicurezza per ciascun gestore code.

I valori possibili sono:

Valore predefinito
Utilizzare la politica di sicurezza predefinita per rendere effettiva. Se un identificativo di sicurezza Windows (SID NT) non viene passato all'OAM per un determinato 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, vedere SID (security identifier)Windows.

Consultare anche Configurazione delle stanze del servizio di autorizzazione: sistemi Windows.

Linux UNIX **SecurityPolicy= utente|gruppo|predefinito**

Sui sistemi UNIX and Linux , il valore specifica se il gestore code utilizza l'autorizzazione basata sull'utente o sul gruppo. I valori non sono sensibili al maiuscolo / minuscolo.

Se non si include l'attributo **SecurityPolicy** , viene utilizzato `default` , che utilizza l'autorizzazione basata sul gruppo.

Riavviare il gestore code per rendere effettive le modifiche. Consultare anche Configurazione delle stanze del servizio di autorizzazione: sistemi Windows.

SharedBindingsUserId= *tipo - utente*

L'attributo **SharedBindingsUserId** si applica solo se il servizio specificato è il servizio di autorizzazione predefinito, ovvero l'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:

Valore predefinito
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'attributo **FastpathBindingsUserId** si applica solo se il servizio specificato è il servizio di autorizzazione predefinito, ovvero 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:

Valore predefinito
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, ovvero l'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:

Valore predefinito
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, and Windows.

Per ulteriori informazioni sui servizi di sicurezza in generale, consultare Configurazione della sicurezza sui sistemi UNIX and Linux.

Stanza di esempio

```
Service:
   Name=AuthorizationService
   EntryPoints=14
```

Concetti correlati
Componenti e servizi installabili per AIX, Linuxe Windows
Riferimenti correlati
Componenti e servizi installabili su IBM i
Informazioni di riferimento sui servizi installabili

Multi Stanza ServiceComponent del file qm.ini

La stanza ServiceComponent specifica le informazioni per il componente del servizio. È necessario specificare le informazioni sul componente del servizio quando viene aggiunto un nuovo servizio installabile. La stanza del servizio di autorizzazione è presente per impostazione predefinita e il componente associato, OAM, è attivo.

Le stanze **Service** e **ServiceComponent** possono essere presenti in qualsiasi ordine e le relative chiavi possono essere presenti anche in qualsiasi ordine. Per una di queste stanze, tutte le chiavi della stanza devono essere presenti. Se una chiave di stanza è duplicata, viene utilizzata l'ultima.

All'avvio, il gestore code elabora ciascuna voce del componente del servizio nel file di configurazione a turno. Quindi carica il modulo del componente specificato, richiamando il punto di ingresso del componente (che deve essere il punto di ingresso per l'inizializzazione del componente), passando ad esso un handle di configurazione.

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 IBM 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.

Stanza di esempio

```
ServiceComponent:
   Service=AuthorizationService
   Name=MQSeries.UNIX.auth.service
   Module=amqzfu
   ComponentDataSize=0
```

Per ulteriori esempi che mostrano una stanza AuthorizationService e le stanze ServiceComponent associate e una stanza NameService e la stanza ServiceComponent associata, consultare “Stanza di servizio del file qm.ini” a pagina 131.

Concetti correlati

Componenti e servizi installabili per AIX, Linuxe Windows

Riferimenti correlati

“Stanza di servizio del file qm.ini” a pagina 131

La stanza Service viene utilizzata per apportare modifiche ai servizi installabili. Questa stanza contiene il nome e il numero di punti di ingresso definiti per il servizio.

Componenti e servizi installabili su IBM i

Informazioni di riferimento sui servizi installabili

Windows Stanza SPX del file qm.ini (soloWindows)

La stanza SPX specifica i parametri di configurazione del protocollo SPX. Questi parametri sovrascrivono gli attributi predefiniti per i canali.

Utilizzare la stanza SPX nel file `qm.ini` per specificare i parametri di configurazione del protocollo SPX.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la pagina delle proprietà del gestore code IBM MQ Explorer SPX .

Socket = 5E86 (predefinito) | *socket_number*
Il numero di socket SPX in notazione esadecimale. Il valore predefinito è X'5E86'.

BoardNum= 0 (predefinito) | *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= *DLLName1*
Il nome della DLL SPX.

Il valore predefinito è WSOCK32.DLL.

Library2= *DLLName2*
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 mostrati in Tabella 13 a pagina 136.

Tabella 13. Richieste di connessione in sospeso predefinite (SPX)	
Piattaforma	**Valore predefinito ListenerBacklog**
Windows Server	100
Windows Workstation	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 13 a pagina 136, 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 connessioni client, il client riceve un codice motivo MQRC_Q_MGR_NOT_AVAILABLE da `MQCONN` e deve ritentare la connessione in un secondo momento.

Multi Stanza SSL del file qm.ini

La stanza SSL viene utilizzata per configurare i canali TLS su un 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 stanza SSL nel file `qm.ini` per configurare il modo in cui i canali TLS sul gestore code tentano di utilizzare le funzioni riportate di seguito e il modo in cui reagiscono se si verificano 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.

AllowOutboundSNI = YES (predefinito) | NO
Se abilitata, i client con capacità SNI imposteranno SNI sul nome del canale IBM MQ di destinazione sul sistema remoto quando si avvia una connessione TLS. Se questo attributo è impostato su `NO`, i client con supporto SNI non imposteranno l'intestazione SNI causando la ricezione da parte delle richieste di connessione in uscita del certificato predefinito del gestore code remoto durante l'handshake TLS e, pertanto, i certificati per canale non possono essere utilizzati.

V 9.1.1 **AllowedCipherSpecifiche =*nome*|*elenco nomi*| ALL**

Specifica un elenco personalizzato di CipherSpecs abilitati per l'utilizzo con i canali IBM MQ su Multiplatforms.

- Un singolo nome CipherSpec oppure
- Un elenco separato da virgole di nomi IBM MQ CipherSpec da riabilitare o
- Il valore speciale di ALL, che rappresenta tutte le CipherSpecs (non consigliato).

Nota: L'abilitazione di **ALL** CipherSpecs non è consigliata poiché abiliterà i protocolli SSL 3.0 e TLS 1.0 e un numero elevato di algoritmi crittografici deboli.

Per ulteriori informazioni, consultare Providing a custom list of enabled CipherSpecs on Multiplatforms in Enabling CipherSpecs.

ULW V 9.1.4 **AllowTLSV13 =Y | YES | T | TRUE| N | NO | F | FALSE**

Specifica se un gestore code è in grado di utilizzare TLS 1.3 CipherSpecs.

- Y, YES, To TRUE: abilita TLS 1.3 che consente al gestore code di utilizzare i CipherSpecsTLS 1.3 .
- N, NO, Fo FALSE: disabilita TLS 1.3, il che significa che il gestore code non è in grado di utilizzare i CipherSpecsTLS 1.3 .

Per ulteriori informazioni, consultare Abilitazione di CipherSpecs.

CDPCheckExtensions= SÌ |NO (predefinito)

Specifica se i canali TLS su questo gestore code tentano di controllare i server CDP denominati nelle estensioni certificato del punto CrlDistribution.

- YES (valore predefinito): i canali TLS tentano di controllare i server CDP per stabilire se un certificato digitale è revocato.
- NO: i canali TLS non tentano di controllare i server CDP. Questo è il valore predefinito.

ULW V 9.1.4 **MinimumRSAKeySize=int**

Specifica la dimensione chiave minima che i certificati RSA devono avere per essere accettati durante un handshake TLS. Consente qualsiasi valore uguale o superiore a 0. Se non specificato, il valore predefinito è 1.

OCSPAuthentication=REQUIRED (predefinito) | WARN | OPTIONAL

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 del canale 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** .

- REQUIRED (valore predefinito): l'errore di determinazione dello stato di revoca causa la chiusura della connessione con 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 (valore predefinito) | NO

Specifica se i canali TLS su questo gestore code tentano di controllare i server OCSP denominati nelle estensioni certificato di accesso AuthorityInfo.

- YES (valore predefinito): i canali TLS provano a controllare i server OCSP per determinare se un certificato digitale è revocato. Questo è il valore predefinito.

- NO: i canali TLS non tentano di controllare i server OCSP.

ULW V 9.1.5 **OCSPTimeout= *numero***

Il numero di secondi di attesa per un responder OCSP durante l'esecuzione di una verifica di revoca.

Se non viene impostato alcun valore, viene utilizzato il valore predefinito IBM MQ di 30 secondi.

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).

Solaris AIX Per i client a 32 bit su piattaforme AIX, e Solaris SPARC, l'indirizzo di rete può essere solo un IPv4 .

Su altre piattaforme, l'indirizzo di rete 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.

ULW V 9.1.5 **SSLHTTPConnectTimeout= *numero*|0**

Il numero di secondi di attesa per stabilire correttamente una connessione di rete a un server HTTP durante l'esecuzione di un controllo di revoca.

Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ 0 (off).

Stanza di esempio

```
SSL:
       OutboundSNI=CHANNEL
      AllowedCipherSpecs=TLS13 CipherSpec list
      AllowTLSV13=Y
      CDPCheckExtensions=NO
      MinimumRSAKeySize=1
      OCSPAuthentication=REQUIRED
      OCSPCheckExtensions=YES
      OCSPTimeout=30
      SSLHTTPConnectTimeout=0
```

Note:

- Il valore predefinito per **OutboundSNI** è `Canale`.
- V 9.1.1 L'elenco **TLS13 CipherSpec** è un elenco di specifiche CipherSpecs non le cifrature alias. Se si richiedono solo cifrature TLS1.3 , è necessario elencarle. Ad esempio:

  TLS_CHACHA20_POLY1305_SHA256
  TLS_AES_256_GCM_SHA384
  TLS_AES_128_GCM_SHA256
  TLS_AES_128_CCM_SHA256
  TLS_AES_128_CCM_8_SHA256

- V 9.1.4 Il valore predefinito per **AllowTLSV13** è Y a meno che non siano state abilitate le cifrature deboli, nel qual caso viene disattivato (a meno che non venga esplicitamente attivato).
- I valori per **CDPCheckExtensions** possono essere solo `Sì` o `No`.

Multi Stanza del pool secondario del file qm.ini

Questa stanza è creata da IBM MQ. Non modificarlo.

La stanza del pool secondario e l'attributo **ShortSubpoolName** all'interno di tale stanza vengono scritti automaticamente da IBM MQ quando si crea un gestore code. IBM MQ sceglie un valore per **ShortSubpoolName**. Non modificare questo valore.

Il nome corrisponde a una directory e a un collegamento simbolico creati all'interno della directory `/var/mqm/sockets` , che IBM MQ utilizza per le comunicazioni interne tra i suoi processi in esecuzione.

Multi Stanza TCP del file qm.ini

La stanza TCP specifica i parametri di configurazione TCP/IP (Transmission Control Protocol/Internet Protocol). Questi parametri sovrascrivono gli attributi predefiniti per i canali.

Utilizzare la sezione TCP nel file `qm.ini` per specificare i parametri di configurazione TCP/IP.

Linux Windows In alternativa, in Linux (x86 e x86-64) e in Windows, utilizzare la pagina delle proprietà del gestore code TCP IBM MQ Explorer SPX .

Porta = 1414 (predefinito) | *numero_porta*
Il numero di porta predefinito, in notazione decimale, per le sessioni TCP/IP. Il numero di porta *ben noto* per IBM MQ è 1414.

Windows **Library1= *DLLName1* (soloWindows)**
Il nome della DLL socket TCP/IP.

Il valore predefinito è WSOCK32.

KeepAlive= NO (valore predefinito) |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 come un backlog di richieste in attesa sulla porta TCP/IP affinché il listener accetti la richiesta. I valori di backlog del listener predefiniti vengono mostrati in Tabella 14 a pagina 139.

Tabella 14. Richieste di connessione in sospeso predefinite (TCP)

Piattaforma	Valore predefinito ListenerBacklog
Windows ServerWindows	100
Linux Linux	100
Solaris Solaris	100
AIX AIX V5.3 o successive	100

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 14 a pagina 139, 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 successivamente.

Il seguente gruppo di proprietà può essere utilizzato per controllare la dimensione dei buffer utilizzati da TCP/IP. I valori vengono passati direttamente al livello TCP/IP del sistema operativo. Prestare molta attenzione quando si utilizzano queste proprietà. Se i valori non sono impostati correttamente, possono influire negativamente sulle prestazioni TCP/IP. Per ulteriori informazioni su come ciò influisce sulle prestazioni, fare riferimento alla documentazione TCP/IP per il proprio ambiente. Un valore zero indica che il sistema operativo gestirà le dimensioni del buffer, in contrapposizione alle dimensioni del buffer fissate da IBM MQ.

Connect_Timeout= 0 (valore predefinito) |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.

I processi del canale IBM MQ si collegano su socket non bloccanti. Pertanto, se l'altra estremità del socket non è pronta, connect () restituisce immediatamente *EINPROGRESS* o *EWOULDBLOCK*. In seguito, la connessione verrà tentata di nuovo, fino a un totale di 20 tentativi, quando viene notificato un errore di comunicazione.

Se `Connect_Timeout` è impostato su un valore diverso da zero, IBM MQ attende il periodo stabilito per la chiamata select () affinché il socket sia pronto. Ciò aumenta le possibilità di riuscita di una chiamata connect () successiva. Questa opzione potrebbe essere utile in situazioni in cui le connessioni richiedono un periodo di attesa, a causa di un carico elevato sulla rete.

SndBuffSize = numero |0 (valore predefinito)
La dimensione in byte del buffer di invio TCP/IP utilizzato dalla fine di invio dei canali. Questo valore di stanza può essere sovrascritto da una stanza più specifica per il tipo di canale, ad esempio RcvSndBuffSize. Se il valore è impostato su 0, vengono utilizzati i valori predefiniti del sistema operativo. Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ , 32768.

Multi Da IBM MQ 8.0, i nuovi gestori code vengono creati automaticamente con un'impostazione predefinita di 0 (consultare “Stanza di esempio” a pagina 141.

RcvBuffSize = numero |0 (predefinito)
La dimensione in byte del buffer di ricezione TCP/IP utilizzato dall'estremità di ricezione dei canali. Questo valore di stanza può essere sovrascritto da una stanza più specifica per il tipo di canale, ad esempio RcvRcvBuffSize. Se il valore è impostato su 0, vengono utilizzati i valori predefiniti del sistema operativo. Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ , 32768.

Multi Da IBM MQ 8.0, i nuovi gestori code vengono creati automaticamente con un'impostazione predefinita di 0 (consultare “Stanza di esempio” a pagina 141.

RcvSndBuffSize = numero0 (valore predefinito)
La dimensione in byte del buffer di invio TCP/IP utilizzato dall'estremità mittente di un canale ricevente. Se il valore è impostato su 0, vengono utilizzati i valori predefiniti del sistema operativo. Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ , 32768.

Multi Da IBM MQ 8.0, i nuovi gestori code vengono creati automaticamente con un'impostazione predefinita di 0 (consultare “Stanza di esempio” a pagina 141.

RcvRcvBuffSize = numero |0 (valore predefinito)
La dimensione in byte del buffer di ricezione TCP/IP utilizzato dall'estremità di ricezione di un canale ricevente. Se il valore è impostato su 0, vengono utilizzati i valori predefiniti del sistema operativo. Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ , 32768.

Multi Da IBM MQ 8.0, i nuovi gestori code vengono creati automaticamente con un'impostazione predefinita di 0 (consultare “Stanza di esempio” a pagina 141.

SvrSndBuffSize = numero |0 (valore predefinito)
La dimensione in byte del buffer di invio TCP/IP utilizzato dall'estremità del server di un canale di connessione server di connessione client. Se il valore è impostato su 0, vengono utilizzati i valori predefiniti del sistema operativo. Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ , 32768.

Multi Da IBM MQ 8.0, i nuovi gestori code vengono creati automaticamente con un'impostazione predefinita di 0 (consultare “Stanza di esempio” a pagina 141.

SvrRcvBuffSize = numero |0 (valore predefinito)
La dimensione in byte del buffer di ricezione TCP/IP utilizzato dall'estremità server di un canale di connessione server di connessione client. Se il valore è impostato su 0, vengono utilizzati i valori predefiniti del sistema operativo. Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ , 32768.

Multi Da IBM MQ 8.0, i nuovi gestori code vengono creati automaticamente con l'impostazione predefinita 0 (consultare “Stanza di esempio” a pagina 141).

Stanza di esempio

```
TCP:
   SndBuffSize=0
   RcvBuffSize=0
   RcvSndBuffSize=0
   RcvRcvBuffSize=0
   ClntSndBuffSize=0
   ClntRcvBuffSize=0
   SvrSndBuffSize=0
   SvrRcvBuffSize=0
```

Nota: Multi Per i nuovi gestori code su Multiplatforms, le dimensioni buffer di invio e ricezione TCP predefinite nella stanza TCP di `qm.ini file` sono impostate per essere gestite dal sistema operativo. Come mostrato nell'esempio precedente, i nuovi gestori code vengono creati automaticamente con l'impostazione predefinita 0 per i buffer di invio e ricezione. Ciò si applica solo ai gestori code nuovi. Le impostazioni del buffer di invio e ricezione TCP per i gestori code migrati dalle precedenti versioni di IBM MQ vengono conservate.

Se le proprietà della dimensione del buffer TCP vengono rimosse dal file `qm.ini` , il buffer predefinito è impostato su 32K. È necessario prestare attenzione quando si utilizza questo valore predefinito poiché 32K potrebbe non essere un buffer appropriato per tutti gli scenari di messaggistica.

Se le proprietà del buffer di invio e ricezione TCP sono impostate su zero, vengono utilizzati i valori predefiniti del sistema operativo. Il metodo per la scelta di questi valori predefiniti varia a seconda del sistema operativo, ma in genere può essere trovato nelle pagine del manuale del sistema operativo "tcp" o get/setsockopt ().

Multi V 9.1.0 Stanza `TuningParameters` del file qm.ini

La stanza TuningParameters specifica le opzioni per l'ottimizzazione del gestore code.

SuppressDspAuthFail= YES |NO (valore predefinito)
Quando è impostato su YES, il gestore code sopprime la creazione di eventi di autorizzazione e la scrittura di messaggi di errore AMQ8077 nel log degli errori quando un controllo di autorizzazione ha esito negativo, se la connessione non dispone dell'autorizzazione + dsp per un oggetto.

ImplSyncOpenOutput=*valore*
`ImplSyncOpenOutput` è il numero minimo di applicazioni che hanno la coda aperta per l'inserimento, prima che un punto di sincronizzazione implicito possa essere abilitato per un inserimento persistente, al di fuori del punto di sincronizzazione. Il valore predefinito di **`ImplSyncOpenOutput`** è 2.

Ciò ha l'effetto che se esiste solo un'applicazione che ha quella coda aperta per un'operazione di inserimento, **`ImplSyncOpenOutput`** viene disattivato.

Specificare `ImplSyncOpenOutput=1` significa che viene sempre considerato un punto di sincronizzazione implicito. È possibile impostare qualsiasi numero intero positivo. Se non si desidera mai aggiungere un punto di sincronizzazione implicito, impostare `ImplSyncOpenOutput=OFF`.

V 9.1.2 **UniformClusterNome =*nome del cluster***
Il nome del cluster IBM MQ che si sta utilizzando come cluster uniforme.

V 9.1.0.9 **OAMLdapConnectTimeout=ora|0 (predefinito)**
Il tempo massimo, in secondi, che il client LDAP attenderà per stabilire una connessione TCP al server. Se si stanno fornendo più server LDAP tramite un elenco nomi di connessione, il timeout si applica a ogni singolo tentativo di connessione, e quindi si tenta una connessione alla voce successiva nell'elenco nomi se questo timeout viene raggiunto.

`time` ha un valore massimo di 3600 secondi e un valore di `0`, che è il valore minimo e il valore predefinito, significa che l'attesa è illimitata.

V 9.1.0.9 **OAMLdapQueryTimeLimit=ora|0 (predefinito)**
Il tempo massimo, in secondi, che il client LDAP attende per ricevere una risposta a una richiesta LDAP dal server, una volta stabilita una connessione e inviata una richiesta LDAP.

`time` ha un valore massimo di 3600 secondi e un valore di `0`, che è il valore minimo e il valore predefinito, significa che l'attesa è illimitata.

V 9.1.0.15 **OAMLdapResponseWarningTime=*soglia***
Se una connessione a un server LDAP ha impiegato più tempo del numero di soglia di secondi specificato dal parametro **OAMLdapResponseWarningTime** , un messaggio AMQ5544W verrà scritto nel log degli errori. La soglia predefinita è 10 secondi.

ExpiryInterval
Indica la frequenza con cui il gestore code esegue la scansione delle code alla ricerca di messaggi scaduti che non sono stati già ripuliti da altre attività della coda. Si tratta di un intervallo di tempo in secondi.

Per impostazione predefinita, lo scanner di scadenza viene eseguito approssimativamente ogni 5 minuti sulle build IBM MQ di produzione.

Avvertenza: La modifica del valore **ExpiryInterval** non è generalmente richiesta ed è necessario modificare questo valore solo sotto la guida del supporto IBM .

Stanza di esempio

V 9.1.0.15

```
TuningParameters:
       SuppressDspAuthFail=NO
       ImplSyncOpenOutput=2
       OAMLdapConnectTimeout=60
       OAMLdapQueryTimeLimit=60
       OAMLdapResponseWarningTime=10
       ExpiryInterval=300
```

Concetti correlati
Punto di sincronizzazione implicito

Multi V 9.1.4 Stanza delle variabili del file qm.ini

La stanza Variabili specifica le variabili di configurazione da utilizzare con i cluster uniformi automatici.

È possibile utilizzare gli attributi elencati nella stanza Variables durante la configurazione cluster automatica di CONNAME e i campi MQSC del nome canale di un canale ricevente del cluster. Le variabili di configurazione non possono essere utilizzate in nessun altro elemento di uno script MQSC.

attributo=valore
Specifica un nome e il valore associato da utilizzare come inserimento durante le definizioni MQSC.

Le coppie *attribute=value* possono essere fornite utilizzando l'opzione della riga comandi **-iv** nel comando **crtmqm** quando si crea un gestore code.

Stanza di esempio

```
Variables:
       CONNAME=127.0.0.1(1414)
```

Concetti correlati

Bilanciamento automatico dell'applicazione

Attività correlate

Creazione di un nuovo cluster uniforme

Riferimenti correlati

Utilizzo della configurazione automatica del cluster

Multi Stanza XAResourceManager del file qm.ini

La stanza XAResourceManager per specificare le informazioni sui gestori risorse coinvolti nelle unità di lavoro globali coordinate dal gestore code.

Utilizzare la stanza XAResourceManager nel file `qm.ini` per specificare le informazioni sui gestori risorse coinvolti nelle unità di lavoro globali coordinate dal gestore code.

Linux Windows In alternativa, su Linux (x86 e x86-64) e Windows, utilizzare la IBM MQ Explorer pagina delle propriet ... del gestore code XA.

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.

IBM 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 delle 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 delle 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 delle 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 delle informazioni di configurazione del gestore risorse per Informix

e consultare la documentazione del database per la stringa appropriata.

Controllo ThreadOf= THREAD | PROCESS

Questo attributo è obbligatorio 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 IBM 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 IBM 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.

Stanza di esempio

```
XAResourceManager:
   Name=DB2 Resource Manager Bank
   SwitchFile=/usr/bin/db2swit
   XAOpenString=MQBankDB
   XACloseString=
   ThreadOfControl=THREAD
```

Nota: 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.

 File qm.ini di esempio per IBM i

Un esempio che mostra il modo in cui i gruppi di attributi possono essere organizzati in un file di configurazione del gestore code per IBM i.

```
#********************************************************************#
#* Module Name: qm.ini                                              *#
#* Type       : IBM MQ queue manager configuration file             *#
# Function    : Define the configuration of a single queue manager *#
#*                                                                  *#
#********************************************************************#
#* Notes      :                                                     *#
#* 1) This file defines the configuration of the queue manager     *#
#*                                                                  *#
#********************************************************************#
Log:
LogPath=QMSATURN.Q
LogReceiverSize=65536

CHANNELS:
```

```
MaxChannels = 20       ; Maximum number of channels allowed.
                       ; Default is 100.
MaxActiveChannels = 10 ; Maximum number of channels allowed to be
                       ; active at any time. The default is the
                       ; value of MaxChannels.

TCP:                   ; TCP/IP entries.
KeepAlive = Yes        ; Switch KeepAlive on.
SvrSndBuffSize=20000   ; Size in bytes of the TCP/IP send buffer for each
                       ; channel instance. Default is 32768.
SvrRcvBuffSize=20000   ; Size in bytes of the TCP/IP receive buffer for each
                       ; channel instance. Default is 32768.
Connect_Timeout=10000  ; Number of seconds before an attempt to connect the
                       ; channel instance times out. Default is zero (no timeout).

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

TuningParameters:
   ImplSyncOpenOutput=2
```

ULW File di configurazione dell'installazione, mqinst.ini

Su UNIX o Linux, il file di configurazione dell'installazione, `mqinst.ini`, contiene informazioni su tutte le installazioni IBM MQ . Su Windows, le informazioni di configurazione dell'installazione si trovano nel registro.

Ubicazione del file `mqinst.ini`

Linux UNIX

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

Importante: Il file `mqinst.ini` non deve essere modificato o a cui si fa riferimento direttamente poiché il formato non è fisso e potrebbe essere modificato.

L'identificativo di installazione, solo per uso interno, è impostato automaticamente e non deve essere modificato.

Invece di modificare direttamente il file `mqinst.ini`, è necessario utilizzare i seguenti comandi per creare, eliminare, interrogare e modificare i valori nel file:

crtmqinst per creare voci.
dltmqinst per eliminare le voci.
dspmqinst per visualizzare le voci.
setmqinst per impostare le voci.

Informazioni sulla configurazione dell'installazione su Windows

Windows

Non esiste alcun file `mqinst.ini` su Windows. Le informazioni di configurazione dell'installazione si trovano nel registro e si trovano nella seguente chiave:

```
HKLM\SOFTWARE\IBM\WebSphere MQ\Installation\InstallationName
```

Importante: Questa chiave non deve essere modificata o a cui si fa riferimento direttamente poiché il suo formato non è fisso e potrebbe cambiare.

Invece, è necessario utilizzare i comandi seguenti per interrogare e modificare i valori nel Registro di sistema:

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.

Multi IBM MQ MQI client file di configurazione, mqclient.ini

I client vengono configurati 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 IBM MQ MQI clients utilizzando un file di testo, simile al file di configurazione del gestore code, `qm.ini`. Il file contiene un numero di stanze, ognuna delle quali contiene un numero di righe del formato **attribute-name** = *valore*.

Il file di configurazione IBM MQ MQI client è generalmente denominato `mqclient.ini` , ma è possibile scegliere di assegnarvi un altro nome. Le informazioni di configurazione in questo file si applicano alle seguenti piattaforme:

- ULW UNIX, Linux, and Windows
- IBM i IBM i

  Nota: Su IBM i, non esiste alcun file `mqclient.ini` predefinito. Tuttavia, è possibile creare il file nell'IFS (Integrated File System) IBM i Integrated File System .

Per ulteriori informazioni, consultare “Ubicazione del file di configurazione client” a pagina 148.

Nota: z/OS La piattaforma z/OS non può essere utilizzata per eseguire client IBM MQ . Pertanto, il file `mqclient.ini` non è presente su IBM MQ for z/OS.

Gli attributi nel file di configurazione IBM MQ MQI client si applicano ai client che utilizzano:

- L'MQI
- IBM MQ classes for Java
- IBM MQ classes for JMS
- IBM MQ classes for .NET
- XMS

Anche se gli attributi nel file di configurazione IBM MQ MQI client si applicano alla maggior parte dei client IBM MQ , esistono alcuni attributi che non vengono letti dai client .NET e XMS .NET gestiti o dai client che utilizzano IBM MQ classes for Java o IBM MQ classes for JMS. Per ulteriori informazioni, consultare “Quali client IBM MQ possono leggere ciascun attributo” a pagina 149.

Le funzioni di configurazione si applicano a tutte le connessioni che un'applicazione client effettua 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).

V 9.1.2 Di seguito è riportato un esempio di un file di configurazione client per Continuous Delivery da IBM MQ 9.1.2:

```
#* Module Name: mqclient.ini                                          *#
#* Type       : IBM MQ MQI client configuration file                  *#
#  Function   : Define the configuration of a client                  *#
#*                                                                    *#
```

```
#********************************************************************#
#* Notes      :                                                       *#
#* 1) This file defines the configuration of a client              *#
#*                                                                    *#
#********************************************************************#

ClientExitPath:
   ExitsDefaultPath=/var/mqm/exits
   ExitsDefaultPath64=/var/mqm/exits64

TCP:
   Library1=DLLName1
   KeepAlive = Yes
   ClntSndBuffSize=32768
   ClntRcvBuffSize=32768
   Connect_Timeout=0

MessageBuffer:
   MaximumSize=-1
   Updatepercentage=-1
   PurgeTime=0

LU62:
   TPName
   Library1=DLLName1
   Library2=DLLName2

PreConnect:
    Module=myMod
    Function=myFunc
    Data=ldap://myLDAPServer.com:389/cn=wmq,ou=ibm,ou=com
    Sequence=1

CHANNELS:
DefRecon=YES
      ServerConnectionParms=SALES.SVRCONN/TCP/hostname.x.com(1414)

Connection:
     ApplName=ExampleApplName
```

Di seguito è riportato un esempio di file di configurazione client per IBM MQ 9.1.0 Long Term Support release e Continuous Delivery prima di IBM MQ 9.1.2:

```
#* Module Name: mqclient.ini                                         *#
#* Type       : IBM MQ MQI client configuration file                 *#
#  Function   : Define the configuration of a client                 *#
#*                                                                    *#
#********************************************************************#
#* Notes      :                                                       *#
#* 1) This file defines the configuration of a client              *#
#*                                                                    *#
#********************************************************************#

ClientExitPath:
   ExitsDefaultPath=/var/mqm/exits
   ExitsDefaultPath64=/var/mqm/exits64

TCP:
   Library1=DLLName1
   KeepAlive = Yes
   ClntSndBuffSize=32768
   ClntRcvBuffSize=32768
   Connect_Timeout=0

MessageBuffer:
   MaximumSize=-1
   Updatepercentage=-1
   PurgeTime=0

LU62:
   TPName
   Library1=DLLName1
   Library2=DLLName2

PreConnect:
    Module=myMod
    Function=myFunc
    Data=ldap://myLDAPServer.com:389/cn=wmq,ou=ibm,ou=com
    Sequence=1
```

```
CHANNELS:
DefRecon=YES
ServerConnectionParms=SALES.SVRCONN/TCP/hostname.x.com(1414)
```

Non è possibile impostare più connessioni di canale utilizzando il file di configurazione client.

Le variabili di ambiente supportate nelle release precedenti a IBM WebSphere MQ 7.0 continuano ad essere supportate nelle release successive 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 MQ classes for JMS, è anche possibile sovrascrivere il file di configurazione client nei modi seguenti:

- Impostando le proprietà nel file di configurazione JMS .
- Impostando le proprietà di sistema Java , che sovrascrive anche il file di configurazione JMS .

Per il client .NET , è possibile anche sovrascrivere il file di configurazione client e le variabili di ambiente equivalenti utilizzando il file di configurazione dell'applicazione .NET .

Commenti nel file di configurazione

Linux UNIX

È possibile utilizzare il punto e virgola '`;`' e l'hash '`#`' per contrassegnare l'inizio di un commento all'interno del file di configurazione. Ciò può contrassegnare un'intera riga come commento o indicare un commento alla fine di una riga che non verrà incluso nel valore di un'impostazione.

Se un valore richiede uno di questi caratteri, è necessario eseguire l'escape di tale carattere utilizzando il carattere barra rovesciata '\'.

Il seguente esempio mostra l'utilizzo dei commenti nel file di configurazione:

```
# Example of an SSL stanza with comments
SSL:
    ClientRevocationChecks=REQUIRED ; Example of an end of line comment
    SSLCryptoHardware=GSK_PKCS11=/driver\;label\;password\;SYMMETRIC_CIPHER_ON # Example of
escaped comment characters.
```

Concetti correlati

“Quali client IBM MQ possono leggere ciascun attributo” a pagina 149
La maggior parte degli attributi nel file di configurazione IBM 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 MQ classes for Java o IBM MQ classes for JMS.

Riferimenti correlati

“Ubicazione del file di configurazione client” a pagina 148
Un file di configurazione IBM MQ MQI client può essere contenuto in un numero di ubicazioni.

Ubicazione del file di configurazione client

Un file di configurazione IBM MQ MQI client può essere contenuto in un numero di ubicazioni.

Un'applicazione del client utilizza il seguente percorso di ricerca per individuare il file di configurazione IBM MQ MQI client :

1. L'ubicazione specificata dalla variabile di ambiente MQCLNTCF.

   Il formato di questa variabile di ambiente è un URLcompleto. 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.

   Note:

- 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 i 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 MQCLNTCF Java .

2. Un file denominato `mqclient.ini` nella directory di lavoro corrente dell'applicazione.
3. Un file denominato `mqclient.ini` nella directory di dati IBM MQ per sistemi Windows, UNIX and Linux .

   Note:

   - La directory di dati IBM MQ non esiste su determinate piattaforme, ad esempio IBM i e z/OS, o nei casi in cui il client è stato fornito con un altro prodotto.

     IBM i Su IBM i, non esiste alcun file `mqclient.ini` predefinito. Tuttavia, il file può essere creato nell'IFS (Integrated File System) IBM i Integrated File System nell'indirizzario `/QIBM/UserData/mqm/`e la variabile di ambiente **MQCLNTCF** definita per puntare ad esso. Ad esempio:

     ```
     ADDENVVAR ENVVAR(MQCLNTCF) VALUE('QIBM/UserData/mqm/mqclient.ini') REPLACE(*YES)
     ```

     Per ulteriori esempi di variabili di ambiente, vedi Variabili di ambiente.

     z/OS La piattaforma z/OS non può essere utilizzata per eseguire client IBM MQ . Pertanto, il file `mqclient.ini` non è presente su IBM MQ for z/OS.

   - Linux UNIX Su sistemi UNIX and Linux , la directory è `/var/mqm`
   - Windows Su piattaforme Windows , configurare la variabile di ambiente MQ_DATA_PATH durante l'installazione in modo che punti alla directory dei dati. Di solito è `C:\ProgramData\IBM\MQ`

     Nota: Se si sta installando solo un client, la variabile di ambiente potrebbe essere MQ_FILE_PATH.
   - Per consentire JRE Java 1.4.2 che non supportano la lettura delle variabili di ambiente, è possibile sovrascrivere manualmente la variabile di ambiente MQ_DATA_PATH con una proprietà di sistema MQ_DATA_PATH Java .

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 `user.home` Java .
   - Linux UNIX Per client C su piattaforme UNIX and Linux , questo è il valore della variabile di ambiente HOME.
   - Windows Per client C su Windows , si tratta dei valori concatenati delle variabili di ambiente HOMEDRIVE e HOMEPATH.

Quali client IBM MQ possono leggere ciascun attributo

La maggior parte degli attributi nel file di configurazione IBM 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 MQ classes for Java o IBM MQ classes for JMS.

Tabella 15. Quali attributi si applicano a ciascun tipo di client

Nome e attributi della stanza `mqclient.ini`	**Descrizione**	**C e .NET non gestito**	**Java**	**JMS**	**Gestita.NET**	**GestitaXMS . NET**
Stanza CHANNELS						

Tabella 15. 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**	**Gestita.NET**	**GestitaXMS . NET**
CCSID	Il numero della serie di caratteri codificati da utilizzare.	Sì	No	No	Sì	Sì
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

Tabella 15. 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**	**Gestita.NET**	**GestitaXMS . NET**
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
MQReconnectTimeout	Il timeout in secondi per riconnettersi a un client.	Sì	No	No	Sì	No
ServerConnectionParametri	L'ubicazione del server IBM 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

Tabella 15. 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**	**Gestita.NET**	**GestitaXMS . NET**
PasswordProtection	Consente di impostare password protette nella struttura MQCSP, piuttosto che utilizzare SSL o TLS.	Sì	Sì	Sì	Sì	Sì
StanzaClientExitPath						
ExitsDefaultPath	Specifica l'ubicazione delle uscite canale a 32 bit per i client.	Sì	Sì	Sì	Sì	Sì
ExitsDefaultPath64	Specifica l'ubicazione delle uscite del canali a 64 bit per i client.	Sì	Sì	Sì	Sì	Sì
JavaExitsClassPath	I valori da aggiungere al percorso classi quando viene eseguita un'uscita Java .	No	Sì	Sì	No	No
V 9.1.2 V 9.1.2 **Stanza Connessione**						
ApplName	Il nome dell'applicazione specificato nel file di configurazione client.	Sì	No	No	No	No
Stanza JMQI						

Tabella 15. 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**	**Gestita.NET**	**GestitaXMS . NET**
useMQCSPauthentication	Controlla se le applicazioni di IBM MQ classes for Java e IBM MQ classes for JMS devono utilizzare la modalità di compatibilità o la modalità di autenticazione MQCSP durante l'autenticazione con un gestore code.	No	Sì	Sì	No	No
Stanza MessageBuffer						
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

Tabella 15. 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**	**Gestita.NET**	**GestitaXMS . NET**
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 PreConnect						
Dati	URL del repository in cui sono memorizzate le definizioni di connessione.	Sì	No	No	No	No
funzione	Nome del punto di immissione funzionale nella libreria che contiene il codice di uscita PreConnect .	Sì	No	No	No	No
Modulo	Il nome del modulo contenente il codice di uscita API.	Sì	No	No	No	No

Tabella 15. 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	Gestita.NET	GestitaXMS . NET
Sequenza	La sequenza in cui questa uscita viene chiamata rispetto ad altre uscite.	Sì	No	No	No	No
Stanza di sicurezza						
DisableClient DisableClient	Disabilita o abilita AMS per le connessioni client a un gestore code.	Sì	Sì	Sì	No	No
Stanza SSL						
AllowOutboundAllowOutbound	Specifica se i client con capacità SNI imposteranno SNI sul nome canale IBM MQ di destinazione sul sistema remoto quando si avvia una connessione TLS.	Sì	No	No	No	No
V 9.1.4 AllowTLSV13	Se un gestore code è in grado di utilizzare TLS 1.3 CipherSpecs.	Sì (client C/C++)	No	No	No	No

Tabella 15. 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**	**Gestita.NET**	**GestitaXMS . 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 15. 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	Gestita.NET	GestitaXMS . 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
V 9.1.4 MinimumRSAKeyDimensione	Specifica la dimensione chiave minima che i certificati RSA devono avere per essere accettati.	Sì (client C/C++)	No	No	No	No
OCSPAuthentication	Definisce il comportamento di IBM 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 MQ agisce sulle estensioni del certificato di accesso AuthorityInfo .	Sì	No	No	No	No

Tabella 15. 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	Gestita.NET	GestitaXMS . NET
SSLCryptoHardware	Imposta la stringa del parametro richiesta per configurare l'hardware crittografico PKCS #11 presente sul sistema.	Sì	No	No	No	No
SSLFipsRequired	Specifica se devono essere utilizzati solo algoritmi certificati FIPS se la crittografia viene eseguita in IBM 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

Tabella 15. 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**	**Gestita.NET**	**GestitaXMS . NET**
SSLKeyReset Conteggio	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						
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

Tabella 15. 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**	**Gestita.NET**	**GestitaXMS . NET**
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
Windows Library1	Solo su Windows , il nome della DLL dei socket TCP/IP.	Sì	No	No	No	No

Multi Stanza CHANNELS del file di configurazione client

Utilizzare la stanza CHANNELS per specificare le informazioni sui canali client.

Nota: La descrizione di ciascun attributo di questa stanza indica quali client IBM MQ possono leggere tale attributo. Per una tabella di riepilogo per tutte le stanze del file di configurazione IBM MQ MQI client, consultare Quali attributi IBM MQ possono essere letti da ciascun client.

I seguenti attributi possono essere inclusi nella stanza CHANNELS:

CCSID = *numero*
Il numero della serie di caratteri codificati da utilizzare.

Questo attributo può essere letto da client C, .NETnon gestiti, .NETgestiti e XMS .NET gestiti.

Il numero CCSID è equivalente alla variabile di ambiente MQCCSID .

ChannelDefinitionDirectory = *percorso*
Il percorso della directory del file contenente la tabella di definizione del canale client.

Questo attributo può essere letto da client C, .NETnon gestiti, .NETgestiti e XMS .NET gestiti.

Windows Sui sistemi Windows , il valore predefinito è la directory dei file di log e di dati IBM MQ , generalmente `C:\ProgramData\IBM\MQ`.

Linux UNIX Su sistemi UNIX and Linux , il valore predefinito è `/var/mqm`.

La directory ChannelDefinitionpuò contenere un URL che funziona in combinazione con l'attributo File ChannelDefinition(consultare “Accesso URL alla CCDT” a pagina 52).

Il percorso della directory ChannelDefinitionè equivalente alla variabile di ambiente **MQCHLLIB** .

ChannelDefinitionFile = *nomefile*|AMQCLCHL.TAB
Il nome del file contenente la tabella di definizione del canale client.

Questo attributo può essere letto da client C, .NETnon gestiti, .NETgestiti e XMS .NET gestiti.

La tabella di definizione del canale client è equivalente alla variabile 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.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti.

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.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti .

La riconnessione automatica del client non è supportata da IBM MQ classes for Java.

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.

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 16. 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

Tabella 16. La riconnessione automatica dipende dai valori impostati nell'applicazione e nel file mqclient.ini (Continua)

Valore DefRecon in `mqclient.ini`	**Opzioni di riconnessione impostate nell'applicazione**			
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).

Questo attributo può essere letto da client C e .NET non gestiti e da client .NET gestiti.

I client IBM MQ classes for JMS possono specificare un timeout per riconnettersi utilizzando la proprietà del factory di connessione CLIENTRECONNECTTIMEOUT. Il valore predefinito per questa proprietà è 1800 secondi (30 minuti).

I client IBM MQ classes for XMS .NET possono specificare un timeout per riconnettersi utilizzando le seguenti proprietà:

- La proprietà factory di connessione CLIENTRECONNECTTIMEOUT. Il valore predefinito per questa proprietà è 1800 secondi (30 minuti). Questa proprietà è valida solo per la modalità gestita.
- La proprietà XMSC.WMQ_CLIENT_RECONNECT_TIMEOUT. Il valore predefinito per questa proprietà è 1800 secondi (30 minuti). Questa proprietà è valida solo per la modalità gestita.

Parametri ServerConnection
ServerConnectionParms equivale alla variabile di ambiente MQSERVER e specifica l'ubicazione del server IBM MQ e il metodo di comunicazione da utilizzare.

Questo attributo può essere letto da client C, .NETnon gestiti, .NETgestiti e XMS .NET gestiti.

L'attributo parametri ServerConnectiondefinisce solo un canale semplice; non è possibile utilizzarlo per definire un canale TLS 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 il carattere barra (/) poiché questo carattere è 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 (predefinito) | YES
Controlla il comportamento della chiamata della funzione MQPUT1 con opzione MQPMO_RESPONSE_AS_Q_DEF.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for Java, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti.

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.

PasswordProtection = Compatibile|sempre|facoltativo
Da IBM MQ 8.0, consente di impostare password protette nella struttura MQCSP, piuttosto che utilizzare TLS.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for Java, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti.

La protezione della password MQCSP è utile per scopi di test e sviluppo in quanto l'utilizzo della protezione della password MQCSP è più semplice rispetto all'impostazione della crittografia TLS, ma non così sicuro.

Per ulteriori informazioni, consultare MQCSP password protection .

Attività correlate
Connessione delle applicazioni MQI IBM MQ ai gestori code

Multi Stanza di percorso ClientExitdel file di configurazione del client

Utilizzare la stanza ClientExitPath per specificare le ubicazioni predefinite delle uscite del canale sul client.

Nota: La descrizione di ciascun attributo di questa stanza indica quali client IBM MQ possono leggere tale attributo. Per una tabella di riepilogo per tutte le stanze del file di configurazione IBM MQ MQI client, consultare Quali attributi IBM MQ possono essere letti da ciascun client.

I seguenti attributi possono essere inclusi nella stanza Percorso ClientExit:

ExitsDefaultPercorso = *stringa*
Specifica l'ubicazione delle uscite di canale a 32 bit per i clienti.

Questo attributo può essere letto da client C, .NETnon gestiti, .NETgestiti, XMS .NETgestiti, IBM MQ classes for Javae IBM MQ classes for JMS . I client IBM MQ classes for Java e IBM MQ classes for JMS utilizzano questo attributo per individuare le uscite di canale a 32 bit non scritte in Java.

ExitsDefaultPath64 = *stringa*
Specifica l'ubicazione delle uscite del canali a 64 bit per i client.

Questo attributo può essere letto da client C, .NETnon gestiti, .NETgestiti, XMS .NETgestiti, IBM MQ classes for Javae IBM MQ classes for JMS . I client IBM MQ classes for Java e IBM MQ classes for JMS utilizzano questo attributo per individuare le uscite del canale a 64 bit non scritte in Java.

JavaExitsClassPath = *stringa*
I valori da aggiungere al percorso classi quando viene eseguita un'uscita Java . Ciò viene ignorato dalle uscite in qualsiasi altra lingua.

Questo attributo può essere letto da client IBM MQ classes for Java e IBM MQ classes for JMS .

Nel file di configurazione JMS , il nome percorso JavaExitsClassviene fornito con lo standard com.ibm.mq.cfg. e questo nome completo viene utilizzato anche nella proprietà di sistema IBM WebSphere MQ 7.0 o successive. In IBM WebSphere MQ 6.0 questo attributo è stato specificato utilizzando la proprietà di sistema com.ibm.mq.exitClasspath, documentata nel file readme IBM WebSphere MQ 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 di exitClasspath , viene ancora rispettato in IBM WebSphere MQ 7.0 o versioni successive.

Multi V 9.1.2 Stanza di connessione del file di configurazione client

Utilizzare la stanza di connessione per specificare un nome applicazione.

Nota: La descrizione di ciascun attributo di questa stanza indica quali client IBM MQ possono leggere tale attributo. Per una tabella di riepilogo per tutte le stanze del file di configurazione IBM MQ MQI client, consultare Quali attributi IBM MQ possono essere letti da ciascun client.

Il seguente attributo può essere incluso nella stanza Connection:

ApplName = ExampleApplname
È possibile specificare un nome applicazione nel file di configurazione client.

Questo attributo può essere utilizzato da client C e .NET non gestiti.

Multi Stanza JMQI del file di configurazione client

Utilizzare la stanza JMQI per specificare i parametri di configurazione per JMQI (Java Message Queuing Interface) utilizzati da IBM MQ classes for Java e IBM MQ classes for JMS.

Nota: La descrizione di ciascun attributo di questa stanza indica quali client IBM MQ possono leggere tale attributo. Per una tabella di riepilogo per tutte le stanze del file di configurazione IBM MQ MQI client, consultare Quali attributi IBM MQ possono essere letti da ciascun client.

Il seguente attributo può essere incluso nella stanza JMQI:

useMQCSPauthentication = NO|SÌ
Controlla se le applicazioni di IBM MQ classes for Java e IBM MQ classes for JMS devono utilizzare la modalità di compatibilità o la modalità di autenticazione MQCSP durante l'autenticazione con un gestore code.

Questo attributo può essere letto da client IBM MQ classes for Javae IBM MQ classes for JMS .

Questo attributo può avere i seguenti valori:

NO
Utilizzare la modalità di compatibilità durante l'autenticazione con un gestore code. Questo è il valore predefinito.

Sì
Utilizzare la modalità di autenticazione MQCSP durante l'autenticazione con un gestore code.

Per ulteriori informazioni sulla modalità di compatibilità e sulla modalità di autenticazione MQCSP, consultare Autenticazione della connessione con il client Java.

Windows 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.

stanza 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 = *DLLName*|WCPIC32
Il nome della DLL APPC.

Library2 = *DLLName*|WCPIC32
Lo stesso di Library1, utilizzato se il codice è memorizzato in due librerie separate.

TPName
Il nome TP da avviare sul sito remoto.

stanza 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.

È equivalente alla variabile di ambiente MQNAME .

NumCmds = *numero*|1
Quanti comandi allocare.

NumSess = *numero*|1
Quante sessioni allocare.

Stanza 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 = SÌ|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 = *DLLName*|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 = *number*|5E86
Il numero di socket SPX in notazione esadecimale.

Multi Stanza MessageBuffer del file di configurazione client

Utilizzare la sezione MessageBuffer per specificare informazioni sui buffer di messaggi.

Nota: La descrizione di ciascun attributo di questa stanza indica quali client IBM MQ possono leggere tale attributo. Per una tabella di riepilogo per tutte le stanze del file di configurazione IBM MQ MQI client, consultare Quali attributi IBM MQ possono essere letti da ciascun client.

I seguenti attributi possono essere inclusi nella sezione MessageBuffer :

MaximumSize = *numero intero*|1
La dimensione, in kilobyte, del buffer di lettura anticipata, nell'intervallo compreso tra 1 e 999 999.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for Java, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti.

Esistono i seguenti valori speciali:

-1
Il client determina il valore appropriato.

0
La lettura anticipata è disabilitata per il client.

PurgeTime = *numero intero*|600
Intervallo, in secondi, dopo il quale vengono eliminati i messaggi rimasti nel buffer di lettura anticipata.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for Java, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti.

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 = *numero 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.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for Java, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti.

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.

Multi Stanza PreConnect del file di configurazione client

Utilizzare la stanza PreConnect per configurare l'uscita PreConnect nel file `mqclient.ini` .

Nota: La descrizione di ciascun attributo di questa stanza indica quali client IBM MQ possono leggere tale attributo. Per una tabella di riepilogo per tutte le stanze del file di configurazione IBM MQ MQI client, consultare Quali attributi IBM MQ possono essere letti da ciascun client.

I seguenti attributi possono essere inclusi nella stanza PreConnect :

Data = *dati_utente*

Questo attributo specifica i dati utente passati all'uscita di preconnessione. I dati passati all'uscita di preconnessione sono specifici per l'implementazione dell'exit di preconnessione che si sta utilizzando e quali dati si prevede di trasmettere.

Questo attributo può essere letto da client C e .NET non gestiti.

Ad esempio, questo attributo può essere utilizzato per specificare l'URL del repository in cui sono memorizzate le definizioni di connessione, ad esempio, quando si utilizza un server LDAP:

```
Data = ldap://myLDAPServer.com:389/cn=wmq,ou=ibm,ou=com
```

Funzione = *myFunc*

Nome del punto di immissione funzionale nella libreria che contiene il codice di uscita PreConnect .

Questo attributo può essere letto da client C e .NET non gestiti.

La definizione della funzione aderisce al prototipo di uscita PreConnect MQ_PRECONNECT_EXIT.

La lunghezza massima di questo campo è MQ_EXIT_NAME_LENGTH.

Modulo = *myMod*

Il nome del modulo contenente il codice di uscita API.

Questo attributo può essere letto da client C e .NET non gestiti.

Se questo campo contiene il nome percorso completo del modulo, viene utilizzato così com' è.

Sequenza = *numero_sequenza*
La sequenza in cui questa uscita viene chiamata rispetto ad altre uscite. Un'uscita con un numero di sequenza basso viene richiamata prima di un'uscita con un numero di sequenza più alto. Non c'è bisogno che la numerazione di sequenza delle uscite sia continua; una sequenza di 1, 2, 3 ha lo stesso risultato di una sequenza di 7, 42, 1096. Questo attributo è un valore numerico senza segno.

Questo attributo può essere letto da client C e .NET non gestiti.

Più stanze PreConnect possono essere definite all'interno del file `mqclient.ini` . L'ordine di elaborazione di ciascuna uscita è determinato dall'attributo Sequenza della stanza.

Attività correlate
Riferimento alle definizioni di connessione mediante un'uscita di pre - connessione da un repository

Multi Stanza di sicurezza del file di configurazione client

Utilizzare la stanza di sicurezza per disattivare o abilitare AMS per le connessioni client a un gestore code.

Nota: La descrizione di ciascun attributo di questa stanza indica quali client IBM MQ possono leggere tale attributo. Per una tabella di riepilogo per tutte le stanze del file di configurazione IBM MQ MQI client, consultare Quali attributi IBM MQ possono essere letti da ciascun client.

Il seguente attributo può essere incluso nella stanza Security:

DisableClientAMS = NO|SÌ
L'attributo DisableClientAMS consente di disabilitare IBM MQ Advanced Message Security (AMS) se si sta utilizzando un client IBM WebSphere MQ 7.5 o successivo per connettersi a un gestore code da una versione precedente del prodotto e viene riportato un errore 2085 (`MQRC_UNKNOWN_OBJECT_NAME`) .

Da IBM WebSphere MQ 7.5, IBM MQ Advanced Message Security (AMS) viene abilitato automaticamente in un client IBM MQ e quindi, per impostazione predefinita, il client tenta di controllare le politiche di sicurezza per gli oggetti nel gestore code. Tuttavia, i server sulle versioni precedenti del prodotto, ad esempio IBM WebSphere MQ 7.1, non hanno AMS abilitato e ciò causa la notifica dell'errore 2085 (`MQRC_UNKNOWN_OBJECT_NAME`) .

I seguenti esempi mostrano come utilizzare l'attributo DisableClientAMS :

- Per disabilitare AMS:

```
Security:
DisableClientAMS=Yes
```

- Per abilitare AMS:

```
Security:
DisableClientAMS=No
```

Questo attributo può essere letto da client C, IBM MQ classes for Javae IBM MQ classes for JMS .

Attività correlate
Disabilitazione di Advanced Message Security sul client

Multi Stanza SSL del file di configurazione client

Utilizzare la stanza SSL per specificare le informazioni sull'utilizzo di TLS.

Nota: La descrizione di ciascun attributo di questa stanza indica quali client IBM MQ possono leggere tale attributo. Per una tabella di riepilogo per tutte le stanze del file di configurazione IBM MQ MQI client, consultare Quali attributi IBM MQ possono essere letti da ciascun client.

I seguenti attributi possono essere inclusi nella stanza SSL:

AllowOutboundSNI = YES (predefinito) | NO
Se abilitata, i client con capacità SNI imposteranno SNI sul nome del canale IBM MQ di destinazione sul sistema remoto quando si avvia una connessione TLS. Se questo attributo è impostato su

NO, i client con supporto SNI non imposteranno l'intestazione SNI causando la ricezione da parte delle richieste di connessione in uscita del certificato predefinito del gestore code remoto durante l'handshake TLS e, pertanto, i certificati per canale non possono essere utilizzati.

Questo attributo può essere letto da client C e .NET non gestiti.

ULW V 9.1.4 **AllowTLSV13 =Y | YES | T | TRUE| N | NO | F | FALSE**

Specifica se un gestore code è in grado di utilizzare TLS 1.3 CipherSpecs (consultare Abilitazione di CipherSpecs).

Questo attributo può essere letto dai client C/C + +.

Questo attributo può presentare i seguenti valori:

- Y (predefinito), YES (predefinito), T (predefinito) o TRUE (predefinito): abilita TLS 1.3 che consente al gestore code di utilizzare TLS 1.3 CipherSpecs.
- N, NO, Fo FALSE: disabilita TLS 1.3, il che significa che il gestore code non è in grado di utilizzare i CipherSpecsTLS 1.3 .

Nota: Quando si utilizza il client MQI, il valore **AllowTLSV13** viene dedotto a meno che non venga specificato esplicitamente nella sezione SSL del file `mqclient.ini` utilizzato dall'applicazione. Per ulteriori informazioni, vedi IBM MQ MQI client and TLS 1.3.

CDPCheckExtensions = YES|NO (predefinito)

CDPCheckExtensions specifica se i canali TLS su questo gestore code tentano di verificare i server CDP denominati nelle estensioni del certificato CrlDistributionPoint.

Questo attributo può essere letto da client C e .NET non gestiti.

Questo attributo può presentare i seguenti valori:

- YES (valore predefinito): i canali TLS tentano di controllare i server CDP per stabilire se un certificato digitale è revocato.
- NO: i canali TLS non tentano di controllare 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.

Consultare Etichetta certificato (CERTLABL) per ulteriori informazioni.

CertificateValPolitica = *stringa*

Determina il tipo di convalida del certificato utilizzato.

Questo attributo può essere letto da client C e .NET non gestiti.

Questo attributo può presentare i seguenti valori:

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.

ClientRevocationAssegni = REQUIRED|OPTIONAL|DISABLED

Determina il modo in cui è configurato il controllo della revoca del certificato se la chiamata di connessione client utilizza un canale 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.

Se si utilizza MQSCO o CCDT, la connessione ha esito positivo. Se non è presente alcun file CCDT e se MQSCO non viene fornito, la connessione non riesce con un codice di errore 2059 e il log degli errori riporta `AMQ9518E: File '/var/mqm/AMQCLCHL.TAB' non trovato`.

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.

Questo attributo può essere letto da client C e .NET non gestiti.

Questo attributo può presentare i seguenti valori:

Nessuna
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.

ULW V 9.1.4 **MinimumRSAKeySize=int**

Specifica la dimensione chiave minima che i certificati RSA devono avere per essere accettati. Consente qualsiasi valore uguale o superiore a 0. Se non specificato, il valore predefinito è 1.

Questo attributo può essere letto dai client C/C + +.

OCSPAuthentication = FACOLTATIVO|OBBLIGATORIO|AVVERTENZA
Definisce il comportamento di IBM MQ quando OCSP è abilitato e il controllo della revoca OCSP non è in grado di determinare lo stato della revoca del certificato. Vedere anche **`ClientRevocationChecks`**.

Questo attributo può essere letto da client C e .NET non gestiti.

Questo attributo può presentare i seguenti valori:

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 IBM MQ agisce sulle estensioni del certificato di accesso AuthorityInfo.

Questo attributo può essere letto da client C e .NET non gestiti.

Se il valore è impostato su `NO`, IBM MQ ignora le estensioni del certificato di accesso AuthorityInfoe non tenta un controllo di sicurezza OCSP. Il valore predefinito è `Sì`.

ULW V 9.1.5 **OCSPTimeout = *numero***
Il numero di secondi di attesa per un responder OCSP durante l'esecuzione di una verifica di revoca.

Questo attributo può essere letto da client C e .NET non gestiti.

Se non viene impostato alcun valore, viene utilizzato il valore predefinito IBM MQ di 30 secondi.

SSLCryptoHardware = *stringa*
Imposta la stringa del parametro richiesta per configurare l'hardware crittografico PKCS #11 presente sul sistema.

Questo attributo può essere letto da client C e .NET non gestiti.

Specificare una stringa nel seguente formato: `GSK_PKCS11 = driver path and filename;token label;token password;symmetric cipher setting;`

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.

Linux UNIX Quando si forniscono i diversi componenti della stringa, è necessario eseguire l'escape dei caratteri punto e virgola utilizzando il carattere barra retroversa, poiché il carattere punto e virgola viene considerato come un commento. Ad esempio: `'\;'`

SSLFipsRequired = YES|NO
Specifica se devono essere utilizzati solo algoritmi certificati FIPS se la crittografia viene eseguita in IBM MQ.

Questo attributo può essere letto da C e da client .NET non gestiti.

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).

Questo attributo può essere letto da C e da client .NET non gestiti.

Solaris AIX Per la piattaforma Sun Solaris SPARC e per client a 32-bit su AIX, l'indirizzo di rete può essere solo un indirizzo IPv4 .

Su altre piattaforme, l'indirizzo di rete 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.

ULW V 9.1.5 **SSLHTTPConnectTimeout = *numero*|0**
Il numero di secondi di attesa che una connessione di rete venga stabilita correttamente su un server HTTP durante l'esecuzione di un controllo di revoca.

Questo attributo può essere letto da client C e .NET non gestiti.

Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ 0 (off).

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.

Questo attributo può essere letto da C e da client .NET non gestiti.

SSLKeyResetConteggio = *intero*|0
Il numero di byte non codificati inviati e ricevuti su un canale TLS prima che la chiave segreta venga rinegoziata.

Questo attributo può essere letto da C e da client .NET non gestiti.

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 TLS utilizzano un conteggio di reimpostazione della chiave segreta pari a 32768 (32Kb). Ciò per evitare un numero eccessivo di reimpostazioni della chiave, che si verificherebbe per i valori di reimpostazione della chiave segreta.

Multi Stanza TCP del file di configurazione client

Utilizzare la stanza TCP per specificare i parametri di configurazione del protocollo di rete TCP.

Nota: La descrizione di ciascun attributo di questa stanza indica quali client IBM MQ possono leggere tale attributo. Per una tabella di riepilogo per tutte le stanze del file di configurazione IBM MQ MQI client, consultare Quali attributi IBM MQ possono essere letti da ciascun client.

I seguenti attributi possono essere inclusi nella stanza TCP:

ClntRcvBuffSize = *numero*|0
La dimensione, in byte, del buffer di ricezione TCP/IP utilizzato dall'estremità client di un canale di connessione server di connessione client.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for Java, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti.

Un valore zero indica che il sistema operativo gestirà le dimensioni del buffer, in contrapposizione alle dimensioni del buffer fissate da IBM MQ. Se il valore è impostato su 0, vengono utilizzati i

valori predefiniti del sistema operativo. Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ , 32768.

ClntSndBuffSize = *numero*|0
La dimensione in byte del buffer di invio TCP/IP utilizzato dall'estremità client di un canale di connessione server di connessione client.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for Java, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti.

Un valore zero indica che il sistema operativo gestirà le dimensioni del buffer, in contrapposizione alle dimensioni del buffer fissate da IBM MQ. Se il valore è impostato su 0, vengono utilizzati i valori predefiniti del sistema operativo. Se non viene impostato alcun valore, viene utilizzato il valore predefinito di IBM MQ , 32768.

Connect_Timeout = *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.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for Javae IBM MQ classes for JMS .

I processi del canale IBM MQ si collegano su socket non bloccanti. Pertanto, se l'altra estremità del socket non è pronta, connect () restituisce immediatamente *EINPROGRESS* o *EWOULDBLOCK*. In seguito, la connessione verrà tentata di nuovo, fino a un totale di 20 tentativi, quando viene notificato un errore di comunicazione.

Se Connect_Timeout è impostato su un valore diverso da zero, IBM MQ attende il periodo stabilito sulla chiamata select () affinché il socket sia pronto. Ciò aumenta le possibilità di riuscita di una chiamata connect () successiva. Questa opzione potrebbe essere utile in situazioni in cui le connessioni richiedono un periodo di attesa, a causa di un carico elevato sulla rete.

Non esiste alcuna relazione tra i parametri Connect_Timeout, ClntSndBuffSizee ClntRcvBuffSize .

IPAddressVersion = MQIPADDR_IPV4|MQIPADDR_IPV6
Specifica quale protocollo IP utilizzare per una connessione di canale.

Questo attributo può essere letto da client C, .NETnon gestiti, .NETgestiti e XMS .NET gestiti.

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 = SÌ|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.

Questo attributo può essere letto da client C, .NETnon gestiti, IBM MQ classes for Java, IBM MQ classes for JMS, .NETgestiti e XMS .NET gestiti.

Windows **Library1 = *NomeDLL*|WSOCK32**
(Solo Windows) Il nome della DLL socket TCP/IP.

Questo attributo può essere letto da client C e .NET non gestiti.

Multi File di configurazione della traccia di attività, mqat.ini

Il file di configurazione della traccia attività, `mqat.ini`, viene utilizzato per configurare il comportamento della traccia attività. Questo file viene utilizzato per definire il livello e la frequenza dei dati di traccia delle attività di report. Il file fornisce anche un modo per definire le regole per abilitare e disabilitare la traccia dell'attività in base al nome di una applicazione.

Il file `mqat.ini` segue lo stesso formato della coppia chiave stanza e parametro - valore dei file `mqs.ini` e `qm.ini` . Il file è composto da una singola stanza, AllActivityTrace, utilizzata per configurare il livello e la frequenza dei dati di traccia delle attività di report per impostazione predefinita per tutta la traccia delle attività. Il file può contenere anche più stanze ApplicationTrace . Ciascuna di queste stanze definisce una

regola per il funzionamento della traccia per una o più connessioni, in base alla corrispondenza del nome dell'applicazione delle connessioni alla regola. Per ulteriori informazioni, consultare Application activity trace e Configuring activity trace behavior using `mqat.ini`.

Il gestore code applica una serie di regole per determinare quali impostazioni di stanza utilizzare per una connessione. Facoltativamente, è possibile sovrascrivere il livello di traccia globale e le impostazioni di frequenza nella stanza AllActivityTrace per le connessioni che corrispondono a una stanza ApplicationTrace . Per ulteriori informazioni, vedere Configurazione del comportamento della traccia dell'attività utilizzando `mqat.ini`.

Percorsi di directory

IBM i Linux UNIX Sui sistemi UNIX and Linux e IBM i , `mqat.ini` si trova nella directory dei dati del gestore code, che è la stessa ubicazione del file `qm.ini` .

Windows Sui sistemi Windows , `mqat.ini` si trova nella directory dei dati del gestore code `C:\Program Files\IBM\WebSphere MQ\qmgrs\queue_manager_name`. Gli utenti che eseguono le applicazioni da tracciare hanno bisogno dell'autorizzazione per leggere questo file.

Multi AllActivityStanza di traccia del file mqat.ini

La stanza di traccia AllActivitydel file di configurazione `mqat.ini` specifica i parametri utilizzati per configurare i livelli di traccia per un gestore code.

Una singola stanza di traccia AllActivitydefinisce le impostazioni per la traccia dell'attività che viene applicata a tutte le connessioni IBM MQ , a meno che non venga sovrascritta.

I singoli valori nella stanza AllActivityTrace possono essere sovrascritti da informazioni più specifiche in una stanza ApplicationTrace.

Se viene specificata più di una stanza di traccia AllActivity, vengono utilizzati i valori nell'ultima stanza. I parametri mancanti dalla traccia AllActivityselezionata assumono valori predefiniti. I parametri e i valori delle stanze di traccia AllActivityprecedenti vengono ignorati.

ActivityInterval
: L'intervallo di tempo in secondi tra i messaggi di traccia. La traccia attività non utilizza un thread timer, quindi il messaggio di traccia non viene scritto nel momento esatto in cui il tempo trascorre, ma viene scritto quando viene eseguita la prima operazione MQI una volta trascorso l'intervallo di tempo. Se questo valore è 0, il messaggio di traccia viene scritto quando la connessione si disconnette (o quando viene raggiunto il conteggio attività). L'impostazione predefinita è 1.

ActivityCount
: Il numero di operazioni MQI tra i messaggi di traccia. Se questo valore è 0, il messaggio di traccia viene scritto quando la connessione si disconnette (o quando trascorre l'intervallo di attività). Il valore predefinito è 100.

TraceLevel
: La quantità di dettagli del parametro tracciata per ogni operazione. La descrizione delle singole operazioni descrive i parametri inclusi per ciascun livello di traccia. Impostare su `LOW`, `MEDIUM`o `HIGH`. Il valore predefinito è `MEDIUM`.

Dati TraceMessage
: La quantità di dati del messaggio tracciati in byte per le operazioni MQGET, MQPUT, MQPUT1e Callback. Il valore predefinito è 0.

Messaggio StopOnGetTrace
: Può essere impostato su `ON` o `OFF`. L'impostazione predefinita è `ON`.

SubscriptionDelivery
: Può essere impostato su `BATCH` o `IMMEDIATE`. Determina se i parametri **`ActivityInterval`** e **`ActivityCount`** devono essere utilizzati quando sono presenti una o più sottoscrizioni di traccia dell'attività. L'impostazione di questo parametro su `IMMEDIATE` determina la sovrascrittura dei valori **`ActivityInterval`** e **`ActivityCount`** con i valori effettivi di 1 quando i dati di traccia hanno una

sottoscrizione corrispondente. Ogni record di traccia dell'attività non viene raggruppato in batch con altri record della stessa connessione e viene invece consegnato alla sottoscrizione immediatamente senza alcun ritardo. L'impostazione `IMMEDIATE` aumenta il sovraccarico delle prestazioni della raccolta dei dati di traccia dell'attività. L'impostazione predefinita è `BATCHED`.

Attività correlate

Configurazione del comportamento della traccia attività utilizzando mqat.ini

Multi Stanza ApplicationTrace del file mqat.ini

Il file di configurazione `mqat.ini` può contenere più stanze ApplicationTrace . Ognuna di queste stanze definisce una regola per il comportamento della traccia per una o più connessioni, in base alla corrispondenza del nome dell'applicazione delle connessioni alla regola.

È possibile impostare i seguenti valori per la stanza ApplicationTrace :

Traccia
Interruttore di traccia dell'attività che può essere impostato su `ON` o `OFF`. Il parametro **`Trace`** è un parametro obbligatorio senza valore predefinito. Può essere utilizzato nella sezione specifica dell'applicazione per stabilire se la traccia dell'attività è attiva per l'ambito della stanza dell'applicazione corrente. Notare che questo valore sovrascrive le impostazioni **ACTVTRC** e **ACTVCONO** per il gestore code.

ApplName
Il parametro **`ApplName`** è specificato come stringa di caratteri ed è un parametro obbligatorio senza valore predefinito. Questo valore viene utilizzato per stabilire a quali applicazioni si applica la sezione ApplicationTrace . Viene associato al valore **`ApplName`** dalla struttura del contesto dell'uscita API (che è equivalente a MQMD.PutApplName). Il contenuto del valore **`ApplName`** varia a seconda dell'ambiente dell'applicazione.

Su Multiplatforms, solo la parte del nome file di MQAXC MQAXC.ApplName corrisponde al valore nella sezione. I caratteri a sinistra del separatore di percorso più a destra vengono ignorati quando viene effettuato il confronto.

Un singolo carattere jolly (*) può essere utilizzato alla fine del valore **`ApplName`** per corrispondere a qualsiasi numero di caratteri dopo tale punto. Se il valore **`ApplName`** è impostato su un singolo carattere jolly (*), il valore **`ApplName`** corrisponde a tutte le applicazioni.

IBM i ApplFunction
Il parametro **`ApplFunction`** viene specificato come stringa di caratteri. Il valore predefinito è *. Il valore di questo parametro viene utilizzato per qualificare i programmi applicativi a cui si applicano la stanza ApplicationTrace e il valore **`ApplName`** .

La stanza è facoltativa ed è valida solo per i gestori code IBM i . Un singolo carattere jolly (*) può essere utilizzato alla fine del valore **`ApplName`** per corrispondere a qualsiasi numero di caratteri. Ad esempio, una stanza ApplicationTrace che specifica **`ApplName`** = ** e **`ApplFunction`** = *AMQSPUT0* si applica a tutti i richiami del programma AMQSPUT0 da qualsiasi lavoro.

ApplClass
Il parametro **`ApplClass`** definisce la classe di una applicazione e può essere impostata sui seguenti valori:

- USER
- MCA
- TUTTO (questo è il valore predefinito)

Per una spiegazione del modo in cui i valori **AppType** corrispondono alle connessioni IBM MQ , consultare la Tabella 3 in Configurazione del comportamento della traccia dell'attività utilizzando mqat.ini.

Facoltativamente, il livello di traccia globale e le impostazioni di frequenza nella stanza di traccia AllActivitypossono essere sovrascritti per quelle connessioni che corrispondono a una stanza ApplicationTrace .

I parametri seguenti possono essere impostati in una stanza ApplicationTrace . Se non sono impostati, il valore viene ereditato dalle impostazioni della stanza di tracciaAllActivity :

ActivityInterval
L'intervallo di tempo in secondi tra i messaggi di traccia. La traccia attività non utilizza un thread timer, quindi il messaggio di traccia non viene scritto nel momento esatto in cui il tempo trascorre, ma viene scritto quando viene eseguita la prima operazione MQI una volta trascorso l'intervallo di tempo. Se questo valore è 0, il messaggio di traccia viene scritto quando la connessione si disconnette (o quando viene raggiunto il conteggio attività). L'impostazione predefinita è 1.

ActivityCount
Il numero di operazioni MQI tra i messaggi di traccia. Se questo valore è 0, il messaggio di traccia viene scritto quando la connessione si disconnette (o quando trascorre l'intervallo di attività). Il valore predefinito è 100.

TraceLevel
La quantità di dettagli del parametro tracciata per ogni operazione. La descrizione delle singole operazioni descrive i parametri inclusi per ciascun livello di traccia. Impostare su `LOW`, `MEDIUM`o `HIGH`. Il valore predefinito è `MEDIUM`.

Dati TraceMessage
La quantità di dati del messaggio tracciati in byte per le operazioni MQGET, MQPUT, MQPUT1e Callback. Il valore predefinito è 0.

Messaggio StopOnGetTrace
Può essere impostato su `ON` o `OFF`. L'impostazione predefinita è `ON`.

Attività correlate
Configurazione del comportamento della traccia attività utilizzando mqat.ini

Configurazione dell'accodamento distribuito

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

Prima di iniziare

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

Se è necessario connettere due gestori code che si trovano su reti fisiche differenti o è necessario comunicare tramite firewall, l'utilizzo di IBM MQ Internet Pass-Thru potrebbe semplificare la configurazione. Per ulteriori informazioni, consultare IBM MQ Internet Pass-Thru.

Procedura

- Utilizzare le informazioni contenute nei seguenti argomenti secondari per collegare le applicazioni utilizzando l'accodamento distribuito:
  - “Tecniche di accodamento distribuito IBM MQ” a pagina 177
  - “Introduzione alla gestione delle code distribuite” a pagina 197
  - “Come inviare un messaggio a un altro gestore code” a pagina 200
  - “Attivazione dei canali” a pagina 221
  - “Sicurezza dei messaggi” a pagina 219
  - ULW “Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 228
  - IBM i “Monitoraggio e controllo dei canali su IBM i” a pagina 253

Concetti correlati
“Configurazione di IBM MQ for z/OS” a pagina 827

Utilizzare questo argomento come guida dettagliata per personalizzare il sistema IBM MQ for z/OS .

Attività correlate

“Configurazione delle connessioni tra client e server” a pagina 15
Per configurare i link di comunicazione tra IBM MQ MQI clients e server, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del link, avviare un listener e definire canali.

“Configurazione di un cluster di gestore code” a pagina 275
I cluster forniscono un meccanismo per l'interconnessione dei gestori code in modo da semplificare sia la configurazione iniziale che la gestione in corso. È possibile definire componenti cluster e creare e gestire cluster.

“Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms” a pagina 83
È possibile modificare il comportamento di IBM MQ o di un singolo gestore code per adattarlo alle esigenze della propria installazione modificando le informazioni nei file di configurazione (`.ini`). È anche possibile modificare le opzioni di configurazione per IBM MQ MQI clients.

“Configurazione dei gestori code su z/OS” a pagina 821
Utilizzare queste istruzioni per configurare i gestori code su IBM MQ for z/OS.

“Impostazione delle comunicazioni con altri gestori code su z/OS” a pagina 901
Questa sezione descrive le preparazioni IBM MQ for z/OS che è necessario effettuare prima di poter iniziare a utilizzare l'accodamento distribuito.

Tecniche di accodamento distribuito IBM 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:

- ULW Esempio di pianificazione del canale dei messaggi per UNIX, Linux, and Windows
- IBM i Esempio di pianificazione del canale dei messaggi per IBM i
- z/OS Esempio di pianificazione del canale dei messaggi per z/OS
- z/OS Esempio di pianificazione del canale dei messaggi per z/OS utilizzo di gruppi di condivisione code

Concetti correlati

Canali
Introduzione all'accodamento dei messaggi
Accodamento distribuito e cluster

Attività correlate

“Configurazione dell'accodamento distribuito” a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

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 “Configurazione dell'accodamento distribuito” a pagina 176. 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 177. z/OS Se i gestori code si trovano in un gruppo di condivisione code e IGQ (intra - group queuing) è abilitato, il flusso di messaggi può essere controllato dagli agent IGQ. Questi agent sono descritti in Accodamento all'interno del gruppo.

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 Tipi di 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 accodamento distribuito e cluster.

Concetti correlati

“Nomi coda nell'intestazione di trasmissione” a pagina 178
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 179
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 17 a pagina 179 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 17. 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	non applicabile
Fornito nella definizione	richiesto	richiesto	facoltativo
2. Alias gestore code (su chiamata OPEN)			
Fornito nella chiamata	(*) richiesto e non QM locale	richiesto	non applicabile
Fornito nella definizione	richiesto	vuoto	facoltativo
3. Alias coda di risposta (su chiamata PUT)			
Fornito nella chiamata	vuoto	(*) richiesto	non applicabile
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. La Figura 8 a pagina 180 mostra un'applicazione che inserisce i messaggi in 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.

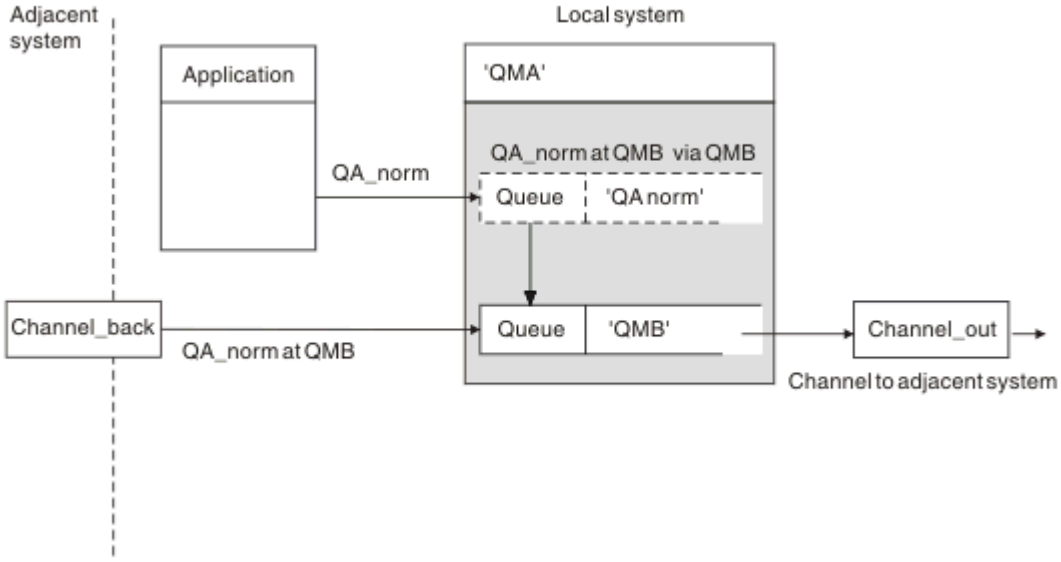


Figura 8. Una definizione di coda remota viene utilizzata per risolvere un nome coda in una coda di trasmissione in un gestore code adiacente

Se si è l'amministratore del sistema IBM 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. Vedere 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.

Riferimenti correlati

Risoluzione nome coda

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.

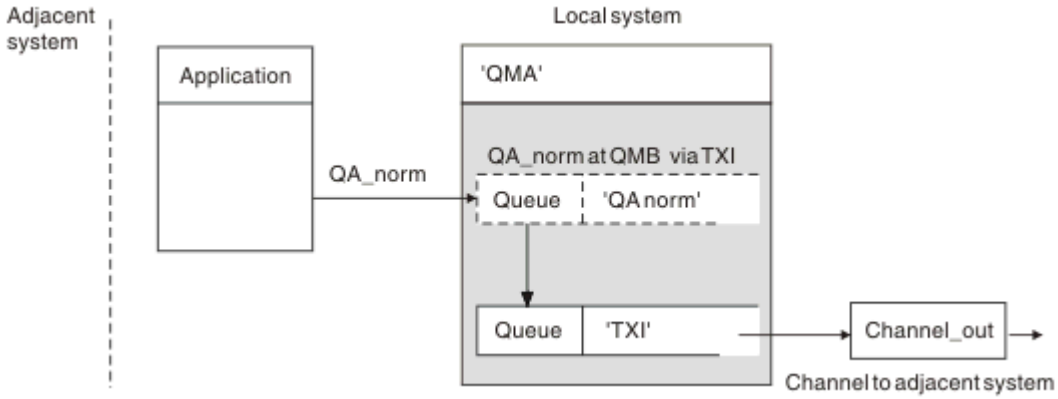


Figura 9. La definizione della coda remota consente l'utilizzo di una coda di trasmissione diversa

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 8 a pagina 180 in “Inserimento di messaggi nelle code remote” a pagina 180. Figura 9 a pagina 181 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 9 a pagina 181, è necessario fornire 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 “Definizione di code cluster” a pagina 276.

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.

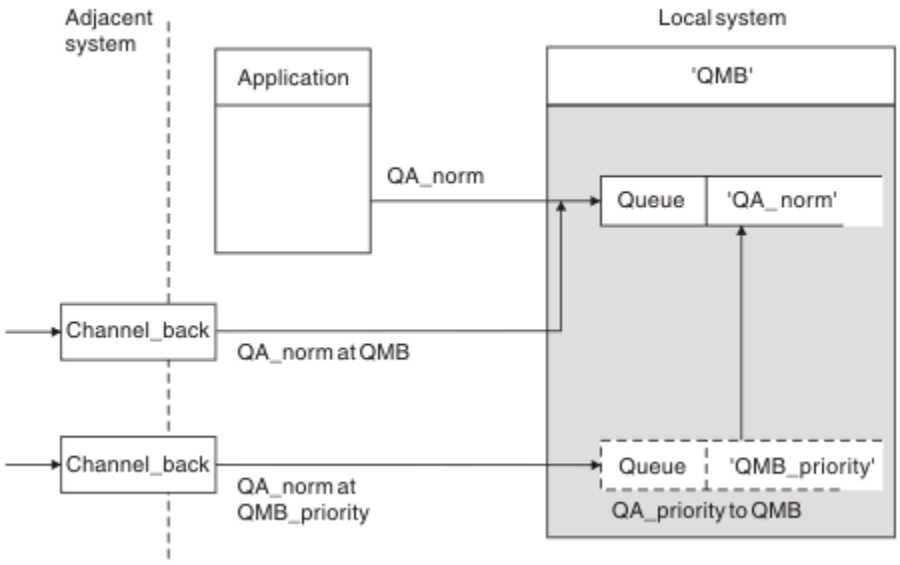


Figura 10. Ricezione diretta dei messaggi e risoluzione del nome del gestore code alias

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 10 a pagina 182 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.

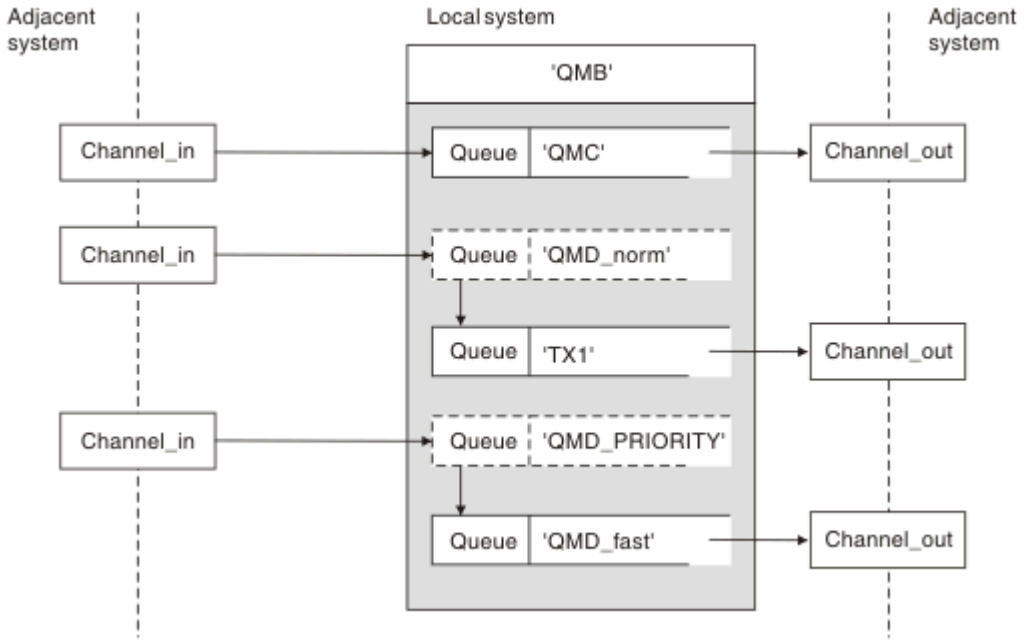


Figura 11. Tre metodi di trasmissione dei messaggi attraverso il sistema

La tecnica mostrata in Figura 10 a pagina 182 in "ricezione di messaggi" a pagina 181, ha mostrato come viene catturato un flusso alias. La Figura 11 a pagina 183 illustra il modo in cui le reti vengono create, 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 il flusso di messaggi alias impostato dall'alias del nome del 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.

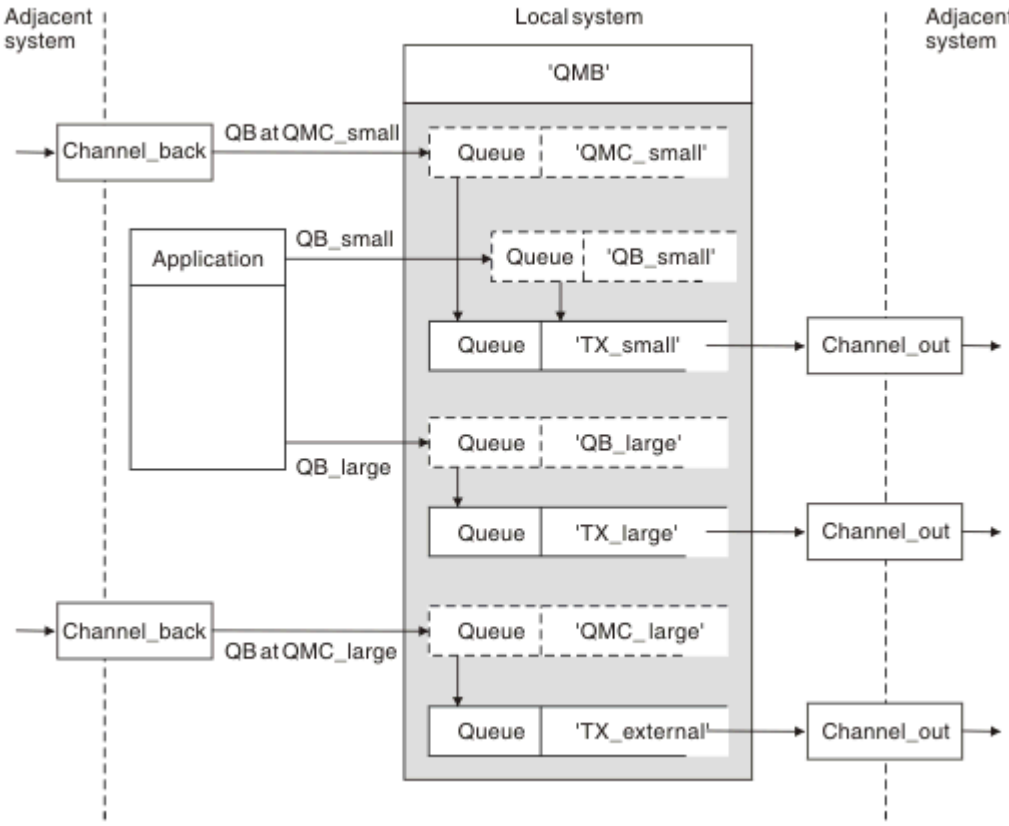


Figura 12. Separazione dei flussi di messaggi

Nell'esempio mostrato in Figura 12 a pagina 185, 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.

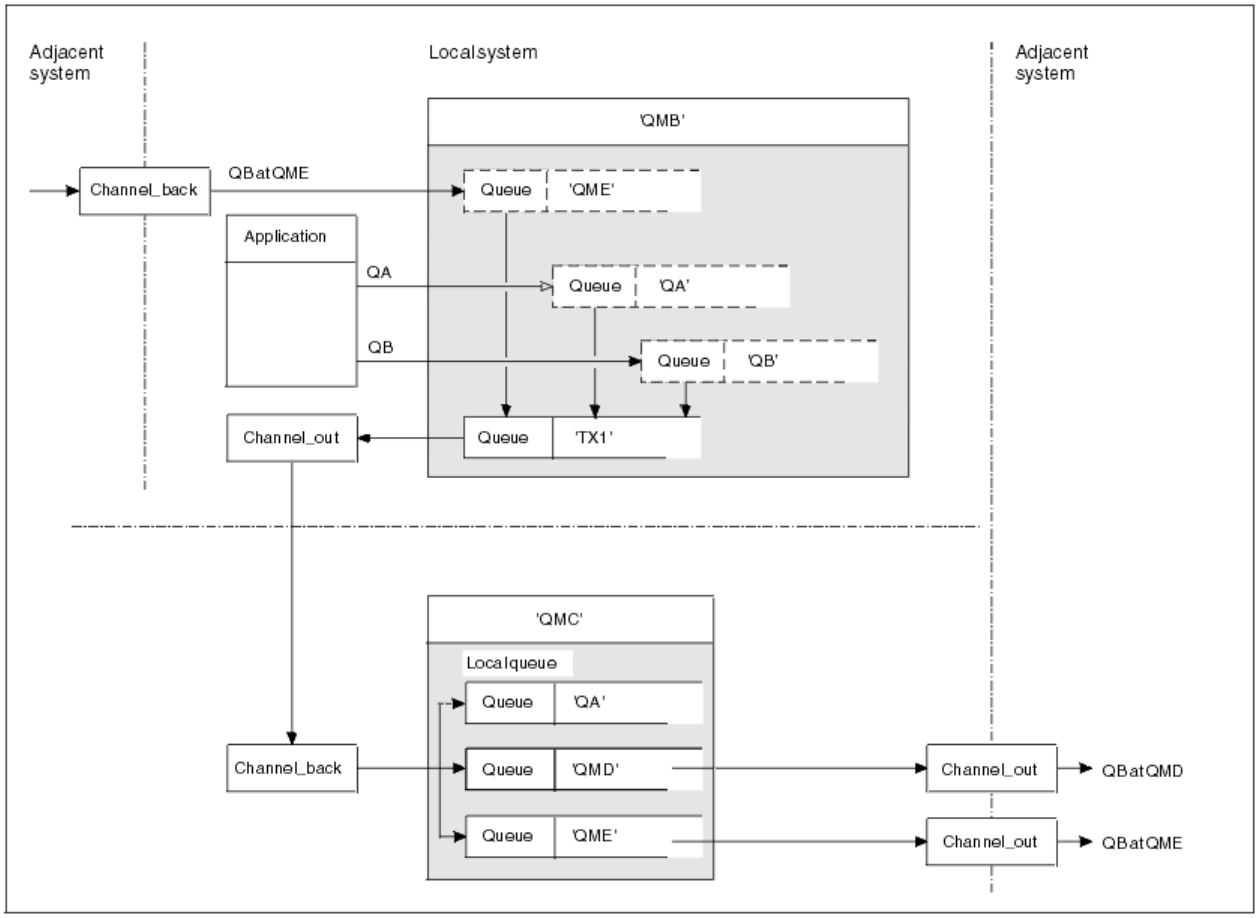


Figura 13. Combinazione dei flussi di messaggi su un canale

La Figura 13 a pagina 186 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.

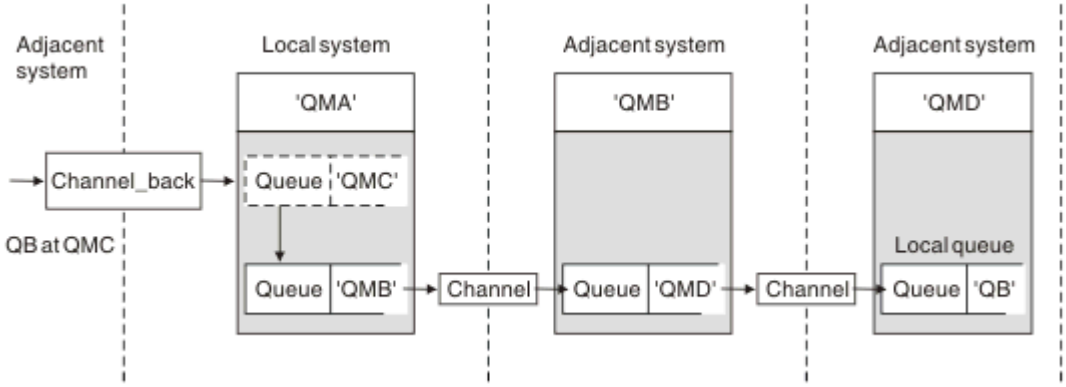


Figura 14. Deviazione dei flussi di messaggi in un'altra destinazione

Figura 14 a pagina 187 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 371.

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 IBM MQ su tutte le piattaforme tranne z/OS, un'applicazione può inviare un messaggio a più 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.

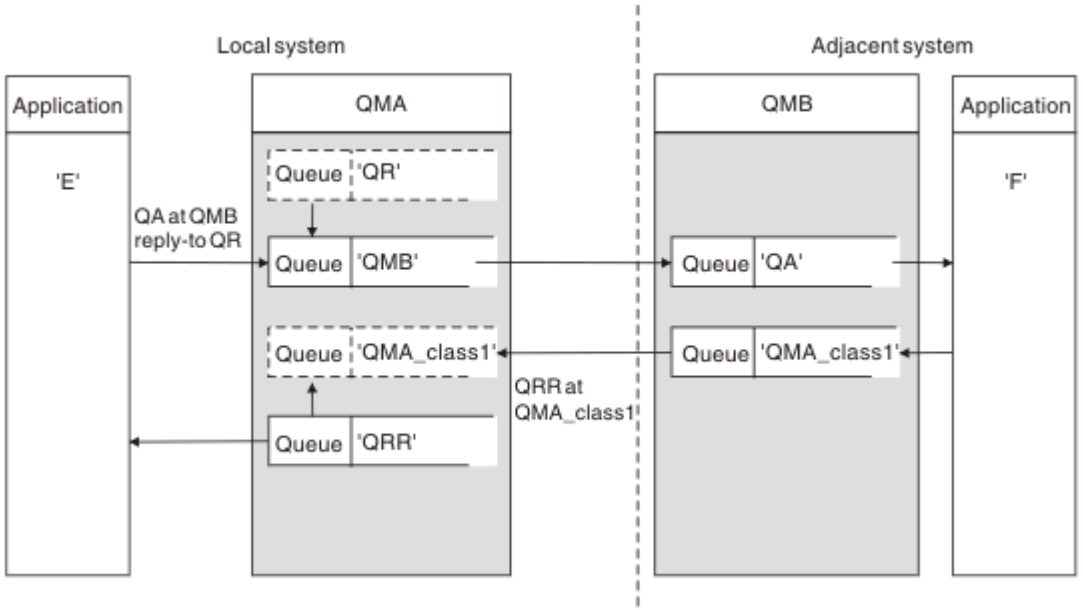


Figura 15. Sostituzione del nome della coda di risposta durante la chiamata PUT

Un loop di elaborazione della coda remota completo che utilizza una coda di risposta viene visualizzato in Figura 15 a pagina 188. Questo loop si applica sia in un ambiente di accodamento distribuito che in un ambiente cluster. I dettagli sono come mostrato in Tabella 21 a pagina 195.

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 179
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 190
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 191
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 192
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 16 a pagina 190, 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.

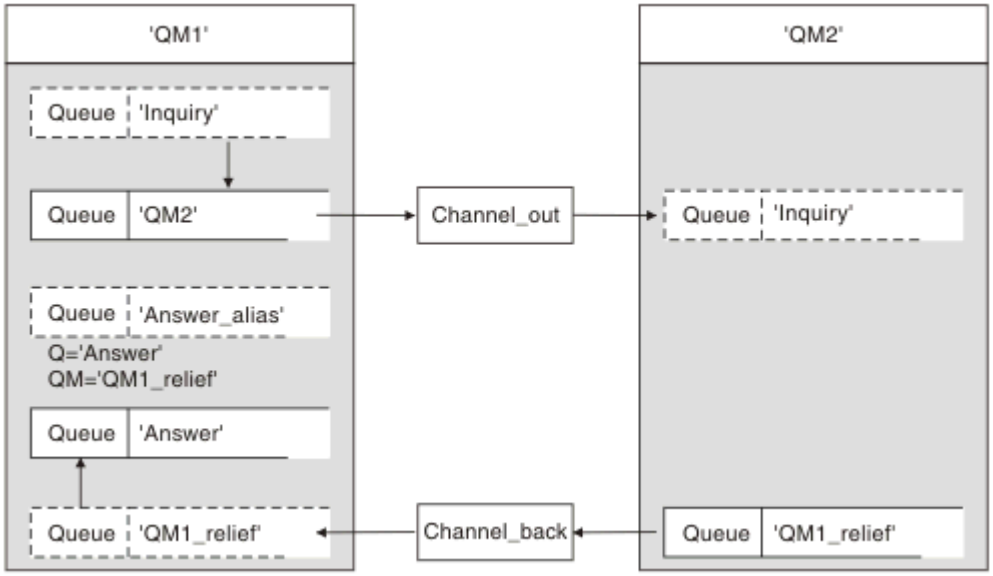


Figura 16. Esempio di alias della coda reply - to

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 IBM MQ in QM1 deve assicurarsi 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

Oggetto	Definizione	
	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 *
	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 di sistema IBM MQ in QM2 deve assicurarsi che la coda locale esista per i messaggi in entrata e che la coda di trasmissione denominata correttamente 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 18. 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 di cluster, consultare Cluster.

z/OS Se i gestori code sono in esecuzione in un QSG (queue sharing group) e IGQ (intra - group queuing) è abilitato, è possibile utilizzare SYSTEM.QSG.TRANSMIT.QUEUE. Per ulteriori informazioni, consultare Intra - group queuing.

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 19 a pagina 195, Tabella 20 a pagina 195e Tabella 21 a pagina 195.

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 19. 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 20. 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 21. 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 controllare che i messaggi siano consegnati nello stesso ordine in cui vengono presi dalla coda di trasmissione.

I numeri di sequenza del canale vengono controllati quando un canale viene avviato e se si verifica una mancata corrispondenza, ciò implica che i dati di sincronia persistenti sono stati persi su entrambi i lati del canale; ad esempio, una configurazione di ripristino di emergenza (DR) o la fine dell'elaborazione batch è stata interrotta quando il canale era in dubbio.

Reimpostando o ignorando le mancate corrispondenze del numero di sequenza, consultare **IgnoreSeqNumberMismatch** nella stanza *Channels del file qm.ini*, non rischia di perdere o duplicare un batch di messaggi e non reimposta lo stato in dubbio di un canale.

Queste informazioni possono essere visualizzate utilizzando DISPLAY CHSTATUS. 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 collegamento di comunicazione senza collegarsi effettivamente ad 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 IBM MQ l'applicazione di visualizzazione dell'instradamento, disponibile tramite il comando di controllo **dspmqrte**, oppure è possibile utilizzare la registrazione dell'attività. Entrambi questi argomenti sono descritti in Riferimento 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 canale messaggi* (MCA), che utilizzano le definizioni del canale per avviare e controllare la comunicazione.

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:

- ULW “Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 228
- z/OS “Monitoraggio e controllo dei canali su z/OS” a pagina 904
- IBM i “Monitoraggio e controllo dei canali su IBM i” a pagina 253

Per esempi di pianificazione del canale di messaggi, consultare:

- ULW Esempio di pianificazione del canale dei messaggi per UNIX, Linux, and Windows
- IBM i Esempio di pianificazione del canale dei messaggi per IBM i
- z/OS Esempio di pianificazione del canale dei messaggi per z/OS
- z/OS Esempio di pianificazione del canale dei messaggi per z/OS utilizzo di gruppi di condivisione code

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

Concetti correlati

“Invio e ricezione di messaggi” a pagina 198
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 206
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 219
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 225
La gestione dei dati di inizializzazione del canale dipende dalla piattaforma IBM MQ .

“Conversione dati per i messaggi” a pagina 226
I messaggi IBM 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 226
IBM 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 227
Altri argomenti da considerare quando si prepara IBM 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.

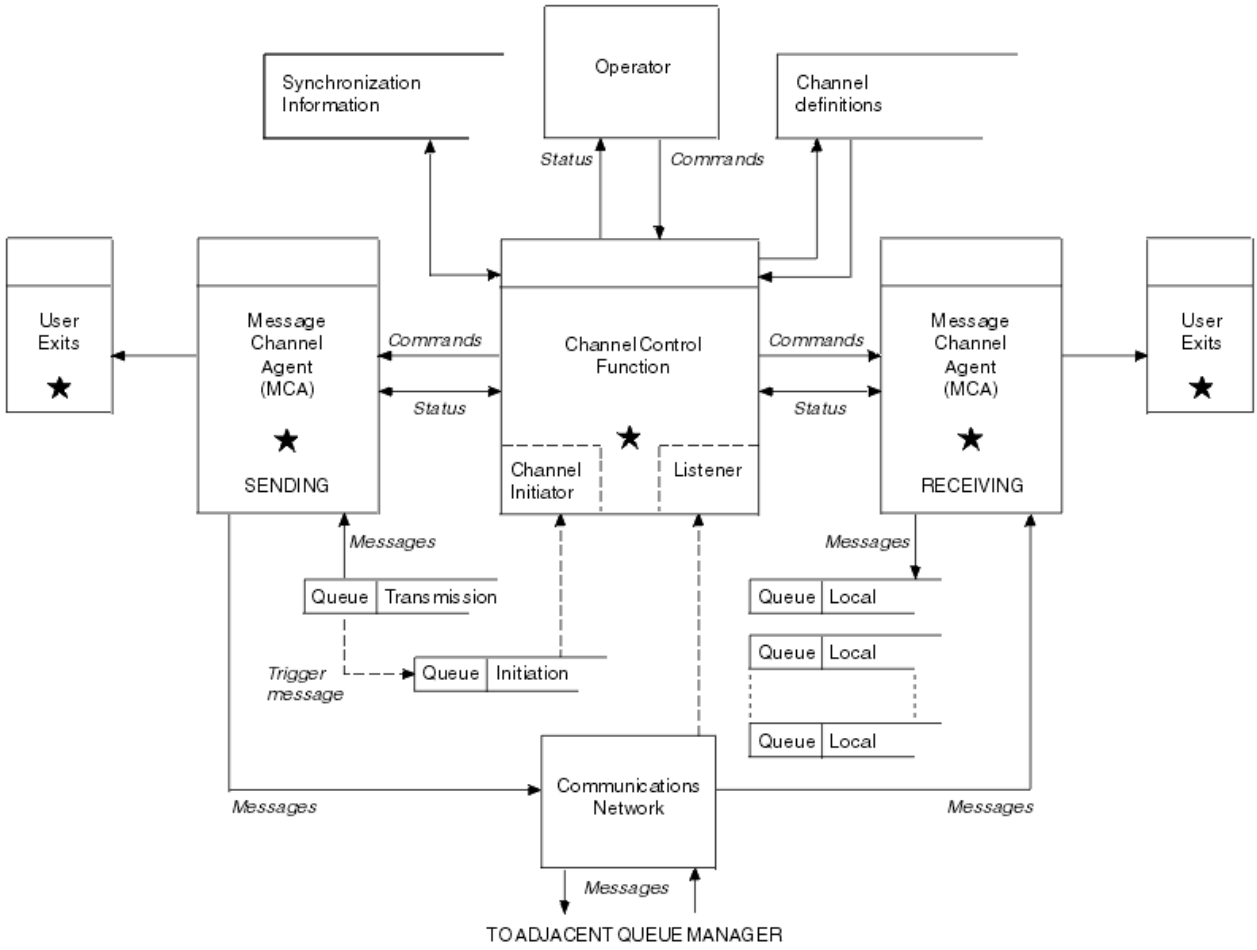


Figura 17. Modello di gestione code distribuite

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 IBM 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 (z/OS richiesto su z/OS, altrimenti 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 IBM MQ :

- Su tutte le piattaforme, è possibile utilizzare i comandi script IBM MQ (MQSC) descritti in Comandi MQSC i comandi PCF (programmable command format) descritti in Automazione delle attività di gestioneo in IBM MQ Explorer.
- z/OS Su z/OS, è anche possibile utilizzare i riquadri Operazione e Controllo descritti in Amministrazione IBM MQ for z/OS .
- IBM i Su IBM i, è anche possibile utilizzare l'interfaccia pannello.

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

Concetti correlati

“Tecniche di accodamento distribuito IBM MQ” a pagina 177
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 197
DQM (Distributed Queue Management) viene utilizzato per definire e controllare le comunicazioni tra gestori code.

“Attivazione dei canali” a pagina 221
IBM 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 219
Oltre alle tipiche funzioni di ripristino di IBM MQ, la gestione della coda distribuita 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.

Attività correlate

“Creazione di gestori code su più piattaforme” a pagina 7
Prima di poter utilizzare messaggi e code, è necessario creare e avviare almeno un gestore code e i relativi oggetti associati. 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 MQ .

“Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 228
Per DQM è necessario creare, monitorare e controllare i canali per i gestori code remoti. È possibile controllare i canali utilizzando comandi, programmi, IBM MQ Explorer, file per le definizioni dei canali e un'area di memoria per le informazioni di sincronizzazione.

“Monitoraggio e controllo dei canali su IBM i” a pagina 253
Utilizzare i comandi e i pannelli DQM per creare, monitorare e controllare i canali dei gestori code remoti. Ogni gestore code ha un programma DQM per il controllo delle interconnessioni ai gestori code remoti compatibili.

“Configurazione delle connessioni tra client e server” a pagina 15
Per configurare i link di comunicazione tra IBM MQ MQI clients e server, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del link, avviare un listener e definire canali.

“Configurazione di un cluster di gestore code” a pagina 275
I cluster forniscono un meccanismo per l'interconnessione dei gestori code in modo da semplificare sia la configurazione iniziale che la gestione in corso. È possibile definire componenti cluster e creare e gestire cluster.

“Impostazione delle comunicazioni con altri gestori code su z/OS” a pagina 901
Questa sezione descrive le preparazioni IBM MQ for z/OS che è necessario effettuare prima di poter iniziare a utilizzare l'accodamento distribuito.

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 IBM MQ for 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 IBM MQ for 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.

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.

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.

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

  z/OS È obbligatorio. È necessario utilizzare la coda di avvio denominata SYSTEM.CHANNEL.INITQ.

  Multi Questo è facoltativo. Si consiglia di denominare la coda di iniziazione SYSTEM.CHANNEL.INITQ.

- Definizione della coda di trasmissione

  Una coda locale con l'attributo USAGE impostato su XMITQ. IBM i Se si utilizza l'interfaccia nativa IBM MQ for IBM i , l'attributo USAGE è *TMQ.

- 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 203
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 su IBM i” a pagina 203
È possibile creare una coda di trasmissione sulla piattaforma IBM i utilizzando il pannello Crea coda MQM.

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 i comandi IBM MQ (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.

Creazione di una coda di trasmissione su IBM i

È possibile creare una coda di trasmissione sulla piattaforma IBM i utilizzando il pannello Crea coda MQM.

È necessario definire una coda locale con l'attributo del campo Utilizzo impostato su *TMQ, per ciascun canale di messaggi di invio.

Se si desidera utilizzare le definizioni di coda remota, utilizzare lo stesso comando per creare una coda di tipo *RMT e Utilizzo di *NORMAL.

Per creare una coda di trasmissione, utilizzare il comando CRTMQ dalla riga comandi per visualizzare il pannello di creazione della prima coda; consultare Figura 18 a pagina 204.

```
Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

Queue name . . . . . .

Queue type . . . . . .  ____     *ALS, *LCL, *MDL, *RMT

Message Queue Manager name . . .  *DFT_____________________________
_____









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

Figura 18. Crea una coda (1)

Immettere il nome della coda e specificare il tipo di coda che si desidera creare: Locale, Remota o Alias. Per una coda di trasmissione, specificare Locale (*LCL) su questo pannello e premere Invio.

Viene visualizzata la seconda pagina del pannello Crea coda MQM; consultare Figura 19 a pagina 204.

```
Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

Queue name . . . . . > HURS.2.HURS.PRIORIT

Queue type . . . . . > *LCL     *ALS, *LCL, *MDL, *RMT
Message Queue Manager name . . .  *DFT
Replace . . . . . .  *NO      *NO, *YES
Text 'description' . . . . . .  '                  '
Put enabled . . . . . .  *YES     *SYSDFTQ, *NO, *YES
Default message priority . . . .  0       0-9, *SYSDFTQ
Default message persistence . .  *NO      *SYSDFTQ, *NO, *YES
Process name . . . . . .  '                  '
Triggering enabled . . . . . .  *NO      *SYSDFTQ, *NO, *YES
Get enabled . . . . . .  *YES     *SYSDFTQ, *NO, *YES
Sharing enabled . . . . . .  *YES     *SYSDFTQ, *NO, *YES



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

Figura 19. Crea una coda (2)

Modificare i valori predefiniti visualizzati. Premere la pagina verso il basso per scorrere fino alla schermata successiva; vedere Figura 20 a pagina 205.

```
Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

Default share option . . . . . *YES     *SYSDFTQ, *NO, *YES
Message delivery sequence . . . *PTY     *SYSDFTQ, *PTY, *FIFO
Harden backout count . . . . . *NO      *SYSDFTQ, *NO, *YES
Trigger type . . . . . *FIRST    *SYSDFTQ, *FIRST, *ALL...
Trigger depth . . . . . 1       1-999999999, *SYSDFTQ
Trigger message priority . . . . 0       0-9, *SYSDFTQ
Trigger data . . . . . '                  '
Retention interval . . . . . 999999999   0-999999999, *SYSDFTQ
Maximum queue depth . . . . . 5000     1-24000, *SYSDFTQ
Maximum message length . . . . . 4194304    0-4194304, *SYSDFTQ
Backout threshold . . . . . 0       0-999999999, *SYSDFTQ
Backout requeue queue . . . . . '                 '
Initiation queue . . . . . '                 '



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

Figura 20. Crea una coda (3)

Immettere *TMQ, per la coda di trasmissione, nel campo Utilizzo di questo pannello e modificare i valori predefiniti mostrati negli altri campi.

```
Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

Usage . . . . . *TMQ     *SYSDFTQ, *NORMAL, *TMQ
Queue depth high threshold . . . 80      0-100, *SYSDFTQ
Queue depth low threshold . . . 20      0-100, *SYSDFTQ
Queue full events enabled . . . *YES     *SYSDFTQ, *NO, *YES
Queue high events enabled . . . *YES     *SYSDFTQ, *NO, *YES
Queue low events enabled . . . . *YES     *SYSDFTQ, *NO, *YES
Service interval . . . . . 999999999   0-999999999, *SYSDFTQ
Service interval events . . . . *NONE     *SYSDFTQ, *HIGH, *OK, *NONE
Distribution list support . . . *NO      *SYSDFTQ, *NO, *YES
Cluster Name . . . . . *SYSDFTQ
Cluster Name List . . . . . *SYSDFTQ
Default Binding . . . . . *SYSDFTQ   *SYSDFTQ, *OPEN, *NOTFIXED




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

Figura 21. Crea una coda (4)

Quando si è soddisfatti che i campi contengono i dati corretti, premere Invio per creare la coda.

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 Programmable Command Formats o quei comandi IBM MQ (MQSC) e i comandi di controllo descritti in “Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 228.

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

Concetti correlati

Determinazione dei problemi per canali

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 IBM MQ su tutte le piattaforme tranne 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 IBM 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 “Configurazione dell'accodamento distribuito” a pagina 176.

Per informazioni sulla definizione dei canali MQI, consultare “Definizione di canali MQI” a pagina 28.

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, consultare “Gestione dei canali in dubbio” a pagina 218.

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 22 a pagina 208 mostra la gerarchia di tutti i possibili stati del canale e gli stati secondari che si applicano a ciascuno degli stati del canale.

Figura 23 a pagina 209 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.

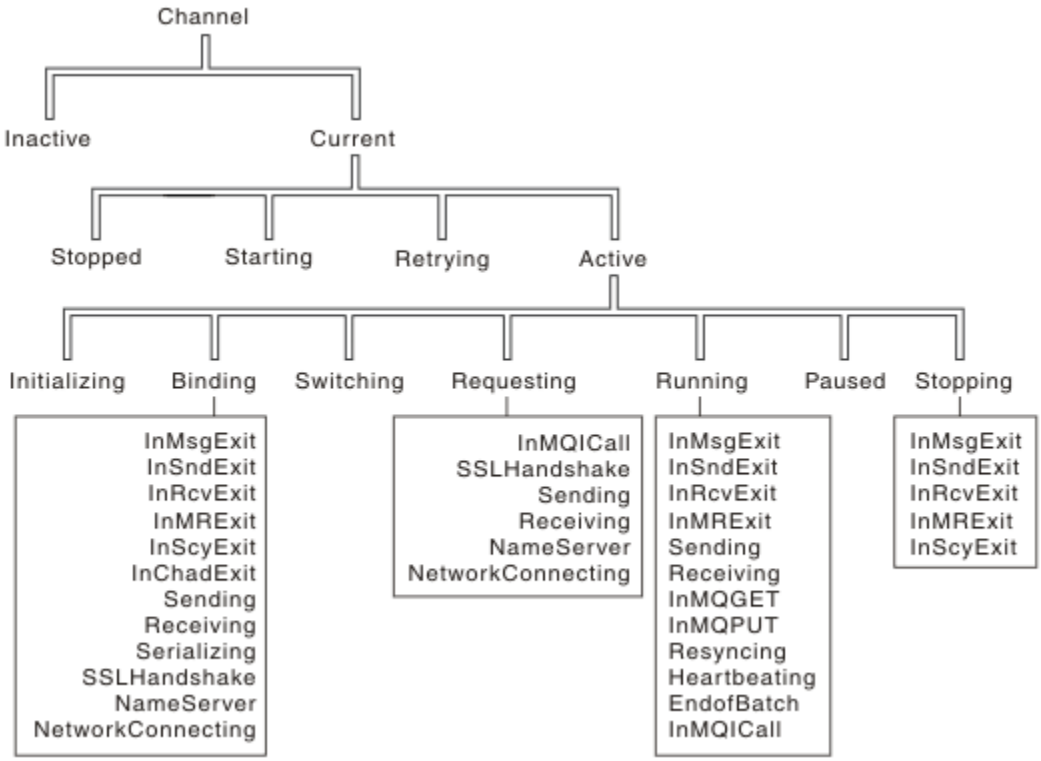


Figura 22. Stati e sottostati del canale

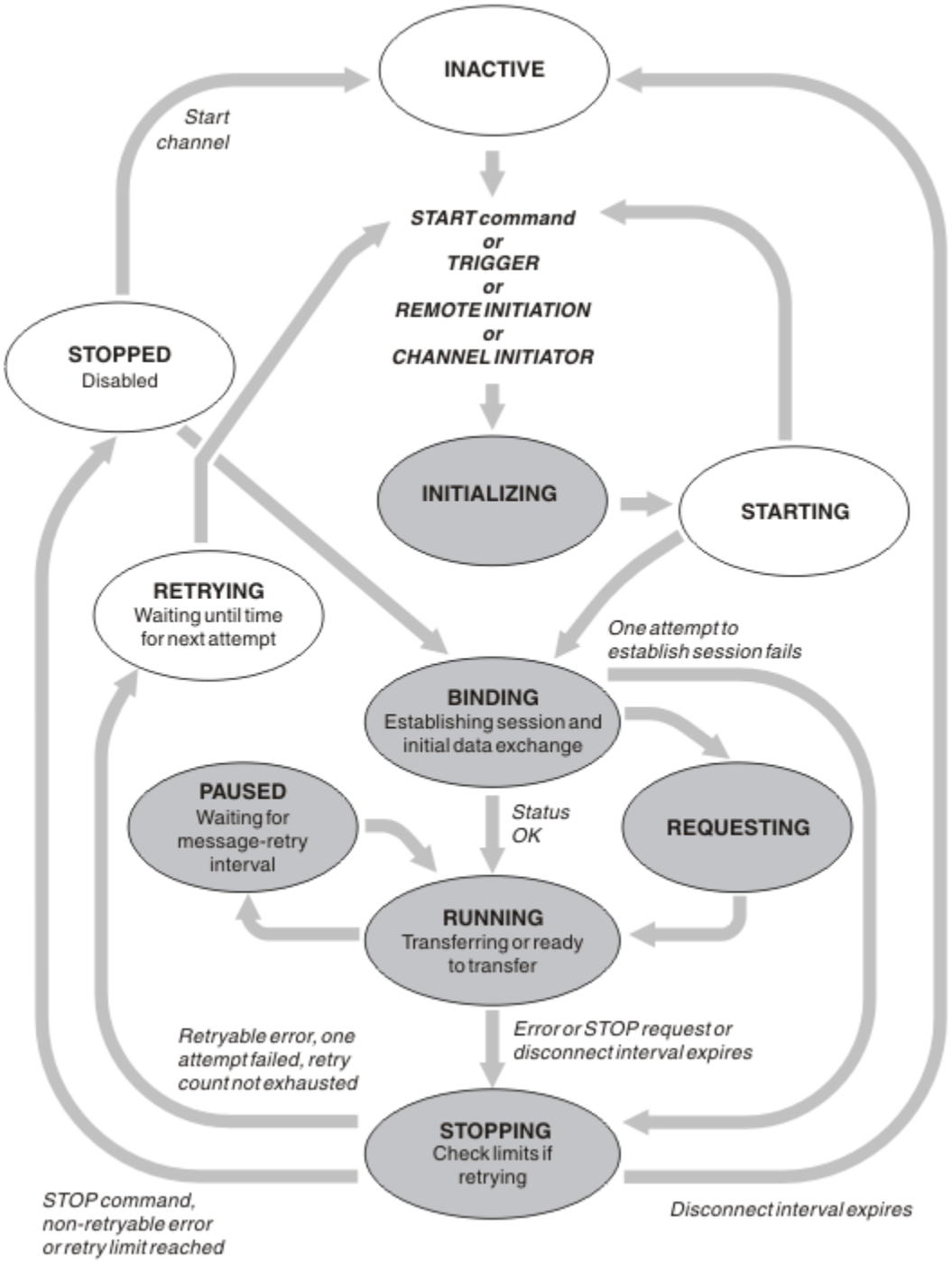


Figura 23. Flussi tra stati del canale

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, RICHIEDENTI, RUNNING, PAUSED o STOPPING) sono evidenziati in Figura 23 a pagina 209.

Un canale attivo può anche visualizzare uno stato secondario che fornisce maggiori dettagli su cosa sta facendo esattamente il canale. Le sottostazioni per ciascuno stato sono mostrati in Figura 22 a pagina 208.

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.

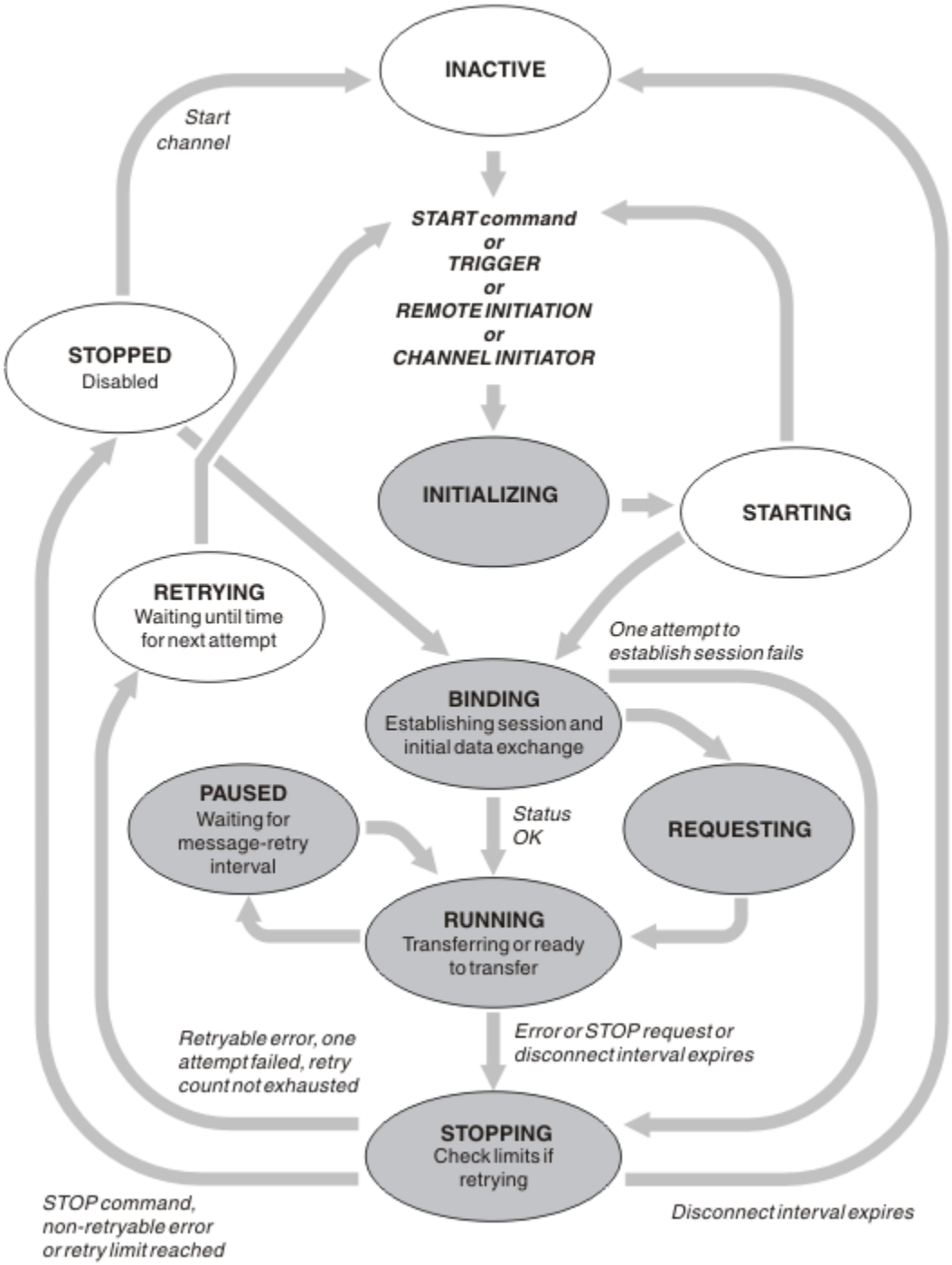


Figura 24. Flussi tra stati del canale

Nota:

1. Quando un canale si trova in uno dei sei stati evidenziati in Figura 24 a pagina 210 (INITIALIZING, BINDING, RICHIEDENTE, IN ESECUZIONE, IN PAUSA 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 quanto segue per la piattaforma:

- z/OS Utilizzare il comando `ALTER QMGR MAXCHL` .
- IBM i Modificare il file di inizializzazione del gestore code.
- Linux UNIX Modificare il file di configurazione del gestore code.
- Utilizzare IBM 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 su come specificare il numero massimo di canali, consultare i seguenti argomenti:

- ULW Amministrazione di IBM MQ.
- IBM i Amministrazione di IBM MQ for IBM i.
- z/OS Amministrazione di IBM MQ for z/OS.

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 z/OS o nella console z/OS , 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 i seguenti argomenti:

- ULW Amministrazione di IBM MQ.
- IBM i Amministrazione di IBM MQ for IBM i.
- z/OS Amministrazione di IBM MQ for z/OS.

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 217).

Nota: Per sistemi IBM i IBM i, UNIX, Linux, and Windows , un iniziatore di canali deve essere 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.

z/OS Se l'iniziatore del canale si arresta mentre un canale si trova nello 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'iniziatore del canale si arresta mentre il canale è in stato ARRESTATO.

Multi Se il gestore code si arresta mentre un canale si trova nello stato REENTAMENTO o ARRESTATO, lo stato del canale viene ricordato quando il gestore code viene riavviato. Da IBM MQ 8.0 in poi, ciò si applica anche ai canali SVRCONN. In precedenza, lo stato del canale per il tipo di canale SVRCONN era stato reimpostato se l'iniziatore del canale era stato arrestato mentre il canale era in stato ARRESTATO.

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 con il parametro **MAXINST** e per impedire che una singola applicazione client esaurisca la capacità del canale di connessione server con il parametro **MAXINSTC** .

Impostare **MAXINST** e **MAXINSTC** con il comando **DEFINE CHANNEL** .

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.

Riferimenti correlati

Attributi e tipi di canale

Definire il canale

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).

Keep alive

In IBM MQ for z/OS, se si sta utilizzando TCP/IP come protocollo di trasporto, è anche possibile specificare un valore per l'attributo del canale intervallo **Keepalive** (KAINT). Si consiglia di assegnare all'intervallo **Keepalive** un valore superiore all'intervallo di heartbeat e un valore inferiore al valore di

disconnessione. È possibile utilizzare questo attributo per specificare un valore di timeout per ciascun canale, come descritto in Intervallo keepalive (KAINT).

In IBM MQ per i sistemi IBM i, UNIX, Linux, and 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).

In IBM MQ per sistemi IBM i, UNIX, Linux, and Windows , il *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.

In IBM MQ for z/OS, 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. Se RCVTIME è impostato, il timeout è impostato su uno dei
   - la HBINT negoziata moltiplicata per una costante
   - HBINT negoziato più un numero costante di secondi
   - un numero costante di secondi

   a seconda del parametro RCVTTYPE e in base a qualsiasi limite imposto da RCVTMIN, se applicabile. RCVTMIN non si applica quando è configurato RCVTTYPE (EQUAL). Se si utilizza un valore costante di RCVTIME e si utilizza un intervallo di heartbeat, non specificare un RCVTIME inferiore all'intervallo di heartbeat. Per i dettagli degli attributi RCVTIME, RCVTMIN e RCVTTYPE, consultare il comando ALTER QMGR .

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 IBM WebSphere MQ 7 Client, gli heartbeat possono fluire sia sul server che sul lato 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.

Impostazioni suggerite

IBM MQ for z/OS

Come punto di partenza iniziale, è possibile utilizzare:

```
/cpf ALTER QMGR TCPKEEP(YES) RCVTTYPE(ADD) RCVTIME(60) ADOPTMCA(ALL) ADOPTCHK(ALL)
```

dove `cpf` è il prefisso del comando per il sottosistema del gestore code.

Consultare ALTER QMGR e IBM MQ network availability per ulteriori informazioni sui vari parametri.

Se l'indirizzo IP del mittente può essere tradotto in più di un indirizzo, potrebbe essere necessario impostare ADOPTCHK su QMNAME anziché su ALL.

IBM MQ for Multiplatforms

In `qm.ini`, aggiungere le seguenti informazioni:

```
TCP:
KeepAlive=Yes
CHANNELS:
AdoptNewMCA=ALL
AdoptNewMCACheck=ALL
```

Per ulteriori informazioni, consultare ALTER QMGR, Stanza dei file di configurazione per l'accodamento distribuitoe “Stanza dei Canali del file qm.ini” a pagina 110 .

Se l'indirizzo IP del mittente potrebbe essere tradotto in più di un indirizzo, potrebbe essere necessario impostare **AdoptNewMCACheck** su QMNAME anziché su ALL.

Adozione di un MCA

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

Se un canale perde il contatto, il canale ricevente può 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 MQ di annullare un canale ricevente e di avviarne uno nuovo al suo posto.

Attività correlate

AmministrazioneIBM MQ

AmministrazioneIBM MQ for z/OS
AmministrazioneIBM MQ for IBM i

Arresto e disattivazione dei canali

È possibile arrestare e sospendere 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 MQ Explorer
- z/OS IBM i altri meccanismi specifici della piattaforma, come segue:

  z/OS **Per z/OS:**
  Il pannello Arresta un canale

  IBM i **Per IBM i:**
  Il comando CL ENDMQMCHL o l'opzione END sul pannello WRKMQMCHL

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.

z/OS Su IBM MQ for z/OS, FORCE interrompe la riassegnazione dei messaggi in corso, lasciando i messaggi BIND_NOT_FIXED parzialmente riassegnati o non in ordine.

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

z/OS Su IBM MQ for z/OS, TERMINATE interrompe la riassegnazione dei messaggi in corso, lasciando i messaggi BIND_NOT_FIXED parzialmente riassegnati o non in ordine.

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.

Informazioni su questa attività

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.

z/OS Se l'iniziatore del canale si arresta mentre un canale si trova nello 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'iniziatore del canale si arresta mentre il canale è in stato ARRESTATO.

Multi Se il gestore code si arresta mentre un canale si trova nello stato REENTAMENTO o ARRESTATO, lo stato del canale viene ricordato quando il gestore code viene riavviato. Da IBM MQ 8.0 in poi, ciò si applica anche ai canali SVRCONN. In precedenza, lo stato del canale per il tipo di canale SVRCONN era stato reimpostato se l'iniziatore del canale era stato arrestato mentre il canale era in stato ARRESTATO.

Procedura

- Riavviare il canale in uno dei seguenti modi:
  - Utilizzando il comando START CHANNEL MQSC.
  - Utilizzando il comando Avvio canale PCF.
  - UtilizzandoIBM MQ Explorer
  - z/OS Su z/OS, utilizzando il pannello Avvia un canale.

- IBM i Su IBM i, utilizzando il comando CL STRMQMCHL o l'opzione START sul pannello WRKMQMCHL.

Gestione dei 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'utilizzo di operatori o programmi che contengono i comandi di gestione del sistema IBM 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.

   Su IBM MQ for 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)
```

IBM i Su IBM MQ for IBM i, è possibile utilizzare il comando Resolve MQM Channel, RSVMQMCHL.

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.

Sicurezza dei messaggi

Oltre alle tipiche funzioni di ripristino di IBM MQ, la gestione della coda distribuita 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 219.

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 25 a pagina 220 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.)

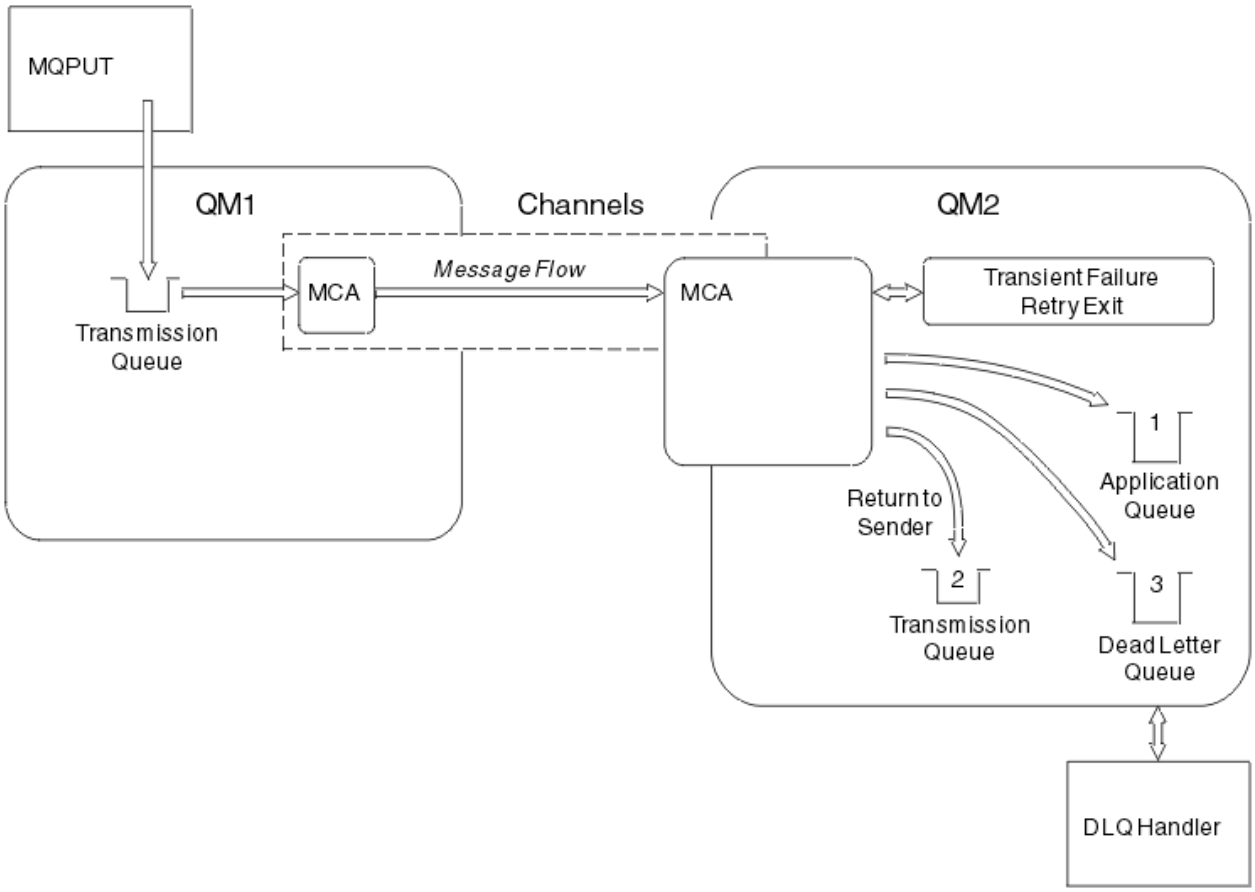


Figura 25. Cosa succede quando un messaggio non può essere consegnato

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 è descritta nella sezione Elaborazione di messaggi su una coda di messaggi non instradabili per sistemi IBM MQ for UNIX, Linux e Windows e in Programma di utilità gestore code di messaggi non instradabili (CSQUDLQH) per sistemi z/OS . 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 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

IBM 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 IBM MQ utilizzando i trigger.

Per informazioni specifiche sulla piattaforma, consultare quanto segue:

- Per Windows, consultare UNIX and Linux systems, “Attivazione dei canali su UNIX, Linux, and Windows.” a pagina 223
- IBM i Per IBM i, consultare “Attivazione dei canali in IBM MQ for IBM i” a pagina 223
- z/OS Per z/OS, consultare “Code di trasmissione e canali di attivazione” a pagina 903

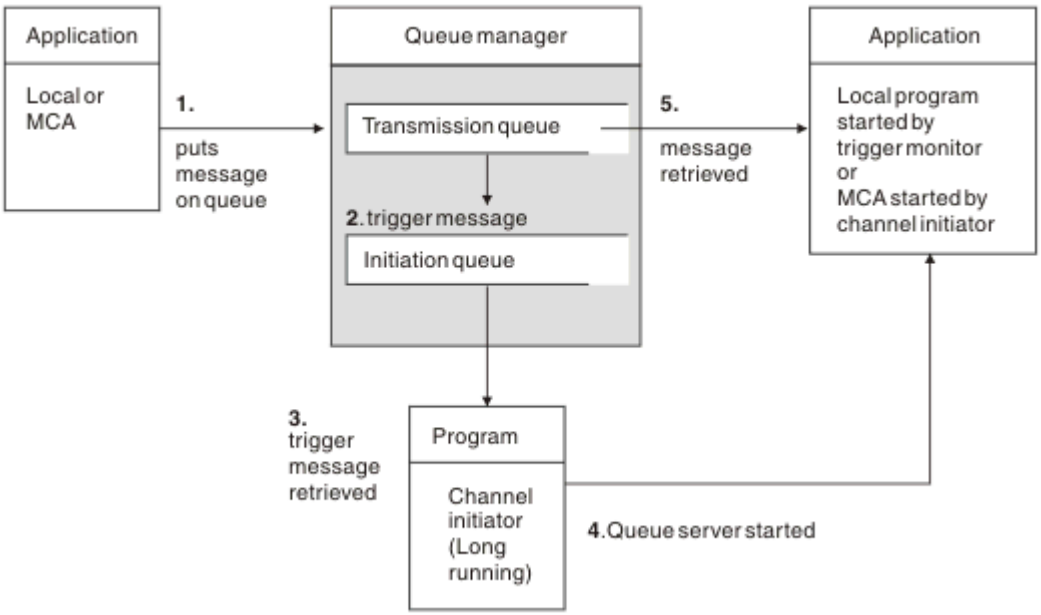


Figura 26. I concetti di attivazione

Gli oggetti richiesti per l'attivazione vengono mostrati in Figura 26 a pagina 222. 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. z/OS Su z/OS, il nome della coda di avvio è fisso, quindi non viene utilizzato sul 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. IBM MQ per i sistemi IBM i IBM i, UNIX, Linux, and 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 dei canali su UNIX, Linux, and Windows.

ULW

È possibile creare una definizione di processo in IBM 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 sistemi IBM MQ for 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.

Attivazione dei canali in IBM MQ for IBM i

IBM i

L'attivazione dei canali in IBM MQ for IBM i viene implementata con il processo dell'iniziatore di canali. Un processo iniziatore di canali per la coda di iniziazione SYSTEM.CHANNEL.INITQ viene avviato automaticamente con il gestore code, a meno che non sia disabilitato modificando l'attributo SCHINIT.

Impostare la coda di trasmissione per il canale, specificando SYSTEM.CHANNEL.INITQ come coda di iniziazione e abilitazione del trigger per la coda. L'iniziatore del canale avvia il primo canale disponibile che specifica questa coda di trasmissione.

```
CRTMQMQ QNAME(MYXMITQ1) QTYPE(*LCL) MQMNAME(MYQMGR)
```

```
TRGENBL(*YES) INITQNAME(SYSTEM.CHANNEL.INITQ)
USAGE(*TMQ)
```

È possibile avviare manualmente fino a tre processi dell'iniziatore di canali con il comando STRMQMCHLI e specificare code di avvio differenti. È anche possibile specificare più di un canale in grado di elaborare la coda di trasmissione e scegliere quale canale avviare. Questa funzione è ancora fornita per essere compatibile con le release precedenti. Il suo utilizzo è obsoleto.

Nota: Solo un canale alla volta può elaborare una coda di trasmissione.

```
STRMQMCHLI QNAME(MYINITQ)
```

Impostare la coda di trasmissione per il canale, specificando TRGENBL (*YES) e, per scegliere quale canale tentare di avviare, specificare il nome del canale nel campo TRIGDATA. Ad esempio:

```
CRTMQMQ QNAME(MYXMITQ2) QTYPE(*LCL) MQMNAME(MYQMGR)
TRGENBL(*YES) INITQNAME(MYINITQ)
USAGE(*TMQ) TRIGDATA(MYCHANNEL)
```

Concetti correlati

“Avvio e arresto dell'iniziatore di canali” a pagina 224
L'attivazione viene implementata utilizzando il processo dell'iniziatore di canali.

Attività correlate

“Configurazione dell'accodamento distribuito” a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM 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 UNIX, Linux, and Windows

IBM i Lavori di intercomunicazione su IBM i

IBM i Stati del canale su IBM i

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 IBM MQ for Multiplatforms , 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 IBM MQ Comandi di controllo per dettagli 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 IBM MQ .

z/OS sistemi

z/OS

In IBM MQ for z/OS, le informazioni di inizializzazione e configurazione vengono specificate utilizzando il comando MQSC **ALTER QMGR** . Se si inseriscono i comandi **ALTER QMGR** nel dataset di input di inizializzazione CSQINP2 , questi vengono elaborati ogni volta che il gestore code viene avviato.

Per eseguire comandi MQSC come **START LISTENER** ogni volta che si avvia l'iniziatore di canali, inserirli nel dataset di input dell'inizializzazione CSQINPX e specificare l'istruzione DD facoltativa CSQINPX nella procedura dell'attività avviata dell'iniziatore di canali.

Per ulteriori informazioni su CSQINP2 e CSQINPX, consultare Personalizzazione dei dataset di input di inizializzazionee ALTER QMGR.

Sistemi Windows, IBM i IBM i, UNIX and Linux

Nei sistemi IBM MQ for Windows, IBM i IBM i, UNIX and Linux , sono presenti file di configurazione che contengono informazioni di configurazione di base sull'installazione IBM MQ .

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

IBM MQ file di configurazione
Questo file contiene informazioni relative a tutti i gestori code sul sistema IBM MQ . Il file si chiama `mqs.ini`. È descritto in “File di configurazione IBM MQ , mqs.ini” a pagina 84.

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 log differisce dal valore predefinito nel file di configurazione IBM 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 IBM i:

```
/QIBM/UserData/mqm/qmgrs/QMNAME/qm.ini
```

Per sistemi Windows :

```
C:\ProgramData\IBM\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 IBM MQ potrebbero richiedere la conversione dei dati quando vengono inviati tra le code su gestori code differenti.

Un messaggio IBM 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

IBM 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 IBM MQ interoperativi sul proprio protocollo di comunicazione proprietario o per inviare messaggi su un protocollo non supportato da IBM MQ . (Non è possibile scrivere il proprio MCA per interagire con un MCA fornito da IBM MQall'altra estremità.)

Se si decide di utilizzare un MCA non fornito da IBM 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 gestione del canale IBM MQ per la configurazione (ad esempio, il comando DEFINE CHANNEL) o il monitoraggio (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 IBM 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 IBM 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.

Linux UNIX Un gestore DLQ viene fornito con IBM MQ su sistemi UNIX and Linux ; per ulteriori informazioni, consultare Il gestore DLQ di esempio, amqsdlq.

IBM i Per ulteriori informazioni su IBM MQ for IBM i, consultare The IBM MQ for IBM i dead-letter queue handler.

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

IBM i Su IBM MQ for IBM i è possibile specificare il numero massimo di canali consentiti nel proprio sistema e il numero massimo che può essere attivo contemporaneamente. Specificare questi numeri nel file `qm.ini` nell'indirizzario QIBM/UserData/mqm/qmgrs/*nome_gestore_code*. 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 IBM 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	LOCAL	STANDARD
Percorso veloce	LOCAL	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).

ULW 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 MQ Explorer, file per le definizioni dei canali e un'area di memoria per le informazioni di sincronizzazione.

Informazioni su questa attività

È possibile utilizzare i seguenti tipi di comandi per controllare i canali:

I comandi IBM MQ (MQSC)
È possibile utilizzare MQSC come singoli comandi in una sessione MQSC in sistemi UNIX, Linux, and Windows . 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 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 i dettagli, consultare Amministrazione utilizzando i comandi di controllo.

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

Linux Windows **IBM MQ Explorer**
Su sistemi Linux e Windows , è possibile utilizzare IBM 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 22 a pagina 230.

Procedura

- “Funzioni richieste per l'impostazione e il controllo dei canali” a pagina 230
- “Introduzione agli oggetti” a pagina 232
- “Impostazione della comunicazione su Windows” a pagina 239
- “Impostazione della comunicazione su UNIX and Linux” a pagina 246

Attività correlate
“Monitoraggio e controllo dei canali su IBM i” a pagina 253
Utilizzare i comandi e i pannelli DQM per creare, monitorare e controllare i canali dei gestori code remoti. Ogni gestore code ha un programma DQM per il controllo delle interconnessioni ai gestori code remoti compatibili.

Riferimenti correlati
ULW Programmi di canale su UNIX, Linux, and Windows
ULW Esempio di pianificazione del canale di messaggi per UNIX, Linux, and Windows
Informazioni di configurazione di esempio
Attributi canale

ULW Funzioni richieste per l'impostazione e il controllo dei canali

Potrebbe essere necessario un certo numero di funzioni IBM 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 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 MQ .

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

- “Introduzione agli oggetti” a pagina 232
- “Creazione di oggetti associati” a pagina 233
- “Creazione di oggetti predefiniti” a pagina 233
- “Creazione di un canale” a pagina 233
- “Visualizzazione di un canale” a pagina 234
- “Visualizzazione dello stato del canale” a pagina 234
- “Controllo dei collegamenti mediante ping” a pagina 235
- “Avvio di un canale” a pagina 235
- “Arresto di un canale” a pagina 237
- “Ridenominazione di un canale” a pagina 237
- “Reimpostazione di un canale” a pagina 238
- “Risoluzione dei messaggi in dubbio su un canale” a pagina 238

Tabella 22 a pagina 230 mostra l'elenco completo delle funzioni IBM MQ di cui potresti aver bisogno.

Tabella 22. Funzioni richieste nei sistemi UNIX, Linux, and Windows

Funzione	**Comandi di controllo**	**MQSC**	**IBM MQ Equivalente di Explorer?**
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 22. Funzioni richieste nei sistemi UNIX, Linux, and Windows (Continua)

Funzione	**Comandi di controllo**	**MQSC**	**IBM MQ Equivalente di Explorer?**
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 22. Funzioni richieste nei sistemi UNIX, Linux, and Windows (Continua)			
Funzione	**Comandi di controllo**	**MQSC**	**IBM MQ Equivalente di Explorer?**
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 sulle piattaforme seguenti: • AIX AIX • Solaris Solaris • Windows Sistemi Windows		No

Nota:

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

ULW 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 IBM MQ (MQSC) o IBM 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:

ULW *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 UNIX, Linux, and Windows.

ULW *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.

Consultare Amministrazione utilizzando i comandi di controllo per ulteriori informazioni sui comandi crtmqm e strmqm.

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.

ULW *Creazione di un canale*

Creare due definizioni di canale, una ad ogni 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 appare in un file di comandi e come viene immesso in UNIX, Linux, and Windows. 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:

- Windows Su Windows utilizzare Ctrl - z per terminare la voce sulla riga comandi.
- Linux UNIX Su UNIX and Linux, utilizzare Ctrl - d.
- In alternativa, su UNIX, Linux, and Windows, utilizzare il comando **end** .

ULW *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
```

ULW *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
- Windows ID thread (solo per 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.

ULW *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, server e mittente cluster. 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 una password viene immessa nella definizione di canale, viene codificata da IBM MQ prima di essere salvata. Viene quindi decodificato prima di scorrere attraverso la conversazione.

ULW *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:

- Linux UNIX Per TCP su UNIX and Linux, inetd può essere configurato per avviare un canale. inetd viene avviata come processo separato.
- Linux UNIX Per LU 6.2 in UNIX and Linux, configurare il proprio prodotto SNA per avviare il processo responder LU 6.2 .

- Windows Per LU 6.2 in 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 **Windows**

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

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

MQ_DATA_PATH rappresenta la directory di alto livello in cui è installato IBM MQ .

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

Linux UNIX **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 UNIX, Linux, and Windows, utilizzare il comando **runmqlsr** per avviare il processo listener IBM 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.

ULW *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 217.

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.

ULW *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, ricordare che un canale ha due definizioni di canale, una a ciascuna estremità. Assicurarsi di rinominare il canale ad entrambe le estremità contemporaneamente.

ULW *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 232
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 206
La funzione di controllo del canale consente di definire, monitorare e controllare i canali.

Attività correlate

"Configurazione dell'accodamento distribuito" a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

Riferimenti correlati

Reimpostazione canale

ULW *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, server o mittente cluster
- È necessario che esista una definizione di canale locale
- Il gestore code locale deve essere in esecuzione

Concetti correlati

"Introduzione agli oggetti" a pagina 232
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 206
La funzione di controllo del canale consente di definire, monitorare e controllare i canali.

Attività correlate

“Configurazione dell'accodamento distribuito” a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

Riferimenti correlati

Risoluzione canale

Windows Impostazione della comunicazione su 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, la connessione deve essere definita e disponibile. Questa sezione spiega come eseguire questa operazione utilizzando i moduli di comunicazione disponibili per sistemi IBM MQ for Windows .

Prima di iniziare

Potrebbe essere utile fare riferimento a Configurazione di esempio - IBM MQ for Windows.

MQ Adv. CD V 9.1.4 Un canale messaggi che utilizza TCP/IP può essere puntato a IBM Aspera fasp.io Gateway, che utilizza un tunnel TCP/IP veloce, in grado di aumentare notevolmente la velocità di trasmissione della rete. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux. Consultare Definizione di una connessione Aspera gateway su Linux.

Informazioni su questa attività

Quando si configura la comunicazione per IBM MQ su Windows, è possibile scegliere tra i seguenti tipi di comunicazione:

- TCP/IP
- LU 6.2
- NetBIOS

Procedura

- Per informazioni sull'impostazione della comunicazione per il sistema Windows , consultare l'argomento secondario per il tipo di comunicazione scelto:
  - “Definizione di un collegamento TCP su Windows” a pagina 240
  - “Definizione di una connessione LU 6.2 su Windows” a pagina 242
  - “Definizione di una connessione NetBIOS su Windows” a pagina 243

  Non tutte le funzioni e le funzioni di IBM MQ for Windows sono disponibili in ambienti che utilizzano protocolli di comunicazioni diversi da TCP/IP. L'elemento non disponibile è IBM MQ Explorer.

Attività correlate

“Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 228
Per DQM è necessario creare, monitorare e controllare i canali per i gestori code remoti. È possibile controllare i canali utilizzando comandi, programmi, IBM 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 15
Per configurare i link di comunicazione tra IBM MQ MQI clients e server, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del link, avviare un listener e definire canali.

“Impostazione della comunicazione su UNIX and Linux” a pagina 246
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, la connessione deve essere definita e disponibile. Questa sezione spiega come eseguire questa operazione utilizzando i moduli di comunicazione disponibili per sistemi IBM MQ for UNIX or Linux .

Riferimenti correlati

“Il tipo di comunicazione da utilizzare” a pagina 15
Piattaforme differenti supportano protocolli di comunicazione differenti. La scelta del protocollo di trasmissione dipende dalla combinazione di IBM MQ MQI client e delle piattaforme server.

Windows *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.

Prima di iniziare

MQ Adv. CD V 9.1.4 Un canale messaggi che utilizza TCP/IP può essere puntato a IBM Aspera fasp.io Gateway, che utilizza un tunnel TCP/IP veloce, in grado di aumentare notevolmente la velocità di trasmissione della rete. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux. Consultare Definizione di una connessione Aspera gateway su Linux.

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 IBM 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 MQ for Windows:

```
TCP:
Port=1822
```

Nota: Per selezionare quale numero di porta TCP/IP utilizzare, IBM 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 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 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 MQ .

Per eseguire il listener fornito con IBM 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 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 MQ da Internet Assigned Numbers Authority per le connessioni in entrata e in uscita.

Per prestazioni ottimali, eseguire il listener IBM MQ come un'applicazione attendibile come descritto in “Esecuzione di canali e listener come applicazioni attendibili” a pagina 228. 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 213.

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.

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.

Consultare “Utilizzo dell'opzione di backlog del listener TCP su IBM MQ for Multiplatforms” a pagina 250 per ulteriori informazioni e il valore specifico per Windows.

Windows *Definizione di una connessione 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 23. 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 Esegui listener o nel programma di transazione richiamabile definito utilizzando TpSetup su Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

MQ_INSTALLATION_PATH rappresenta la directory di livello superiore in cui è installato IBM 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 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

“Invio fine su LU 6.2 su Windows” a pagina 242
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 su Windows” a pagina 243
I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente.

Windows *Invio fine su LU 6.2 su Windows*

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
```

Windows *Ricezione su LU 6.2 su Windows*

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 IBM 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 IBM 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.

Windows *Definizione di una connessione NetBIOS su Windows*

Una connessione NetBIOS si applica solo a un client e a un server su cui è in esecuzione Windows. IBM MQ utilizza tre tipi di risorsa NetBIOS quando stabilisce una connessione NetBIOS a un altro prodotto IBM 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, solo un nome NetBIOS deve essere disponibile per l'utilizzo da parte di IBM 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 IBM MQ le acquisisca. L'amministratore della rete LAN dovrebbe essere in grado di chiarire questo.

Concetti correlati

“Definizione del nome IBM MQ locale NetBIOS” a pagina 244
Il nome NetBIOS locale utilizzato dai processi del canale IBM MQ può essere specificato in tre modi.

“Definizione dei limiti di nome, comando e sessione NetBIOS del gestore code” a pagina 245
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 245
Affinché i canali funzionino correttamente su NetBIOS, è necessario che il supporto dell'adattatore a ciascuna estremità sia compatibile. IBM 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** nel comando runmqlsr.

“Avvio della connessione NetBIOS” a pagina 245
Definizione delle fasi necessarie per avviare una connessione.

“Definizione del listener di destinazione per la connessione NetBIOS” a pagina 246
Definizione delle operazioni da eseguire all'estremità ricevente della connessione NetBIOS .

Windows *Definizione del nome IBM MQ locale NetBIOS*

Il nome NetBIOS locale utilizzato dai processi del canale IBM 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 immettere un comando SET MQNAME in ciascuna finestra in cui viene avviato un processo IBM 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 verificano dei problemi nello stabilire un canale NetBIOS e nel log degli errori del gestore code sono presenti dei messaggi di errore che mostrano un codice di ritorno NetBIOS 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 .

Windows *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
```

Windows *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 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** nel comando runmqlsr.

Il numero di adattatore LAN predefinito utilizzato da IBM 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 l'articolo della Microsoft Knowledge Base 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.

Windows *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. Su 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
```

Windows *Definizione del 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 IBM 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 IBM MQ come un'applicazione attendibile come descritto in “Esecuzione di canali e listener come applicazioni attendibili” a pagina 228. Consultare Limitazioni per le applicazioni attendibili per informazioni sulle applicazioni attendibili.

È possibile arrestare tutti i listener IBM 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.

Linux UNIX Impostazione della comunicazione su UNIX and Linux

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, la connessione deve essere definita e disponibile. Questa sezione spiega come eseguire questa operazione utilizzando i moduli di comunicazione disponibili per sistemi IBM MQ for UNIX or Linux .

Prima di iniziare

Potrebbe essere utile fare riferimento alle sezioni seguenti:

- AIX Configurazione di esempio IBM MQ for AIX
- Solaris Configurazione di esempio IBM MQ for Solaris
- Linux Configurazione di esempio - IBM MQ per Linux

MQ Adv. CD V 9.1.4 Un canale messaggi che utilizza TCP/IP può essere puntato a IBM Aspera fasp.io Gateway, che utilizza un tunnel TCP/IP veloce, in grado di aumentare notevolmente la velocità di trasmissione della rete. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux. Consultare Definizione di una connessione Aspera gateway su Linux.

Informazioni su questa attività

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.

Quando si configura la comunicazione per IBM MQ su UNIX and Linux, è possibile scegliere tra i seguenti tipi di comunicazione:

- TCP/IP
- LU 6.2

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 IBM MQ MQI clients, potrebbe essere utile disporre di canali alternativi che utilizzano protocolli di trasmissione differenti. Per ulteriori informazioni su IBM MQ MQI clients, consultare Panoramica di IBM MQ MQI clients.

Procedura

Per informazioni sull'impostazione della comunicazione per il sistema UNIX and Linux , consultare l'argomento secondario per il tipo di comunicazione scelto:

- “Definizione di un collegamento TCP su UNIX and Linux” a pagina 247
- “Definizione di una connessione LU 6.2 su UNIX and Linux” a pagina 251
- MQ Adv. Linux CD V 9.1.4 “Definizione di una connessione Aspera gateway su Linux” a pagina 783

Attività correlate

“Monitoraggio e controllo dei canali su UNIX, Linux, and Windows” a pagina 228
Per DQM è necessario creare, monitorare e controllare i canali per i gestori code remoti. È possibile controllare i canali utilizzando comandi, programmi, IBM 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 15
Per configurare i link di comunicazione tra IBM MQ MQI clients e server, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del link, avviare un listener e definire canali.

“Impostazione della comunicazione su Windows” a pagina 239
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, la connessione deve essere definita e disponibile. Questa sezione spiega come eseguire questa operazione utilizzando i moduli di comunicazione disponibili per sistemi IBM MQ for Windows .

Riferimenti correlati

“Il tipo di comunicazione da utilizzare” a pagina 15
Piattaforme differenti supportano protocolli di comunicazione differenti. La scelta del protocollo di trasmissione dipende dalla combinazione di IBM MQ MQI client e delle piattaforme server.

Linux UNIX *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.

Prima di iniziare

MQ Adv. CD V 9.1.4 Un canale messaggi che utilizza TCP/IP può essere puntato a IBM Aspera fasp.io Gateway, che utilizza un tunnel TCP/IP veloce, in grado di aumentare notevolmente la velocità di trasmissione della rete. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux. Consultare Definizione di una connessione Aspera gateway su Linux.

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 IBM 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 IBM 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 su UNIX and Linux” a pagina 249
Per avviare i canali su UNIX and Linux, è necessario modificare il file `/etc/services` e il file `inetd.conf`

“Utilizzo dell'opzione di backlog del listener TCP su IBM MQ for Multiplatforms” a pagina 250
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 IBM MQ” a pagina 251
Per eseguire il listener fornito con IBM MQ, che avvia nuovi canali come thread, utilizzare il comando `runmqlsr` .

“Utilizzo dell'opzione TCP/IP SO_KEEPALIVE” a pagina 251
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.

Linux UNIX *Utilizzo del listener TCP/IP su UNIX and Linux*

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 superutente 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 IBM 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 IBM 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:

- AIX Su AIX:

  ```
  refresh -s inetd
  ```

- Solaris Su Solaris 10 o versioni successive:

  ```
  inetconv
  ```

- Linux UNIX 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 locale utilizzate dai processi IBM MQ . Per impostare la locale:

1. Creare uno script di shell che imposta le variabili di ambiente LANG, LC_COLLATE, LC_CTYPE, LC_MONETARY, LC_NUMERIC, LC_TIME e LC_MESSAGES sulla locale utilizzata per altri processi IBM MQ .
2. Nello stesso script di shell, richiamare il programma listener.
3. Modificare il file `inetd.conf` per richiamare lo script 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 IBM 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 di backlog del listener TCP su IBM MQ for Multiplatforms" a pagina 250.

Multi *Utilizzo dell'opzione di backlog del listener TCP su IBM MQ for Multiplatforms*

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 mostrati in Tabella 24 a pagina 250.

Tabella 24. Numero massimo di richieste di connessione in sospeso accodate su una porta TCP/IP

Piattaforma server	**Numero massimo di richieste di connessione**
AIX AIX	100
Linux Linux	100
IBM i IBM i	255
Solaris Solaris	100
Windows ServerWindows	100

Se il backlog raggiunge i valori mostrati in Tabella 24 a pagina 250, la connessione TCP/IP viene rifiutata e non è possibile avviare il canale.

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
```

Ciò sovrascrive il numero massimo predefinito di richieste in sospeso (consultare Tabella 24 a pagina 250) 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` abilitata:

- 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.

Concetti correlati

"Utilizzo dell'opzione backlog del listener TCP" a pagina 925

Quando si riceve su TCP/IP, viene impostato un numero massimo di richieste di connessione in sospeso. Queste richieste in sospeso possono essere considerate un *backlog* di richieste in attesa sulla porta TCP/IP affinché il listener accetti la richiesta.

Linux UNIX *Utilizzo del listener IBM MQ*

Per eseguire il listener fornito con IBM 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 IBM MQ come un'applicazione attendibile come descritto in “Esecuzione di canali e listener come applicazioni attendibili” a pagina 228. Consultare Limitazioni per le applicazioni attendibili per informazioni sulle applicazioni attendibili.

È possibile arrestare tutti i listener IBM 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.

Linux UNIX *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 213) 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.

Linux UNIX *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 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 25. 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.	-

Tabella 25. Impostazioni sul sistema UNIX and Linux locale per una piattaforma del gestore code remoto (Continua)

Piattaforma remota	**TPNAME**	**TPPATH**
z/OS utilizzo 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
Windows	Come specificato nel comando Windows Esegui listener o nel programma di transazione richiamabile definito utilizzando TpSetup su Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

MQ_INSTALLATION_PATH rappresenta la directory di livello superiore in cui è installato IBM 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

"Invio fine su LU 6.2 su UNIX and Linux" a pagina 252
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 su UNIX and Linux" a pagina 252
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.

Linux UNIX *Invio fine su LU 6.2 su UNIX and Linux*

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
```

Solaris Su Solaris, impostare la variabile di ambiente APPC_LOCAL_LU in modo che sia il nome LU locale.

Viene utilizzato SECURITY PROGRAM, dove supportato da CPI-C, quando IBM MQ tenta di stabilire una sessione SNA.

Linux UNIX *Ricezione su LU 6.2 su UNIX and Linux*

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 livello superiore in cui è installato IBM MQ .

Sui sistemi in cui è possibile impostare l'ID utente, specificare un utente che sia un membro del gruppo mqm.

Solaris AIX Su AIXe Solaris, 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.

IBM i Monitoraggio e controllo dei canali su IBM i

Utilizzare i comandi e i pannelli DQM per creare, monitorare e controllare i canali dei gestori code remoti. Ogni gestore code ha un programma DQM per il controllo delle interconnessioni ai gestori code remoti compatibili.

Informazioni su questa attività

Il seguente elenco è una breve descrizione dei componenti della funzione di controllo del canale:

- Le definizioni di canale vengono conservate come oggetti del gestore code.
- I comandi del canale sono una sottoserie della serie di comandi IBM MQ for IBM i .

  Utilizzare il comando GO CMDMQM per visualizzare la serie completa di comandi IBM MQ for IBM i .
- Utilizzare i pannelli di definizione del canale o i comandi 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
- I canali possono essere gestiti anche utilizzando MQSC
- I canali possono essere gestiti anche utilizzando IBM MQ Explorer.
- I numeri di sequenza e gli identificativi *LUW (logical unit of work)* vengono memorizzati nel file di sincronizzazione e utilizzati per la sincronizzazione del canale.

È possibile utilizzare i comandi e i pannelli per: definire i canali dei messaggi e gli oggetti associati e monitorare e controllare i canali dei messaggi. Utilizzando il pulsante F4=Prompt , è possibile specificare il relativo gestore code. Se non si utilizza il prompt, viene utilizzato il gestore code predefinito. Con F4=Prompt, viene visualizzato un pannello aggiuntivo in cui è possibile immettere il nome del gestore code pertinente e, a volte, altri dati.

Gli oggetti da definire con i pannelli sono:

- Code di trasmissione
- Definizioni di coda remota
- Definizioni alias gestore code
- Definizioni alias coda di risposta

- Code locali di risposta
- Definizioni di canali di messaggi

Per ulteriori informazioni sui concetti coinvolti nell'utilizzo di questi oggetti, consultare “Configurazione dell'accodamento distribuito” a pagina 176.

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

Inoltre, il link di comunicazione particolare per ogni 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 e TCP/IP, consultare la guida alla comunicazione specifica per l'installazione.

Procedura

- Per ulteriori informazioni sulla creazione e l'utilizzo degli oggetti, consultare:
  - “Creazione di oggetti su IBM i” a pagina 254
  - “Creazione di un canale su IBM i” a pagina 254
  - “Avvio di un canale su IBM i” a pagina 257
  - “Selezione di un canale su IBM i” a pagina 257
  - “Esplorazione di un canale su IBM i” a pagina 258
  - “Ridenominazione di un canale su IBM i” a pagina 260
  - “Gestione dello stato del canale su IBM i” a pagina 260
  - “Opzioni di gestione canale su IBM i” a pagina 261

Concetti correlati

“Impostazione della comunicazione per IBM i” a pagina 267
Quando un canale di gestione dell'accodamento distribuito viene avviato, tenta di utilizzare la connessione specificata nella definizione del canale. Perché abbia esito positivo, è necessario che la connessione sia definita e disponibile.

Attività correlate

“Configurazione delle connessioni tra client e server” a pagina 15
Per configurare i link di comunicazione tra IBM MQ MQI clients e server, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del link, avviare un listener e definire canali.

Riferimenti correlati

Configurazione di esempio - IBM MQ for IBM i
Esempio di pianificazione del canale di messaggi per IBM MQ for IBM i
Comandi CL di IBM MQ for IBM i

IBM i Creazione di oggetti su IBM i

È possibile utilizzare il comando CRTMQMQ per creare la coda e gli oggetti alias.

È possibile creare gli oggetti coda e alias, come ad esempio: 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.

Per un elenco di oggetti predefiniti, vedere Sistema e oggetti predefiniti.

IBM i Creazione di un canale su IBM i

È possibile creare un canale dal pannello Crea canale o utilizzando il comando CRTMQMCHL sulla riga comandi.

Per creare un canale:

1. Utilizzare F6 dal pannello Gestione canali MQM (WRKMQMCHL).

In alternativa, utilizzare il comando CRTMQMCHL dalla riga comandi.

In entrambi i casi, viene visualizzato il pannello Crea canale. Tipo:

- Il nome del canale nel campo fornito
- Il tipo di canale per questa estremità del link

2. Premere il tasto Invio

Nota: È necessario denominare tutti i canali nella rete in modo univoco. Come mostrato in Diagramma di rete che mostra tutti i canali, inclusi i nomi dei gestori code di origine e di destinazione nel nome del canale, è un buon modo per farlo.

Le voci vengono convalidate e gli errori vengono riportati immediatamente. Correggere gli errori e continuare.

Viene visualizzato il pannello delle impostazioni del canale appropriato per il tipo di canale scelto. Completare i campi con le informazioni precedentemente raccolte. Premere Invio per creare il canale.

Viene fornita una guida per decidere il contenuto dei vari campi nelle descrizioni dei pannelli di definizione del canale nei pannelli di aiuto e in Attributi canale.

```
Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

Channel name . . . . . . . . . . > CHANNAME_____________
Channel type . . . . . . . . . . > *SDR__    *RCVR, *SDR, *SVR, *RQSTR...
Message Queue Manager name     *DFT_____________________________
_____
Replace . . . . . . . . . . . .  *NO_     *NO, *YES
Transport type . . . . . . . . .  *TCP____    *LU62, *TCP, *SYSDFTCHL
Text 'description' . . . . . . . > 'Example Channel Definition'_____________
_____________________________
Connection name . . . . . . . .  *SYSDFTCHL_____________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________
More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Figura 27. Crea canale (1)

```
Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

Transmission queue . . . . . .  'TRANSMISSION_QUEUE_NAME'_____________________
_____________________
Message channel agent . . . . .  *NONE_______  Name, *SYSDFTCHL, *NONE
Library . . . . . .  __________  Name
Message channel agent user ID .  *SYSDFTCHL__ Character value...
Coded Character Set Identifier   *SYSDFTCHL__ 0-9999, *SYSDFTCHL
Batch size . . . . . .  50_________  1-9999, *SYSDFTCHL
Disconnect interval . . . . . .  6000_______  1-999999, *SYSDFTCHL
Short retry interval . . . . . .  60_________  0-999999999, *SYSDFTCHL
Short retry count . . . . . .  10_________  0-999999999, *SYSDFTCHL
Long retry interval . . . . . .  1200_______  0-999999999, *SYSDFTCHL
Long retry count . . . . . .  999999999__  0-999999999, *SYSDFTCHL
Security exit . . . . . .  *NONE_____  Name, *SYSDFTCHL, *NONE
Library . . . . . .  __________  Name
Security exit user data . . . .  *SYSDFTCHL_____________________

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

Figura 28. Crea canale (2)

```
Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

Send exit . . . . . .  *NONE_______  Name, *SYSDFTCHL, *NONE
Library . . . . . .  ___________ Name
+ for more values   __________
Send exit user data . . . . . .  _________________________________
+ for more values  _________________________________
Receive exit . . . . . .  *NONE_____  Name, *SYSDFTCHL, *NONE
Library . . . . . .  __________  Name
+ for more values  __________
__________
Receive exit user data . . . . .  _________________________________
+ for more values  _________________________________
Message exit . . . . . .  *NONE_____  Name, *SYSDFTCHL, *NONE
Library . . . . . .  __________  Name
+ for more values  __________
__________
More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Figura 29. Crea canale (3)

```
Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

Message exit user data . . . . .  _________________________________
+ for more values  _________________________________
Convert message . . . . . .  *SYSDFTCHL_  *YES, *NO, *SYSDFTCHL
Sequence number wrap . . . . . .  999999999__  100-999999999, *SYSDFTCHL
Maximum message length . . . . .  4194304____  0-4194304, *SYSDFTCHL
Heartbeat interval . . . . . .  300________  0-999999999, *SYSDFTCHL
Non Persistent Message Speed . .  *FAST_____  *FAST, *NORMAL, *SYSDFTCHL
Password . . . . . .  *SYSDFTCHL_  Character value, *BLANK...
Task User Profile . . . . . .  *SYSDFTCHL_  Character value, *BLANK...
Transaction Program Name . . . .  *SYSDFTCHL




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

Figura 30. Crea canale (4)

IBM i Avvio di un canale su IBM i

È possibile avviare un canale dal pannello Gestione canali oppure utilizzando il comando STRMQMCHL sulla riga comandi.

I listener sono validi solo per TCP. Per i listener SNA, è necessario configurare il sottosistema di comunicazione.

Per consentire alle applicazioni di scambiare messaggi, è necessario avviare un programma listener per le connessioni in entrata utilizzando il comando STRMQMLSR.

Per connessioni in uscita, è necessario avviare il canale in uno dei modi seguenti:

1. Utilizzare il comando CL STRMQMCHL, 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.)

   ```
   STRMQMCHL CHLNAME(QM1.TO.QM2) MQNAME(MYQMGR)
   ```

2. Utilizzare un iniziatore di canali per attivare il canale. Un iniziatore di canali viene avviato automaticamente all'avvio del gestore code. Questo avvio automatico può essere eliminato modificando la stanza chinit nel file qm.ini per tale gestore code.
3. Utilizzare il comando WRKMQMCHL per avviare il pannello Gestione canali e scegliere l'opzione 14 per avviare un canale.

IBM i Selezione di un canale su IBM i

È possibile selezionare un canale dal pannello Gestione canali.

Per selezionare un canale, utilizzare il comando WRKMQMCHL per iniziare dal pannello Gestione canali:

1. Spostare il cursore sul campo dell'opzione associato al nome del canale richiesto.
2. Immettere un numero di opzione.
3. Premere Invio per attivare la scelta.

Se si seleziona più di un canale, le opzioni vengono attivate in sequenza.

```
Work with MQM Channels

Queue Manager Name . . :  CNX

Type options, press Enter.
2=Change  3=Copy  4=Delete  5=Display  8=Work with Status  13=Ping
14=Start  15=End  16=Reset  17=Resolve

Opt   Name           Type    Transport   Status
CHLNIC          *RCVR    *TCP     INACTIVE
CORSAIR.TO.MUSTANG    *SDR    *LU62    INACTIVE
FV.CHANNEL.MC.DJE1    *RCVR    *TCP     INACTIVE
FV.CHANNEL.MC.DJE2    *SDR    *TCP     INACTIVE
FV.CHANNEL.MC.DJE3    *RQSTR   *TCP     INACTIVE
FV.CHANNEL.MC.DJE4    *SVR    *TCP     INACTIVE
FV.CHANNEL.PETER     *RCVR    *TCP     INACTIVE
FV.CHANNEL.PETER.LU   *RCVR    *LU62    INACTIVE
FV.CHANNEL.PETER.LU1   *RCVR    *LU62    INACTIVE
More...
Parameters or command
===>
F3=Exit  F4=Prompt  F5=Refresh  F6=Create  F9=Retrieve  F12=Cancel
F21=Print
```

Figura 31. Gestione canali

IBM i Esplorazione di un canale su IBM i

È possibile sfogliare un canale dal pannello Visualizza canale o utilizzando il comando DSPMQMCHL sulla riga comandi.

Per visualizzare le impostazioni di un canale, utilizzare il comando WRKMQMCHL per iniziare dal pannello Visualizzazione canale:

1. Immettere l'opzione 5 (Visualizzazione) rispetto al nome canale richiesto.
2. Premere Invio per attivare la scelta.

Se si seleziona più di un canale, vengono presentati in sequenza.

In alternativa, è possibile utilizzare il comando DSPMQMCHL dalla riga comandi.

Ciò comporta la visualizzazione del pannello Visualizzazione canale appropriato con i dettagli delle impostazioni correnti per il canale. I campi sono descritti in Attributi canale.

```
Display MQM Channel

Channel name . . . . . :  ST.JST.2TO1
Queue Manager Name . . . . . :  QMREL
Channel type . . . . . :  *SDR
Transport type . . . . . :  *TCP
Text 'description' . . . . . :  John's sender to WINSDOA1

Connection name . . . . . :  MUSTANG


Transmission queue . . . . . :  WINSDOA1

Message channel agent . . . . :
Library . . . . . :
Message channel agent user ID :  *NONE
Batch interval . . . . . :  0
Batch size . . . . . :  50
Disconnect interval . . . . . :  6000



F3=Exit  F12=Cancel  F21=Print
```

Figura 32. Visualizzazione di un canale TCP/IP (1)

```
Display MQM Channel

Short retry interval . . . . . :  60
Short retry count . . . . . :  10
Long retry interval . . . . . :  6000
Long retry count . . . . . :  10
Security exit . . . . . :
Library . . . . . :
Security exit user data . . . :
Send exit . . . . . :
Library . . . . . :
Send exit user data . . . . . :
Receive exit . . . . . :
Library . . . . . :
Receive exit user data . . . . :
Message exit . . . . . :
Library . . . . . :
Message exit user data . . . . :
More...



F3=Exit  F12=Cancel  F21=Print
```

Figura 33. Visualizzazione di un canale TCP/IP (2)

```
Display MQM Channel

Sequence number wrap . . . . . :  999999999
Maximum message length . . . . :  10000
Convert message . . . . . :  *NO
Heartbeat interval . . . . . .  300
Nonpersistent message speed . .  *FAST









Bottom



F3=Exit  F12=Cancel  F21=Print
```

Figura 34. Visualizzare un canale TCP/IP (3)

IBM i Ridenominazione di un canale su IBM i

È possibile ridenominare un canale dal pannello Gestione canali.

Per ridenominare un canale di messaggi, iniziare dal pannello Gestione canali:

1. Chiudere il canale.
2. Utilizzare l'opzione 3 (Copia) per creare un duplicato con il nuovo nome.
3. Utilizzare l'opzione 5 (Visualizzazione) per verificare che sia stata creata correttamente.
4. Utilizzare l'opzione 4 (Cancellazione) per eliminare il canale originale.

Se si decide di rinominare un canale di messaggi, assicurarsi che entrambe le estremità del canale vengano rinominate contemporaneamente.

IBM i Gestione dello stato del canale su IBM i

È possibile gestire lo stato del canale dal pannello Gestione stato del canale.

Utilizzare il comando WRKMQMCHST per visualizzare il primo di una serie di pannelli che mostrano lo stato dei canali. È possibile visualizzare i pannelli di stato in sequenza quando si seleziona Modifica vista (F11).

In alternativa, selezionando l'opzione 8 (Gestisci stato) dal pannello Gestisci canali MQM viene visualizzato anche il primo pannello di stato.

```
MQSeries Work with Channel Status

Type options, press Enter.
5=Display  13=Ping  14=Start  15=End  16=Reset  17=Resolve


Opt Name          Connection      Indoubt   Last Seq
CARTS_CORSAIR_CHAN  GBIBMIYA.WINSDOA1    NO        1
CHLNIC        9.20.2.213       NO        3
FV.CHANNEL.PETER2   9.20.2.213       NO      6225
JST.1.2        9.20.2.201       NO       28
MP_MUST_TO_CORS    9.20.2.213       NO       100
MUSTANG.TO.CORSAIR  GBIBMIYA.WINSDOA1    NO       10
MP_CORS_TO_MUST    9.20.2.213       NO       101
JST.2.3        9.5.7.126        NO       32
PF_WINSDOA1_LU62   GBIBMIYA.IYA80020    NO       54
PF_WINSDOA1_LU62   GBIBMIYA.WINSDOA1    NO       500
ST.JCW.EXIT.2TO1.CHL 9.20.2.213       NO       216

Bottom
Parameters or command
===>
F3=Exit  F4=Prompt  F5=Refresh  F6=Create  F9=Retrieve  F11=Change view
F12=Cancel  F21=Print
```

Figura 35. Primo della serie di pannelli di stato del canale

Le opzioni disponibili nel pannello Gestione stato canale sono:

Opzione di menu	Descrizione
5=Display	Visualizza le impostazioni del canale.
13=Ping	Avvia un'azione Ping, dove appropriato.
14=Start	Avvia il canale.
15=End	Arresta il canale.
16=Reset	Reimposta il numero di sequenza del canale.
17=Resolve	Risolve manualmente una situazione di canale in dubbio.

IBM i Opzioni di gestione canale su IBM i

Il pannello Gestione canali viene raggiunto con il comando WRKMQMCHL e consente di monitorare lo stato di tutti i canali elencati e di emettere comandi per canali selezionati.

Le opzioni disponibili nel pannello Gestione canale sono:

Opzione di menu	Descrizione
“2=Change” a pagina 262	Modifica gli attributi di un canale.
“3=Copy” a pagina 262	Copia gli attributi di un canale in un nuovo canale.
“4=Delete” a pagina 262	Elimina un canale.
“5=Display” a pagina 262	Visualizza le impostazioni correnti per il canale.
“6=Create” a pagina 262	Visualizza il pannello Crea canale
“8=Work con stato” a pagina 263	Visualizza i pannelli di stato del canale.
“13=Ping” a pagina 264	Esegue la funzione Ping per verificare la connessione al sistema adiacente scambiando un messaggio di dati fisso con l'estremità remota.

Opzione di menu	Descrizione
“14=Start” a pagina 264	Avvia il canale selezionato o reimposta un canale ricevente disabilitato.
“15=End” a pagina 265	Richiede la chiusura del canale.
“16=Reset” a pagina 266	Richiede al canale di reimpostare i numeri di sequenza su questa estremità del collegamento. I numeri devono essere uguali ad entrambe le estremità per l'avvio del canale.
“17=Resolve” a pagina 266	Richiede al canale di risolvere i messaggi in dubbio senza stabilire una connessione all'altra estremità.
“18=Visualizza autorizzazione” a pagina 266	Visualizza l'autorizzazione dell'oggetto IBM MQ
“19=Concedi autorizzazione” a pagina 266	Concede l'autorizzazione all'oggetto IBM MQ
“20=Revoca autorizzazione” a pagina 267	Revoca l'autorizzazione sull'oggetto IBM MQ
“21=Ripristina oggetto” a pagina 267	Recupera l'oggetto IBM MQ
“22=Registrazione immagine” a pagina 267	Immagine oggetto Record IBM MQ

IBM i *2=Change*

Utilizzare l'opzione Modifica per modificare una definizione di canale esistente.

L'opzione Modifica, o il comando CHGMQMCHL, modifica una definizione di canale esistente, ad eccezione del nome del canale. Sovrascrivere i campi da modificare nel pannello di definizione del canale e salvare la definizione aggiornata premendo Invio.

IBM i *3=Copy*

Utilizzare l'opzione Copia per copiare un canale esistente.

L'opzione Copia utilizza il comando CPYMQMCHL per copiare un canale esistente. Il pannello Copia consente di definire il nome del nuovo canale. Tuttavia, è necessario limitare i caratteri utilizzati ai caratteri validi per i nomi oggetto IBM i ; consultare Amministrazione IBM MQ for IBM i.

Premere Invio sul pannello Copia per visualizzare i dettagli delle impostazioni correnti. È possibile modificare qualsiasi nuova impostazione del canale. Salvare la nuova definizione di canale premendo Invio.

IBM i *4=Delete*

Utilizzare l'opzione Elimina per eliminare il canale selezionato.

Viene visualizzato un pannello per confermare o annullare la richiesta.

IBM i *5=Display*

Utilizzare l'opzione Visualizzazione per visualizzare le definizioni correnti per il canale.

Questa scelta visualizza il pannello con i campi che mostrano i valori correnti dei parametri e protetti dall'input utente.

IBM i *6=Create*

Utilizzare l'opzione Crea per visualizzare il pannello Crea canale.

Utilizzare l'opzione Crea oppure immettere il comando CRTMQMCHL dalla riga comandi per ottenere il pannello Crea canale. Esistono esempi di pannelli Crea canale, a partire da Figura 27 a pagina 255.

Con questo pannello, si crea una definizione di canale da una schermata di campi riempiti con valori predefiniti forniti da IBM MQ for IBM i. Immettere il nome del canale, selezionare il tipo di canale che si sta creando e il metodo di comunicazione da utilizzare.

Quando si preme Invio, viene visualizzato il pannello. Immettere le informazioni in tutti i campi richiesti in questo pannello e nei pannelli rimanenti, quindi salvare la definizione premendo Invio.

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 ai caratteri validi per nomi oggetto IBM MQ for IBM i .

Tutti i pannelli hanno valori predefiniti forniti da IBM MQ for IBM i per alcuni campi. È possibile personalizzare questi valori oppure modificarli durante la creazione o la copia dei canali. Per personalizzare i valori, consultare *IBM MQ for IBM i Amministrazione di sistema*.

È possibile creare la propria serie di valori predefiniti del canale impostando canali dummy con i valori predefiniti richiesti per ciascun tipo di canale e copiandoli ogni volta che si desidera creare nuove definizioni di canale.

Riferimenti correlati

Attributi canale

IBM i *8=Work con stato*

Utilizzare Gestione stato per visualizzare informazioni dettagliate sullo stato del canale.

La colonna di stato indica se il canale è attivo o inattivo e viene visualizzato continuamente nel pannello Gestisci canali MQM. Usare l'opzione 8 (Gestione stato) per visualizzare ulteriori informazioni sullo stato. In alternativa, queste informazioni possono essere visualizzate dalla riga comandi con il comando WRKMQMCHST. Consultare “Gestione dello stato del canale su IBM i” a pagina 260.

- Nome canale
- Tipo di canale
- Stato dei canali
- Istanza canale
- Gestore code remoto
- Nome coda di trasmissione
- Nome connessione di comunicazione
- Stato in dubbio del canale
- Ultimo numero sequenza
- Numero di messaggi in dubbio
- Sequenza in sospeso
- Numero di messaggi nella coda di trasmissione
- Identificativo LUW (Logical unit of work)
- Identificativo LUW (logical unit of work / unità logica di lavoro) in dubbio
- Stato secondario canale
- Controllo canale
- Compressione intestazione
- Compressione messaggi
- Indicatore tempo di compressione
- Indicatore di velocità di compressione
- Indicatore tempo di coda della trasmissione
- Indicatore tempo di rete

- Indicatore ora di uscita
- Indicatore dimensione batch
- Conversazioni condivise correnti
- Numero massimo di conversazioni condivise

IBM i *13=Ping*

Utilizzare l'opzione Ping per scambiare un messaggio di dati fisso con l'estremità remota.

Un ping IBM MQ eseguito correttamente fornisce al supervisore del sistema la certezza che il canale 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.

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

Il risultato dello scambio di messaggi viene presentato nel pannello Ping ed è il testo del messaggio restituito, insieme all'ora in cui è stato inviato il messaggio e all'ora in cui è stata ricevuta la risposta.

Ping con LU 6.2

Quando il Ping viene richiamato in IBM MQ for IBM i, viene eseguito con l'ID utente dell'utente che richiede la funzione, mentre il normale modo in cui viene eseguito un programma del canale è per l'ID utente QMQM da utilizzare per i programmi del canale. L'ID utente passa al lato ricevente e deve essere valido sul lato ricevente per l'assegnazione della conversazione LU 6.2 .

IBM i *14=Start*

Utilizzare l'opzione Avvia per avviare un canale manualmente.

L'opzione di avvio è disponibile per i canali mittente, server e richiedente. Non è necessario dove è stato impostato un canale con il trigger del gestore code.

L'opzione Start viene utilizzata anche per i canali ricevente, server - connessione, mittente cluster e ricevente cluster. L'avvio di un canale ricevente in stato STOPPED indica che può essere avviato dal canale remoto.

Quando avviato, l'MCA mittente legge il file di definizione del 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 utilizza il trigger, è necessario avviare il processo trigger in esecuzione continua per monitorare la coda di iniziazione. Il comando STRMQMCHLI può essere utilizzato per avviare il processo.

All'estremità di un canale, il processo di ricezione potrebbe essere avviato in risposta all'avvio di un canale dall'estremità di invio. Il metodo per eseguire questa operazione è diverso per i canali connessi LU 6.2 e TCP/IP:

- I canali connessi LU 6.2 non richiedono alcuna azione esplicita all'estremità di ricezione di un canale.
- I canali TCP connessi richiedono l'esecuzione continua di un processo listener. Questo processo attende le richieste di avvio del canale dall'estremità remota del collegamento e avvia il processo definito nelle definizioni di canale per tale connessione.

  Quando il sistema remoto è IBM i, è possibile utilizzare il comando STRMQMLSR.

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, essere abilitata per GET e non avere altri canali che la utilizzano.
- Gli MCA, locali e remoti, devono esistere.
- Il link di comunicazione deve essere disponibile.
- I gestori code devono essere in esecuzione, locali e remoti.
- Il canale messaggi deve essere inattivo.

Per trasferire i messaggi, devono esistere le code remote e le definizioni di coda remota.

Viene restituito un messaggio al pannello che conferma che la richiesta di avviare un canale è stata accettata. Per confermare che il processo di avvio ha avuto esito positivo, controllare il log di sistema o premere F5 (aggiornare il pannello).

IBM i *15=End*

Utilizzare Fine per arrestare l'attività del canale

Utilizzare l'opzione Fine per richiedere al canale di arrestare l'attività. Il canale non invia ulteriori messaggi.

Selezionare F4 prima di premere Invio per scegliere se il canale diventa ARRESTATO o INATTIVO e se arrestare il canale utilizzando un arresto CONTROLLATO o IMMEDIATE. Un canale arrestato deve essere riavviato dall'operatore per diventare nuovamente attivo. È possibile attivare un canale inattivo.

Arresta immediatamente

Utilizzare Arresta immediatamente per arrestare un canale senza completare alcuna unità di lavoro.

Questa opzione termina il processo del canale. Di conseguenza, il canale non completa l'elaborazione del batch di messaggi corrente e, pertanto, non può lasciare il canale in dubbio. In generale, è meglio per gli operatori utilizzare l'opzione di arresto controllato.

Arresto controllato

Utilizzare Arresta controllato per arrestare un canale alla fine dell'unità di lavoro corrente.

Questa scelta 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.

Riavvio dei canali arrestati

Quando un canale passa allo stato ARRESTATO, è necessario riavviarlo manualmente. Puoi riavviare il canale nei modi seguenti:

- Utilizzando il comando MQSC **START CHANNEL** .
- Utilizzando il comando PCF **Start Channel** .
- Utilizzando IBM MQ Explorer.
- z/OS Su z/OS, utilizzando il pannello Avvia un canale.
- IBM i Su IBM i, utilizzando il comando **STRMQMCHL CL** o l'opzione **START** sul pannello WRKMQMCHL.

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.

z/OS Se l'iniziatore del canale si arresta mentre un canale si trova nello 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'iniziatore del canale si arresta mentre il canale è in stato ARRESTATO.

Multi Se il gestore code si arresta mentre un canale si trova nello stato REENTAMENTO o ARRESTATO, lo stato del canale viene ricordato quando il gestore code viene riavviato. Da IBM MQ 8.0 in poi, ciò si applica anche ai canali SVRCONN. In precedenza, lo stato del canale per il tipo di canale SVRCONN era stato reimpostato se l'iniziatore del canale era stato arrestato mentre il canale era in stato ARRESTATO.

IBM i *16=Reset*

Utilizzare l'opzione Reimposta per forzare una nuova sequenza di messaggi.

L'opzione Reimposta modifica il numero di sequenza del messaggio. Utilizzarlo con attenzione e solo dopo aver utilizzato l'opzione Risolvi per risolvere eventuali situazioni in dubbio. Questa opzione è disponibile solo sul canale mittente o server. Il primo messaggio avvia la nuova sequenza al successivo avvio del canale.

IBM i *17=Resolve*

Utilizzare l'opzione Risolvi per forzare un commit locale o un backout dei messaggi in dubbio conservati in una coda di trasmissione.

Utilizzare l'opzione Risolvi quando i messaggi sono in dubbio da parte di un mittente o di un server, ad esempio perché un'estremità del collegamento è terminata e non vi è alcuna possibilità che venga ripristinata. L'opzione Resolve accetta uno dei seguenti 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
- La definizione del canale, locale, deve esistere
- Il gestore code deve essere in esecuzione, locale

IBM i *18=Visualizza autorizzazione*

Utilizzare l'opzione Visualizzazione autorizzazione per visualizzare le azioni che un utente è autorizzato ad eseguire su un determinato oggetto IBM MQ .

Per un oggetto scelto e per un utente, il comando DSPMQAUT mostra le autorizzazioni di cui l'utente dispone per eseguire azioni su un oggetto IBM MQ . Se l'utente è un membro di più gruppi, il comando mostra l'autorizzazione combinata di tutti i gruppi all'oggetto.

IBM i *19=Concedi autorizzazione*

Utilizzare l'opzione Concedi autorizzazione per concedere l'autorità di eseguire azioni sugli oggetti IBM MQ a un altro utente o gruppo di utenti.

il comando GRTMQMAUT è disponibile solo per gli utenti del gruppo QMQMADM. Un utente in QMQMADM concede l'autorizzazione ad altri utenti per eseguire azioni sugli oggetti IBM MQ indicati nel comando identificando gli utenti per nome o concedendo l'autorizzazione a tutti gli utenti in *PUBLIC.

IBM i *20=Revoca autorizzazione*

Utilizzare Revoca autorizzazione per eliminare l'autorizzazione ad eseguire azioni sugli oggetti dagli utenti.

Il comando RVKMQMAUT è disponibile solo per gli utenti del gruppo QMQMADM. Un utente nel gruppo QMQMADM rimuove l'autorizzazione da altri utenti per eseguire azioni sugli oggetti IBM MQ indicati nel comando identificando gli utenti per nome o revocando l'autorizzazione a tutti gli utenti in *PUBLIC.

IBM i *21=Ripristina oggetto*

Utilizzare Ripristina oggetto per ripristinare gli oggetti danneggiati dalle informazioni memorizzate nei giornali IBM MQ .

Recupera oggetto utilizza il comando RCRMQMOBJ (Re-create MQ Object) per recuperare tutti gli oggetti danneggiati indicati nel comando. Se un oggetto non è danneggiato, non viene eseguita alcuna azione su tale oggetto.

IBM i *22=Registrazione immagine*

Utilizzare l'immagine record per ridurre il numero di ricevitori di giornale richiesti per il recupero di una serie di oggetti e per ridurre al minimo il tempo di recupero.

Il comando RCDMQMIMG prende un punto di controllo per tutti gli oggetti selezionati nel comando. Sincronizza i valori correnti degli oggetti nell'IFS (integrated file system) con le informazioni successive sugli oggetti, come MQPUT e MQGET registrati nei ricevitori di giornale.

Quando il comando viene completato, gli oggetti nell'IFS sono aggiornati e non è più necessario che tali ricevitori di giornale siano presenti per ripristinare gli oggetti. Tutti i ricevitori di giornale scollegati possono essere scollegati (purché non sia necessario che siano presenti per ripristinare altri oggetti).

IBM i Impostazione della comunicazione per IBM i

Quando un canale di gestione dell'accodamento distribuito viene avviato, tenta di utilizzare la connessione specificata nella definizione del canale. Perché abbia esito positivo, è necessario che la connessione sia definita e disponibile.

DQM è una funzione di accodamento remoto per IBM MQ for IBM i. Fornisce programmi di controllo del canale per il Gestore code IBM MQ for IBM i che formano l'interfaccia per i collegamenti di comunicazione, controllabili dall'operatore di sistema.

Quando un canale di gestione dell'accodamento distribuito viene avviato, tenta di utilizzare la connessione specificata nella definizione del canale. Perché abbia esito positivo, è necessario che la connessione sia definita e disponibile. Questa sezione spiega come verificare che la connessione sia definita e disponibile.

Prima di avviare un canale, la coda di trasmissione deve essere definita come descritto in questa sezione e deve essere inclusa nella definizione del canale di messaggi.

È possibile scegliere l'etere delle seguenti due forme di comunicazione tra sistemi IBM MQ for IBM i :

- “Definizione di un collegamento TCP su IBM i” a pagina 268

  Per TCP, è possibile utilizzare un indirizzo host e tali connessioni sono configurate come descritto in *IBM i Communication Configuration Reference*.

  Nell'ambiente TCP, a ogni servizio distribuito viene assegnato un unico indirizzo TCP che può essere utilizzato dalle macchine remote per accedere al servizio. L'indirizzo TCP è composto da un nome host / numero e un numero di porta. Tutti i gestori code utilizzano tale numero per comunicare tra loro tramite TCP.
- “Ricezione su TCP” a pagina 269

  Questa forma di comunicazione richiede la definizione di una IBM i unità logica SNA di tipo 6.2 (LU 6.2) che fornisce il collegamento fisico tra il sistema IBM i che serve il gestore code locale e quello che serve il gestore code remoto. Fare riferimento al manuale *IBM i Communication Configuration Reference* per dettagli sulla configurazione delle comunicazioni in IBM i.

Ove necessario, l'accordo di attivazione deve essere preparato anche con la definizione dei processi e delle code necessari.

MQ Adv. CD V 9.1.4 Un canale messaggi che utilizza TCP/IP può essere puntato a IBM Aspera fasp.io Gateway, che utilizza un tunnel TCP/IP veloce, in grado di aumentare notevolmente la velocità di trasmissione della rete. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux. Consultare Definizione di una connessione Aspera gateway su Linux.

Attività correlate

“Monitoraggio e controllo dei canali su IBM i” a pagina 253
Utilizzare i comandi e i pannelli DQM per creare, monitorare e controllare i canali dei gestori code remoti. Ogni gestore code ha un programma DQM per il controllo delle interconnessioni ai gestori code remoti compatibili.

Riferimenti correlati

Configurazione di esempio - IBM MQ for IBM i

Esempio di pianificazione del canale di messaggi per IBM MQ for IBM i

Lavori di intercomunicazione su IBM i

Stati del canale su IBM i

IBM i *Definizione di un collegamento TCP su IBM i*

È possibile definire una connessione TCP all'interno della definizione di canale utilizzando il campo Nome connessione.

La definizione del canale contiene un campo, CONNECTION NAME, che contiene l'indirizzo di rete TCP della destinazione o il nome host (ad esempio ABCHOST). L'indirizzo di rete TCP può essere in formato decimale puntato IPv4 (ad esempio, 127.0.0.1) o esadecimale IPv6 (ad esempio, 2001:DB8:0:0:0:0:0:0). Se CONNECTION NAME è un nome host o un server dei nomi, la tabella host IBM i viene utilizzata per convertire il nome host in un indirizzo host TCP.

Un numero di porta è richiesto per un indirizzo TCP completo; se questo numero non viene fornito, viene utilizzato il numero di porta predefinito 1414. All'estremità iniziale di una connessione (tipi di canale mittente, richiedente e server) è possibile fornire un numero di porta facoltativo per la connessione, ad esempio:

```
Connection name 127.0.0.1 (1555)
```

In questo caso, l'estremità di avvio tenta di collegarsi ad un programma di ricezione alla porta 1555.

MQ Adv. CD V 9.1.4 Un canale messaggi che utilizza TCP/IP può essere puntato a IBM Aspera fasp.io Gateway, che utilizza un tunnel TCP/IP veloce, in grado di aumentare notevolmente la velocità di trasmissione della rete. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux. Consultare Definizione di una connessione Aspera gateway su Linux.

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.

Consultare “Utilizzo dell'opzione di backlog del listener TCP su IBM MQ for Multiplatforms” a pagina 250 per ulteriori informazioni e il valore specifico per IBM i.

Concetti correlati

“Ricezione su TCP” a pagina 269

I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente. Per rispondere alla richiesta di avvio, è necessario avviare un programma listener per rilevare le richieste di rete in arrivo e avviare il canale associato. Questo programma listener viene avviato con il comando STRMQMLSR.

IBM i *Ricezione su TCP*

I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente. Per rispondere alla richiesta di avvio, è necessario avviare un programma listener per rilevare le richieste di rete in arrivo e avviare il canale associato. Questo programma listener viene avviato con il comando STRMQMLSR.

È possibile avviare più di un listener per ciascun gestore code. Per impostazione predefinita, il comando STRMQMLSR utilizza la porta 1414, ma è possibile sovrascrivere questo valore. Per sovrascrivere l'impostazione predefinita, aggiungere le seguenti istruzioni al file qm.ini del gestore code selezionato. In questo esempio, il listener deve utilizzare la porta 2500:

```
TCP:
Port=2500
```

Il file qm.ini si trova in questa directory IFS: /QIBM/UserData/mqm/qmgrs/ *nome gestore code*.

Questo nuovo valore viene letto solo quando viene avviato il listener TCP. Se un listener è già in esecuzione, questa modifica non viene visualizzata da tale programma. Per utilizzare il nuovo valore, arrestare il listener ed emettere nuovamente il comando STRMQMLSR. Ora, ogni volta che si utilizza il comando STRMQMLSR, il listener assume il valore predefinito della nuova porta.

In alternativa, è possibile specificare un numero di porta diverso nel comando STRMQMLSR. Ad esempio:

```
STRMQMLSR MQMNAME( queue manager name ) PORT(2500)
```

Questa modifica rende il listener predefinito sulla nuova porta per la durata del lavoro listener.

Utilizzo dell'opzione TCP SO_KEEPALIVE

Se si desidera utilizzare l'opzione SO_KEEPALIVE (per ulteriori informazioni, consultare “Verifica che l'altra estremità del canale sia ancora disponibile” a pagina 213) è necessario aggiungere la seguente voce al file di configurazione del gestore code (qm.ini nella directory IFS, /QIBM/UserData/mqm/qmgrs/ *nome gestore code*):

```
TCP:
KeepAlive=yes
```

È quindi necessario immettere il seguente comando:

```
CFGTCP
```

Selezionare l'opzione 3 (Modifica attributi TCP). È ora possibile specificare un intervallo di tempo in minuti. È possibile specificare un valore compreso tra 1 e 40320 minuti; il valore predefinito è 120.

Utilizzo dell'opzione backlog del listener TCP

Quando si riceve su TCP, viene impostato un numero massimo di richieste di connessione in sospeso. Questo numero può essere considerato un *backlog* di richieste in attesa sulla porta TCP affinché il listener accetti la richiesta.

Il valore di backlog del listener predefinito su IBM i è 255. Se il backlog raggiunge questo valore, la connessione TCP viene rifiutata e non è possibile avviare il canale.

Per i canali MCA, ciò fa sì che il canale entri in uno stato RETRY e ritenti la connessione in seguito.

Per le connessioni client, il client riceve un codice motivo MQRC_Q_MGR_NOT_AVAILABLE da MQCONN e può ritentare la connessione in un secondo momento.

Tuttavia, per evitare questo errore, è possibile aggiungere una voce nel file qm.ini :

```
ListenerBacklog = n
```

Ciò sovrascrive il numero massimo predefinito di richieste in sospeso (255) per il listener TCP.

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.

IBM i *Definizione di una connessione LU 6.2 su IBM i*

Definire i dettagli delle comunicazioni LU 6.2 utilizzando un nome modalità, un nome TP e un nome connessione di una connessione LU 6.2 completa.

La fine iniziata del collegamento deve avere una definizione di voce di instradamento per completare questo oggetto CSI. Ulteriori informazioni sulla gestione delle richieste di lavoro dai sistemi LU 6.2 remoti sono disponibili in *IBM i Programming: Work Management Guide*.

Per informazioni, consultare il manuale *Multiplatform APPC Configuration Guide* e la seguente tabella.

Tabella 26. Impostazioni sul sistema IBM i locale per una piattaforma del gestore code remoto

Piattaforma remota	**TPNAME**
z/OS o MVS	Le stesse informazioni del lato corrispondente sul gestore code remoto.
IBM i	Uguale al valore di confronto nella specifica di instradamento sul sistema IBM i .
Sistemi UNIX and Linux	Il programma di transazione richiamabile definito nella configurazione della LU remota 6.2 .
Windows	Come specificato nel comando Windows Esegui listener o nel programma di transazione richiamabile definito utilizzando TpSetup su Windows.

Se si dispone di più di un gestore code sullo stesso computer, verificare che i nomi TP nelle definizioni del canale siano univoci.

Concetti correlati

“Fine inizializzazione (mittente)” a pagina 270
Utilizzare il comando CRTMQMCHL per definire un canale di tipo trasporto *LU62.

“Fine avviata (Ricevente)” a pagina 273
Utilizzare il comando CRTMQMCHL per definire l'estremità di ricezione del collegamento del canale dei messaggi con tipo di trasporto *LU62.

IBM i *Fine inizializzazione (mittente)*

Utilizzare il comando CRTMQMCHL per definire un canale di tipo trasporto *LU62.

L'utilizzo dell'oggetto CSI è facoltativo in IBM MQ for IBM i V5.3 o versioni successive.

Il pannello di avvio finale viene mostrato nella Figura LU 6.2 pannello di impostazione della comunicazione - avvio finale. Per ottenere il pannello completo come mostrato, premere F10 dal primo pannello.

```
Create Comm Side Information (CRTCSI)

Type choices, press Enter.

Side information . . . . . > WINSDOA1   Name
Library . . . . . >  QSYS    Name, *CURLIB
Remote location . . . . . > WINSDOA1   Name
Transaction program . . . . . > MQSERIES

Text 'description' . . . . . .  *BLANK


Additional Parameters

Device . . . . . .  *LOC     Name, *LOC
Local location . . . . . .  *LOC     Name, *LOC, *NETATR
Mode . . . . . .  JSTMOD92   Name, *NETATR
Remote network identifier . . .  *LOC     Name, *LOC, *NETATR, *NONE
Authority . . . . . .  *LIBCRTAUT  Name, *LIBCRTAUT, *CHANGE...

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

Figura 36. Pannello di impostazione della comunicazione LU 6.2 - inizio

Completare i campi di inizio come segue:

Informazioni laterali
Assegnare a questa definizione un nome utilizzato per memorizzare l'oggetto di informazioni lato da creare, ad esempio WINSDOA1.

Nota: Per LU 6.2, il collegamento tra la definizione del canale di messaggi e la connessione di comunicazione è il campo **Nome connessione** della definizione del canale di messaggi all'estremità di invio. Questo campo contiene il nome dell'oggetto CSI.

Libreria
Il nome della libreria in cui è memorizzata questa definizione.

L'oggetto CSI deve essere disponibile in una libreria accessibile al programma che serve il canale dei messaggi, ad esempio QSYS, QMQM e QGPL.

Se il nome non è corretto, è mancante o non è possibile trovarlo, si verifica un errore all'avvio del canale.

Ubicazione remota
Specifica il nome dell'ubicazione remota con cui comunica il programma.

In breve, questo parametro obbligatorio contiene il nome dell'unità logica del partner sul sistema remoto, come definito nella descrizione dell'unità utilizzata per il collegamento di comunicazione tra i due sistemi.

Il nome dell' **Ubicazione remota** può essere trovato immettendo il comando DSPNETA sul sistema remoto e visualizzando il nome dell'ubicazione locale predefinito.

Programma di transazione
Specifica il nome (massimo 64 caratteri) del programma di transazione sul sistema remoto da avviare. Può essere un nome processo di transazione, un nome programma, il nome canale o una stringa di caratteri che corrisponde al **Valore di confronto** nella voce di instradamento.

Questo parametro è obbligatorio.

Nota: Per specificare i nomi dei programmi di transazioni di servizi SNA, immettere la rappresentazione esadecimale del nome del programma di transazioni di servizio. Ad esempio, per specificare un nome del programma di transazione servizio con una rappresentazione esadecimale di 21F0F0F1, immettere X'21F0F0F1'.

Ulteriori informazioni sui nomi dei programmi di transazione del servizio SNA sono disponibili nel manuale *SNA Transaction Programmer's Reference* per il tipo LU 6.2.

Se l'estremità di ricezione è un altro sistema IBM i , il nome del **Programma di transazione** viene utilizzato per far corrispondere l'oggetto CSI all'estremità di invio con la voce di instradamento all'estremità di ricezione. Questo nome deve essere univoco per ogni gestore code sul sistema IBM i di destinazione. Consultare il parametro **Program to call** in Initiated end (Receiver). Consultare anche il parametro **Dati di confronto: valore di confronto** nel pannello Aggiungi voce di instradamento.

Descrizione testo
Una descrizione (fino a 50 caratteri) per ricordare l'uso previsto di questa connessione.

Periferica
Specifica il nome della descrizione unità utilizzata per il sistema remoto. I valori possibili sono:

***LOC**
L'unità è determinata dal sistema.

Nome - periferica
Specificare il nome dell'unità associata all'ubicazione remota.

Ubicazione locale
Specifica il nome dell'ubicazione locale. I valori possibili sono:

***LOC**
Il nome dell'ubicazione locale è determinato dal sistema.

***NETATR**
Viene utilizzato il valore LCLLOCNAME specificato negli attributi di rete del sistema.

Nome - ubicazione - locale
Specificare il nome della propria ubicazione. Specificare l'ubicazione locale se si desidera indicare un nome di ubicazione specifica per l'ubicazione remota. Il nome dell'ubicazione può essere trovato utilizzando il comando DSPNETA.

Modalità
Specifica la modalità utilizzata per controllare la sessione. Questo nome è lo stesso di CPI (Common Programming Interface) - Communications Mode_Name. I valori possibili sono:

***NETATR**
Viene utilizzata la modalità negli attributi di rete.

BLANK
Vengono utilizzati otto caratteri vuoti.

Nome - modalità
Specificare un nome di modalità per l'ubicazione remota.

Nota: Poiché la modalità determina la priorità di trasmissione della sessione di comunicazioni, potrebbe essere utile definire diverse modalità a seconda della priorità dei messaggi inviati; ad esempio MQMODE_HI, MQMODE_MED e MQMODE_LOW. (È possibile avere più di un CSI che punta alla stessa ubicazione.)

Identificativo di rete remota
Specifica l'identificativo di rete remota utilizzato con l'ubicazione remota. I valori possibili sono:

***LOC**
Viene utilizzato l'ID di rete remota per l'ubicazione remota.

***NETATR**
Viene utilizzato l'identificativo di rete remota specificato negli attributi di rete.

***NONE**
La rete remota non ha nome.

ID - rete - remota
Specificare un ID rete remota. Utilizzare il comando DSPNETA nell'ubicazione remota per trovare il nome di questo ID di rete. È l''ID di rete locale ' nell'ubicazione remota.

Autorità

Specifica l'autorizzazione che si sta fornendo agli utenti che non hanno un'autorizzazione specifica sull'oggetto, che non si trovano in un elenco di autorizzazioni e con un profilo di gruppo che non ha un'autorizzazione specifica sull'oggetto. I valori possibili sono:

***LIBCRTAUT**

L'autorizzazione pubblica per l'oggetto viene presa dal parametro CRTAUT della libreria specificata. Questo valore viene determinato al momento della creazione. Se il valore CRTAUT per la libreria cambia dopo la creazione dell'oggetto, il nuovo valore non influisce sugli oggetti esistenti.

***CHANGE**

L'autorizzazione alla modifica consente all'utente di eseguire funzioni di base sull'oggetto; tuttavia, l'utente non può modificare l'oggetto. L'autorizzazione alla modifica fornisce l'autorizzazione operativa sull'oggetto e su tutti i dati.

***ALL**

L'utente può eseguire tutte le operazioni tranne quelle limitate al proprietario o controllate dall'autorizzazione di gestione dell'elenco di autorizzazioni. L'utente può controllare l'esistenza dell'oggetto e specificare la sicurezza per l'oggetto, modificare l'oggetto ed eseguire funzioni di base sull'oggetto. L'utente può modificare la proprietà dell'oggetto.

***USE**

L'autorizzazione all'uso fornisce l'autorizzazione operativa sull'oggetto e l'autorizzazione alla lettura.

***EXCLUDE**

L'autorizzazione di esclusione impedisce all'utente di accedere all'oggetto.

Elenco autorizzazioni

Specificare il nome dell'elenco di autorizzazioni con l'autorizzazione utilizzata per le informazioni laterali.

IBM i *Fine avviata (Ricevente)*

Utilizzare il comando CRTMQMCHL per definire l'estremità di ricezione del collegamento del canale dei messaggi con tipo di trasporto *LU62.

Lasciare vuoto il campo CONNECTION NAME e verificare che i dettagli corrispondenti corrispondano all'estremità di invio del canale. Per i dettagli, vedi Creazione di un canale.

Per consentire all'estremità di avvio di avviare il canale di ricezione, aggiungere una voce di instradamento ad un sottosistema alla fine avviata. Il sottosistema deve essere quello che assegna l'unità APPC utilizzata nelle sessioni LU 6.2 . Pertanto, deve avere una voce di comunicazioni valida per tale unità. La voce di instradamento richiama il programma che avvia l'estremità di ricezione del canale messaggi.

Utilizzare i comandi IBM i (ad esempio, ADDRTGE) per definire la fine del collegamento avviato da una sessione di comunicazioni.

Il pannello di fine inizializzato viene mostrato in LU 6.2 pannello di impostazione della comunicazione - aggiungere la voce di instradamento.

```
Add Routing Entry (ADDRTGE)

Type choices, press Enter.

Subsystem description . . . . .  QCMN     Name
Library . . . . . .   *LIBL    Name, *LIBL, *CURLIB
Routing entry sequence number .  1       1-9999
Comparison data:
Compare value . . . . . .  MQSERIES

Starting position . . . . . .  37      1-80
Program to call . . . . . .  AMQCRC6B   Name, *RTGDTA
Library . . . . . .  QMAS400    Name, *LIBL, *CURLIB
Class . . . . . .  *SBSD     Name, *SBSD
Library . . . . . .  *LIBL     Name, *LIBL, *CURLIB
Maximum active routing steps . .  *NOMAX    0-1000, *NOMAX
Storage pool identifier . . . .  1       1-10



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

Figura 37. Pannello di impostazione delle comunicazioni LU 6.2 - fine avviata

Descrizione del sottosistema
Il nome del sottosistema in cui risiede questa definizione. Utilizzare il comando IBM i WRKSBSD per visualizzare e aggiornare la descrizione del sottosistema appropriata per la specifica di instradamento.

Numero di sequenza della voce di instradamento
Un numero univoco nel sottosistema per identificare questa definizione di comunicazione. È possibile utilizzare valori compresi tra 1 e 9999.

Dati di confronto: valore di confronto
Una stringa di testo da confrontare con la stringa ricevuta quando la sessione viene avviata da un parametro **Programma di transazione** , come mostrato nella Figura 1. La stringa di caratteri deriva dal campo Programma di transazione del CSI mittente.

Dati di confronto: posizione iniziale
La posizione del carattere nella stringa in cui deve iniziare il confronto.

Nota: Il campo della posizione iniziale è la posizione del carattere nella stringa per il confronto e questa posizione è sempre 37.

Programma da chiamare
Il nome del programma che esegue il programma messaggi in entrata da chiamare per avviare la sessione.

Il programma, AMQCRC6A, viene richiamato per il gestore code predefinito. Questo programma viene fornito con IBM MQ for IBM i e imposta l'ambiente e richiama AMQCRS6A.

Per ulteriori gestori code:

- Ogni gestore code ha un programma richiamabile LU 6.2 specifico ubicato nella propria libreria. Questo programma viene denominato AMQCRC6B e viene generato automaticamente quando viene creato il gestore code.
- Ogni gestore code richiede una voce di instradamento specifica con dati di instradamento univoci da aggiungere. Questi dati di instradamento devono corrispondere al nome del **Programma di transazione** fornito dal sistema richiedente (consultare Inizio fine (Mittente)).

Un esempio viene mostrato in LU 6.2 pannello di impostazione delle comunicazioni - visualizzare le voci di instradamento:

```
Display Routing Entries
System:  MY400
Subsystem description:  QCMN      Status:  ACTIVE

Type options, press Enter.
5=Display details

Start
Opt  Seq Nbr  Program    Library    Compare Value   Pos
10   *RTGDTA           'QZSCSRVR'     37
20   *RTGDTA           'QZRCSRVR'     37
30   *RTGDTA           'QZHQTRG'     37
50   *RTGDTA           'QVPPRINT'     37
60   *RTGDTA           'QNPSERVR'     37
70   *RTGDTA           'QNMAPINGD'    37
80   QNMAREXECD  QSYS     'AREXECD'     37
90   AMQCRC6A   QMQMBW    'MQSERIES'     37
100   *RTGDTA           'QTFDWNLD'     37
150   *RTGDTA           'QMFRCVR'     37


F3=Exit  F9=Display all detailed descriptions  F12=Cancel
```

Figura 38. Pannello di impostazione delle comunicazioni LU 6.2 - fine avviata

Nel pannello di configurazione delle comunicazioni LU 6.2 - voci di instradamento di visualizzazione, il numero di sequenza 90 rappresenta il gestore code predefinito e fornisce la compatibilità con le configurazioni delle release precedenti (ovvero, V3R2, V3R6, V3R7e V4R2) di IBM MQ for IBM i. Queste release consentono un solo gestore code. I numeri di sequenza 92 e 94 rappresentano due ulteriori gestori code denominati ALPHA e BETA creati con librerie QMALPHA e QMBETA.

Nota: È possibile avere più di una voce di instradamento per ciascun gestore code utilizzando dati di instradamento differenti. Queste voci forniscono l'opzione di priorità di lavoro differenti a seconda delle classi utilizzate.

Classe
Il nome e la libreria della classe utilizzata per i passi avviati tramite questa specifica di instradamento. La classe definisce gli attributi dell'ambiente di esecuzione del passo di instradamento e specifica la priorità lavoro. È necessario specificare una voce di classe appropriata. Utilizzare, ad esempio, il comando WRKCLS per visualizzare le classi esistenti o per creare una classe. Ulteriori informazioni sulla gestione delle richieste di lavoro dai sistemi LU 6.2 remoti sono disponibili in *IBM i Programming: Work Management Guide*.

Nota sulla gestione del lavoro

Il lavoro AMQCRS6A non è in grado di sfruttare le normali funzioni di gestione lavoro di IBM i documentate in Gestione lavoro poiché non viene avviato nello stesso modo di altri lavori IBM MQ . Per modificare le proprietà di runtime dei lavori del destinatario LU62 , è possibile apportare una delle seguenti modifiche:

- Modificare la descrizione della classe specificata nella specifica di instradamento per il lavoro AMQCRS6A
- Modificare la descrizione del lavoro sulla specifica di comunicazioni

Consultare *IBM i Programming: Work Management Guide* per ulteriori informazioni sulla configurazione dei lavori di comunicazione.

Configurazione di un cluster di gestore code

I cluster forniscono un meccanismo per l'interconnessione dei gestori code in modo da semplificare sia la configurazione iniziale che la gestione in corso. È possibile definire componenti cluster e creare e gestire cluster.

Prima di iniziare

Per un'introduzione ai concetti di cluster, consultare Cluster.

Quando si progetta il cluster del gestore code, è necessario prendere alcune decisioni. Vedi Cluster di esempio e Progettazione dei cluster.

Attività correlate

“Spostamento di una definizione di argomento del raggruppamento in un gestore code differente” a pagina 404
Per l'host argomento instradato o i cluster instradati direttamente, potrebbe essere necessario spostare una definizione dell'argomento del cluster durante la disattivazione di un gestore code o perché un gestore code del cluster ha riportato un errore o non è disponibile per un periodo di tempo significativo.

Riferimenti correlati

Elimina argomento

Definizione dei componenti di un cluster

I cluster sono composti da gestori code, canali cluster e code cluster. È possibile definire le code del cluster e modificare alcuni aspetti degli oggetti cluster predefiniti. È possibile ottenere informazioni di configurazione e stato sui canali definiti automaticamente e sulla relazione tra i singoli canali mittente del cluster e le code di trasmissione.

Consultare i seguenti argomenti secondari per informazioni sulla definizione di ciascuno dei componenti cluster:

Concetti correlati

Componenti di un cluster

Canali cluster

Attività correlate

Definizione degli argomenti del cluster

“Configurazione di un nuovo cluster” a pagina 287
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.

“Aggiunta di un gestore code a un cluster” a pagina 299
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.

Definizione di 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 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.

z/OS Una coda del cluster può essere una coda condivisa dai membri di un gruppo di condivisione di code in IBM 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

Un gestore code può memorizzare i messaggi per altri gestori code di 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 creata automaticamente una coda di trasmissione cluster differente 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 stanno utilizzando delle SYSTEM.CLUSTER.TRANSMIT.QUEUES dedicate con un gestore code che era stato aggiornato da una versione del prodotto antecedente a IBM WebSphere MQ 7.5, assicurarsi che laSYSTEM.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 tranne che su z/OS. z/OS Su z/OS, la definizione può essere definita con l'esempio fornito **CSQ4INSX**.

È possibile configurare un gestore code per trasferire i messaggi ad altri gestori code con 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. IBM MQ crea automaticamente una definizione equivalente ad una definizione di 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
```

Concetti correlati

Code cluster

Riferimenti correlati

Nome ClusterChannel(MQCHAR20)

Utilizzo dei canali mittenti del cluster definiti in modo automatico

Dopo aver introdotto un gestore code in un cluster effettuando le definizioni CLUSSDR e CLUSRCVR iniziali, IBM MQ crea automaticamente altre definizioni del canale mittente del cluster quando richiesto per spostare i messaggi in un altro gestore code del cluster. È possibile visualizzare le informazioni sui canali mittenti del cluster definiti automaticamente, ma non è possibile modificarle. Per modificarne il funzionamento, è possibile utilizzare un'uscita di definizione automatica del canale.

Prima di iniziare

Per un'introduzione ai canali definiti automaticamente, consultare Canali mittenti del cluster definiti automaticamente.

Informazioni su questa attività

I canali mittente del cluster definiti automaticamente vengono creati dal cluster come e quando necessario e rimangono attivi fino a quando non vengono arrestati utilizzando le normali regole di intervallo di disconnessione.

I canali mittenti del cluster (CLUSSDR) possono essere definiti automaticamente per spostare i messaggi dell'applicazione e i messaggi di gestione del cluster interni. Ad esempio, in un cluster di pubblicazione / sottoscrizione (uno in cui è stato definito un argomento del cluster), i canali possono essere definiti tra repository parziali per consentire lo scambio dello stato di 'sottoscrizione proxy '. Quando non sono richiesti (inattivi) per un periodo di tempo prolungato, i CLUSSDR definiti automaticamente vengono rimossi dalla cache di un repository parziale delle informazioni sul cluster e non sono più visibili su tale gestore code.

Multi Su Multipiattaforme, OAM (object authority manager) non è consapevole dell'esistenza di canali mittenti del cluster definiti automaticamente. Se si immettono i comandi **start**, **stop**, **ping**, **reset**o **resolve** su un canale mittente del cluster definito automaticamente, OAM controlla se si è autorizzati a eseguire la stessa azione sul canale ricevente del cluster corrispondente.

z/OS Su z/OS, è possibile proteggere un canale mittente del cluster definito automaticamente come qualsiasi altro canale.

Procedura

- Visualizzare le informazioni sui canali definiti automaticamente per un determinato gestore code cluster.

  Non è possibile visualizzare automaticamente i canali definiti utilizzando il comando DISPLAY CHANNEL **runmqsc** . Per visualizzare i canali definiti automaticamente utilizzare il seguente comando:

  ```
  DISPLAY CLUSQMGR(qMgrName)
  ```

- Visualizza lo stato del canale definito automaticamente per un determinato CLUSRCVR.

  Per visualizzare lo stato del canale CLUSSDR definito automaticamente corrispondente alla definizione di canale CLUSRCVR creata, utilizzare il seguente comando:

  ```
  DISPLAY CHSTATUS(channelname)
  ```

- Utilizzare un'uscita di definizione automatica del canale per modificare il comportamento di un canale definito automaticamente.

  È possibile utilizzare l'uscita di definizione automatica del canale IBM MQ se si desidera scrivere un programma di uscita utente per personalizzare un canale mittente del cluster o un canale ricevente del cluster. Ad esempio, è possibile utilizzare l'uscita di definizione automatica del canale in un ambiente cluster per apportare le seguenti modifiche:

  - Personalizzare le definizioni delle comunicazioni, ovvero i nomi SNA LU6.2 .

- Aggiungere o rimuovere altre uscite, ad esempio uscite di sicurezza.
- Modificare i nomi delle uscite canale.

  Il nome dell'uscita del canale CLUSSDR viene generato automaticamente dalla definizione di canale CLUSRCVR e, pertanto, potrebbe non essere appropriato per le proprie esigenze, soprattutto se le due estremità del canale si trovano su piattaforme differenti.

  Il formato dei nomi di uscita è diverso su piattaforme differenti. Ad esempio:

  - z/OS Sulla piattaforma z/OS , il formato del parametro SCYEXIT (*nome uscita di sicurezza*) è `SCYEXIT('SECEXIT')`
  - Windows Su piattaforme Windows , il formato del parametro SCYEXIT (*nome uscita di sicurezza*) è `SCYEXIT(' drive:\path\library (secexit)')`

  Nota: z/OS Se non è presente alcuna uscita di definizione automatica del canale, il gestore code z/OS ricava il nome dell'uscita del canale CLUSSDR dalla definizione del canale CLUSRCVR sull'altra estremità del canale. Per derivare il nome dell'uscita z/OS da un nome nonz/OS , viene utilizzato l'algoritmo seguente:

  - I nomi di uscita su Multipiattaforme sono nel formato generale *percorso*/*libreria* (*funzione*).
  - Se è presente *function* , vengono utilizzati fino a otto caratteri.
  - Altrimenti, vengono utilizzati fino a otto caratteri della *libreria* .

  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 i gestori code precedenti a IBM WebSphere MQ 7, impostare l'attributo **PROPCTL** su un valore NONE.

  Ogni canale mittente del cluster definito automaticamente è basato sul corrispondente canale ricevente del cluster. Prima di IBM WebSphere MQ 7, il canale ricevente del cluster non ha un attributo **PROPCTL** , quindi questo attributo è impostato su COMPAT nel canale mittente del cluster definito automaticamente.

  Se il cluster deve utilizzare **PROPCTL** per rimuovere le intestazioni dell'applicazione come RFH2 dai messaggi che vanno da un gestore code IBM WebSphere MQ 7 o successivo a un gestore code su una versione precedente di IBM MQ, è necessario scrivere un'uscita di definizione automatica del canale che imposta **PROPCTL** sul valore NONE.

- Utilizzare l'attributo del canale LOCLADDR per controllare gli aspetti dell'indirizzamento.
  - Per abilitare un canale in uscita (TCP) per utilizzare un particolare indirizzo IP, porta o intervallo di porte, utilizzare l'attributo del canale LOCLADDR. Ciò 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 possibile scrivere un'uscita di definizione automatica del canale per forzare il valore LOCLADDR in uno qualsiasi dei relativi canali CLUSSDR definiti automaticamente. È necessario specificarlo anche nel canale definito manualmente CLUSSDR .
  - 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 o un intervallo di porte specifici per tutte le relative comunicazioni in uscita.

  Nota: 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 .

Multi Su Multipiattaforme, è possibile impostare un valore di indirizzo locale predefinito che viene 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.

Riferimenti correlati

Indirizzo locale (LOCLADDR)

Utilizzo degli oggetti cluster predefiniti

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.

Per un elenco completo di questi oggetti, consultare Oggetti cluster predefiniti. Il seguente elenco include solo gli oggetti che è possibile modificare.

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.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 z/OS , tranne in z/OS . 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*.

Concetti correlati

Oggetti cluster predefiniti

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

I messaggi tra i gestori code con cluster vengono memorizzati nelle code di trasmissione cluster e inoltrati dai canali mittenti del cluster. 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. L'elaborazione di questo switch è automatizzata e transazionale.

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. La “Selezione di code di trasmissione predefinite per canali mittente del cluster” a pagina 282 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 283 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 284 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 IBM WebSphere MQ 7.5, le connessioni cluster hanno condiviso la singola coda di trasmissione cluster, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Da IBM WebSphere MQ 7.5 in poi, si ha l'opzione di canali mittenti del cluster che non condividono 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 Cluster: Pianificazione della configurazione delle code di trasmissione cluster 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 334.

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 39 a pagina 283. 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`.

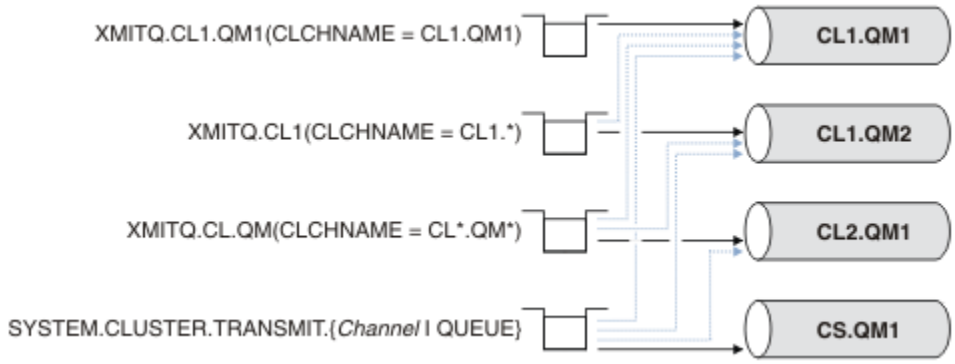


Figura 39. Precedenza coda di trasmissione / canale mittente del cluster

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 39 a pagina 283 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 39 a pagina 283 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 del 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.QUEUE`e 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.

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. Quando è disponibile 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 40 a pagina 286, `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 dei 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 poi come separare i messaggi per un determinato canale su 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 40 a pagina 286, 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.QUEUE`o 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.

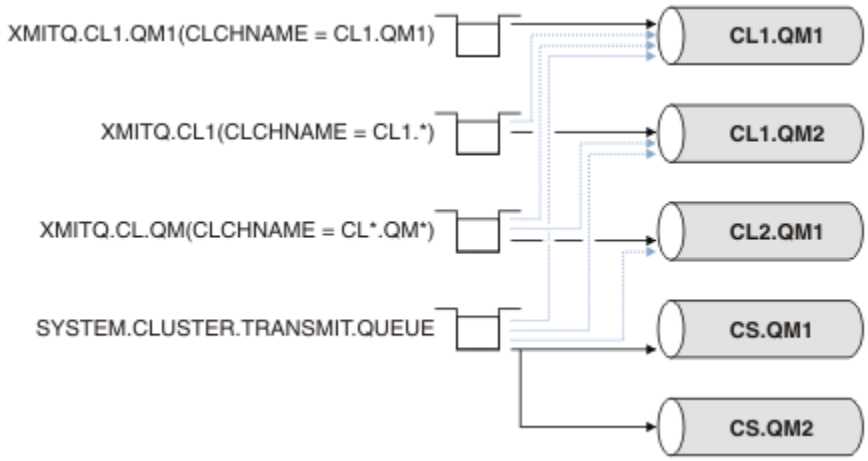


Figura 40. Più canali mittente cluster

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 284.

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

Canali cluster

“Calcolo della dimensione del log” a pagina 599
Stima della dimensione del log necessaria per un gestore code.

Attività correlate

Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster

Clustering: pianificazione della configurazione delle code di trasmissione del cluster

“Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 324
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 301
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 331
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 334
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.

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.

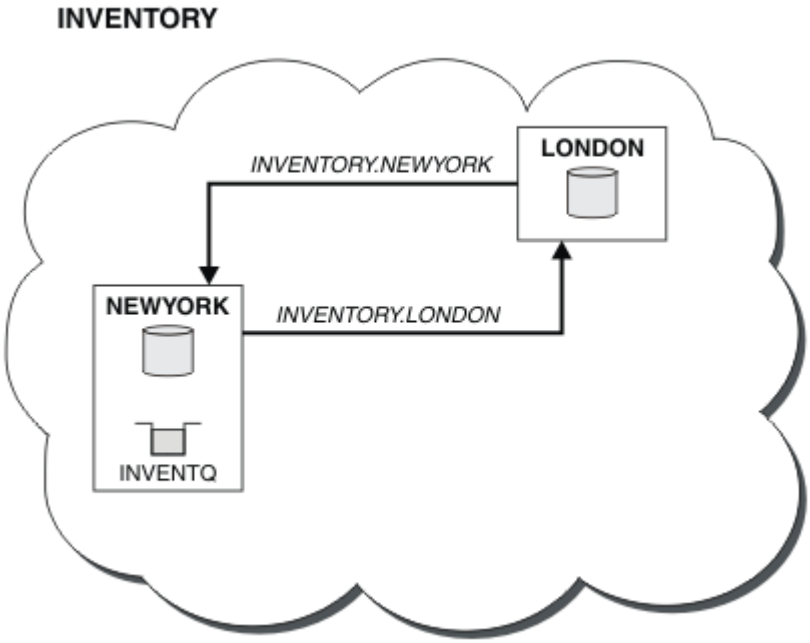
Prima di iniziare

- Invece di attenersi alle seguenti istruzioni, è possibile utilizzare una delle procedure guidate fornite con IBM 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 aiutino l'utente a comprendere le operazioni eseguite per configurare un cluster, consultare “Definizione di code cluster” a pagina 276, Canali cluster e Listener.

Informazioni su questa attività

Si sta configurando una nuova rete IBM 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.

Questo è il seguente aspetto del



cluster:

È possibile configurare ciascun gestore code nel cluster per inviare messaggi ad altri gestori code nel cluster utilizzando code di trasmissione del 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.

INVENTORY è un cluster piccolo. Tuttavia, è utile come prova di concetto. La cosa importante da capire su questo cluster è l'ambito che offre per il miglioramento futuro.

Procedura

- “Impostazione di un cluster utilizzando TCP/IP con una coda di trasmissione singola per gestore code” a pagina 289
- “Configurazione di un cluster su TCP/IP utilizzando più code di trasmissione per gestore code” a pagina 292

- “Configurazione di un cluster utilizzando LU 6.2 su z/OS” a pagina 295
- “Verifica del cluster” a pagina 297

Concetti correlati

Cluster

Confronto tra cluster e accodamento distribuito

Componenti di un cluster

Attività correlate

“Configurazione di un cluster di gestore code” a pagina 275

I cluster forniscono un meccanismo per l'interconnessione dei gestori code in modo da semplificare sia la configurazione iniziale che la gestione in corso. È possibile definire componenti cluster e creare e gestire cluster.

Impostazione di un cluster utilizzando TCP/IP con una coda di trasmissione singola per gestore code

Questo è uno dei tre argomenti che descrivono diverse configurazioni per un cluster semplice.

Prima di iniziare

Per una panoramica del cluster che viene creato, consultare “Configurazione di un nuovo cluster” a pagina 287.

L'attributo del gestore code, **DEFCLXQ**, deve essere lasciato come valore predefinito, SCTQ.

Informazioni su questa attività

Attenersi a questa procedura per impostare un cluster su Multipiattaforme utilizzando il protocollo di trasporto TCP/IP. z/OS Su z/OS, è necessario seguire le istruzioni in “Definizione di un collegamento TCP su z/OS” a pagina 923 per impostare la connessione TCP/IP, anziché definire i listener nel passo “4” a pagina 290. Altrimenti, i passaggi sono gli stessi per z/OS, ma i messaggi di errore vengono scritti nella console, piuttosto che nel log degli errori del gestore code.

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 299.

   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 IBM 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 di gestore code locale utilizzando il comando ALTER QMGR e specificando l'attributo REPOS :

```
ALTER QMGR REPOS(INVENTORY)
```

```
1 : ALTER QMGR REPOS(INVENTORY)
AMQ8005: IBM 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)
```

   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, è possibile definire un canale ricevente del cluster su cui il gestore code può ricevere messaggi. Vedere Cluster - receiver channel: CLUSRCVR . Il canale CLUSRCVR definisce il nome della 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 con punti IPv4 . Ad esempio, 192.0.2.0o IPv6 formato esadecimale; 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 utilizza 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 .

   Definire manualmente il canale CLUSSDR da ogni gestore code del repository completo a ogni altro gestore code del repository completo nel cluster. Fare riferimento a Canale mittente del cluster: CLUSSDR . In questo caso, ci sono solo due gestori code, entrambi con repository completi. Ciascuno di essi ha bisogno di un canale CLUSSDR definito manualmente 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.

Operazioni successive

Sei ora pronto a verificare il cluster.

Attività correlate

“Configurazione di un cluster su TCP/IP utilizzando più code di trasmissione per gestore code” a pagina 292
Questo è uno dei tre argomenti che descrivono diverse configurazioni per un cluster semplice.

“Configurazione di un cluster utilizzando LU 6.2 su z/OS” a pagina 295
Questo è uno degli argomenti della struttura ad albero che descrivono diverse configurazioni per un cluster semplice.

Configurazione di un cluster su TCP/IP utilizzando più code di trasmissione per gestore code

Questo è uno dei tre argomenti che descrivono diverse configurazioni per un cluster semplice.

Prima di iniziare

Per una panoramica del cluster che viene creato, consultare “Configurazione di un nuovo cluster” a pagina 287.

Informazioni su questa attività

Attenersi a questa procedura per impostare un cluster su Multipiattaforme utilizzando il protocollo di trasporto TCP/IP. 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 utilizzare anche code di trasmissione differenti, seguire l'attività, “Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 301.

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 299.

   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 IBM 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 di gestore code locale utilizzando il comando ALTER QMGR e specificando l'attributo REPOS :

```
ALTER QMGR REPOS(INVENTORY)
```

```
1 : ALTER QMGR REPOS(INVENTORY)
AMQ8005: IBM 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 299 e “Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 301.

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)
```

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, è possibile definire un canale ricevente del cluster su cui il gestore code può ricevere messaggi. Vedere Cluster - receiver channel: CLUSRCVR . Il canale CLUSRCVR definisce il nome della 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 con punti IPv4 . Ad esempio, `192.0.2.0`o IPv6 formato esadecimale; 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 utilizza 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 .

   Definire manualmente il canale CLUSSDR da ogni gestore code del repository completo a ogni altro gestore code del repository completo nel cluster. Fare riferimento a Canale mittente del cluster: CLUSSDR . In questo caso, ci sono solo due gestori code, entrambi con repository completi. Ciascuno di essi ha bisogno di un canale CLUSSDR definito manualmente 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.

Operazioni successive

Sei ora pronto a verificare il cluster.

Attività correlate

“Impostazione di un cluster utilizzando TCP/IP con una coda di trasmissione singola per gestore code” a pagina 289
Questo è uno dei tre argomenti che descrivono diverse configurazioni per un cluster semplice.

“Configurazione di un cluster utilizzando LU 6.2 su z/OS” a pagina 295
Questo è uno degli argomenti della struttura ad albero che descrivono diverse configurazioni per un cluster semplice.

Configurazione di un cluster utilizzando LU 6.2 su z/OS

Questo è uno degli argomenti della struttura ad albero che descrivono diverse configurazioni per un cluster semplice.

Prima di iniziare

Per una panoramica del cluster che viene creato, consultare “Configurazione di un nuovo cluster” a pagina 287.

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 299.

   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 di gestore code locale utilizzando il comando ALTER QMGR e specificando l'attributo REPOS :

   ```
   ALTER QMGR REPOS(INVENTORY)
   ```

   ```
   1 : ALTER QMGR REPOS(INVENTORY)
   AMQ8005: IBM 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.

   z/OS Consultare L'iniziatore di canali su z/OS e “Ricezione su LU 6.2” a pagina 927.

   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, è possibile definire un canale ricevente del cluster su cui il gestore code può ricevere messaggi. Vedere Cluster - receiver channel: CLUSRCVR . Il canale CLUSRCVR definisce il nome della 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 .

   Definire manualmente il canale CLUSSDR da ogni gestore code del repository completo a ogni altro gestore code del repository completo nel cluster. Fare riferimento a Canale mittente del cluster: CLUSSDR . In questo caso, ci sono solo due gestori code, entrambi con repository completi. Ciascuno di essi ha bisogno di un canale CLUSSDR definito manualmente 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.

Operazioni successive

Sei ora pronto a verificare il cluster.

Attività correlate

“Impostazione di un cluster utilizzando TCP/IP con una coda di trasmissione singola per gestore code” a pagina 289
Questo è uno dei tre argomenti che descrivono diverse configurazioni per un cluster semplice.

“Configurazione di un cluster su TCP/IP utilizzando più code di trasmissione per gestore code” a pagina 292
Questo è uno dei tre argomenti che descrivono diverse configurazioni per un cluster semplice.

Verifica del cluster

Gli argomenti peer descrivono tre diverse configurazioni per un cluster semplice. Questo argomento spiega come verificare il cluster.

Prima di iniziare

In questo argomento si presuppone che si stia verificando un cluster creato mediante una delle seguenti attività:

- “Impostazione di un cluster utilizzando TCP/IP con una coda di trasmissione singola per gestore code” a pagina 289.
- “Configurazione di un cluster su TCP/IP utilizzando più code di trasmissione per gestore code” a pagina 292.
- “Configurazione di un cluster utilizzando LU 6.2 su z/OS” a pagina 295.

Per una panoramica del cluster creato, consultare “Configurazione di un nuovo cluster” a pagina 287.

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 287. 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 creare definizioni su altri gestori code per l'invio al canale ricevente del cluster INVENTORY.PARIS. Le altre definizioni vengono effettuate automaticamente quando necessario. Vedere Canali cluster.

3. z/OS
   Avviare l'iniziatore di canali su IBM MQ for z/OS.
4. Definire un canale CLUSSDR nel gestore code PARIS.

   Quando si aggiunge a un cluster un gestore code che non è un repository completo, si definisce un solo canale mittente del cluster per stabilire una connessione iniziale a tale repository. Fare riferimento a Canale mittente del cluster: CLUSSDR .

   Su PARIS, creare la seguente definizione per un canale CLUSSDR denominato INVENTORY.LONDON nel 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')
   ```

5. Opzionale: Se si sta aggiungendo a un cluster un gestore code che è stato precedentemente rimosso dallo stesso cluster, verificare che venga visualizzato come membro del cluster. In caso contrario, completare i seguenti passi aggiuntivi:
   a) 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 aggiornamenti sullo stato a tutti i gestori code interessati. Consultare Refreshing in a large cluster can affect performance and availability of the cluster.
   b) Riavvia il canale CLUSSDR

      (ad esempio, utilizzando il comando START CHANNEL).
   c) Riavviare il canale CLUSRCVR.

Risultati

La seguente figura mostra il cluster configurato da questa attività.

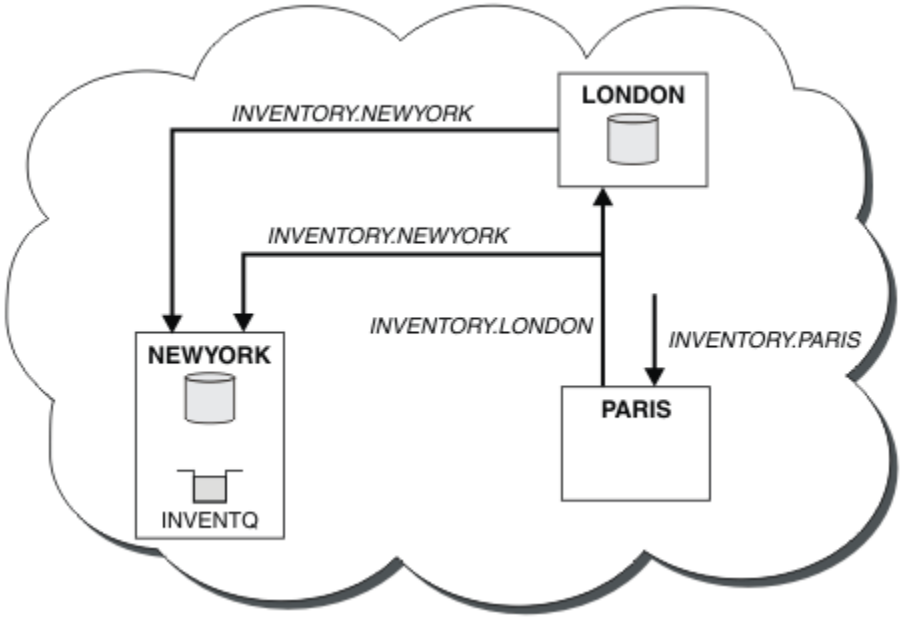


Figura 41. Il cluster INVENTORY con tre gestori code

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 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 287.

Informazioni su questa attività

Questa attività è un'alternativa a "Aggiunta di un gestore code a un cluster" a pagina 299, 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 stanno utilizzando delle SYSTEM.CLUSTER.TRANSMIT.QUEUES dedicate con un gestore code che era stato aggiornato da una versione del prodotto antecedente a IBM WebSphere MQ 7.5, assicurarsi che laSYSTEM.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 creare definizioni su altri gestori code per l'invio al canale ricevente del cluster INVENTORY.PARIS. Le altre definizioni vengono effettuate automaticamente quando necessario. Vedere Canali cluster.

4. Definire un canale CLUSSDR nel gestore code PARIS.

   Quando si aggiunge a un cluster un gestore code che non è un repository completo, si definisce un solo canale mittente del cluster per stabilire una connessione iniziale a tale repository. Fare riferimento a Canale mittente del cluster: CLUSSDR .

   Su PARIS, creare la seguente definizione per un canale CLUSSDR denominato INVENTORY.LONDON nel 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.

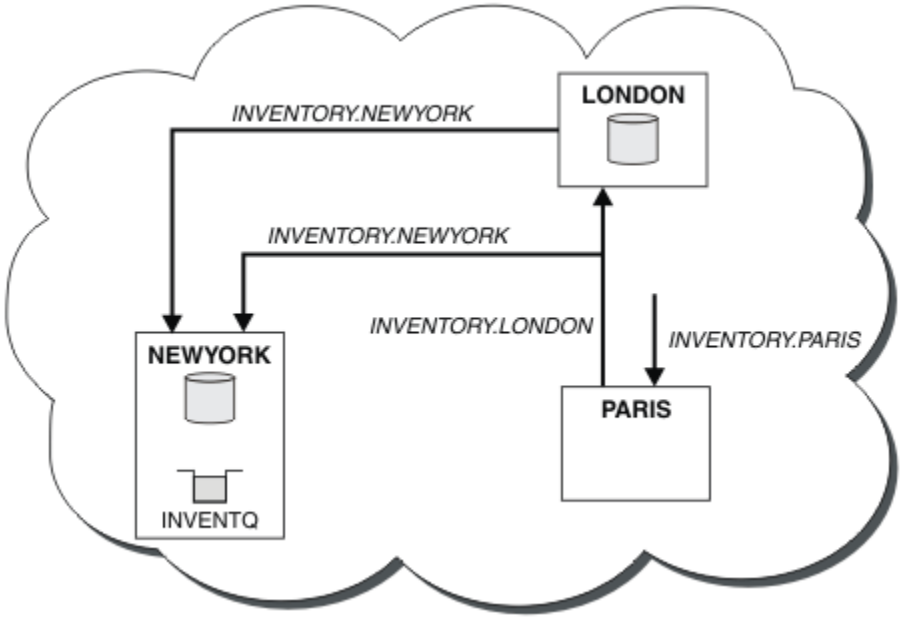


Figura 42. Il cluster INVENTORY con tre gestori code

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.

Attività correlate

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 .

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 287. 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 MQ di individuare il nome della connessione dal sistema, omettendo CONNAMEo specificando CONNAME(' '). IBM 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 si sta aggiungendo a un cluster un gestore code che è stato precedentemente rimosso dallo stesso cluster, verificare che venga visualizzato come membro del cluster. In caso contrario, completare i seguenti passi aggiuntivi:
   a) 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 aggiornamenti sullo stato a tutti i gestori code interessati. Consultare Refreshing in a large cluster can affect performance and availability of the cluster.
   b) Riavvia il canale CLUSSDR

      (ad esempio, utilizzando il comando START CHANNEL).
   c) Riavviare il canale CLUSRCVR.

Risultati

Il cluster configurato da questa attività è lo stesso di "Aggiunta di un gestore code a un cluster" a pagina 299:

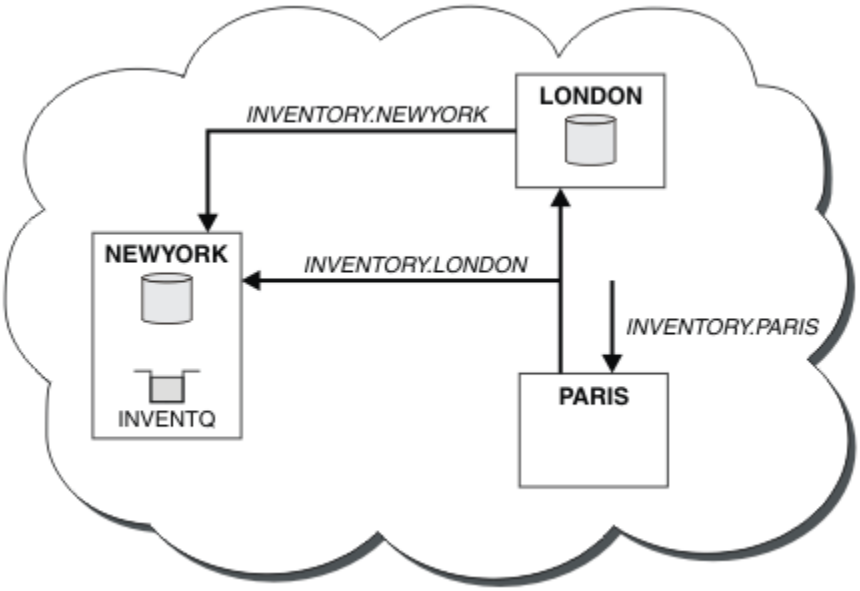


Figura 43. Il cluster INVENTORY con tre gestori code

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 MQ risolve +QMNAME+ nel nome del gestore code (LONDON). IBM MQ mette quindi in corrispondenza la definizione di un canale denominato INVENTORY.LONDON con la corrispondente definizione CLUSRCVR .

IBM 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.

Attività correlate

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.

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 299. 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 310.

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 si sta aggiungendo a un cluster un gestore code che è stato precedentemente rimosso dallo stesso cluster, verificare che venga visualizzato come membro del cluster. In caso contrario, completare i seguenti passi aggiuntivi:
   a) 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 aggiornamenti sullo stato a tutti i gestori code interessati. Consultare Refreshing in a large cluster can affect performance and availability of the cluster.
   b) Riavvia il canale CLUSSDR

      (ad esempio, utilizzando il comando START CHANNEL).
   c) Riavviare il canale CLUSRCVR.
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 44 a pagina 308 mostra il cluster INVENTORY configurato da questa attività.

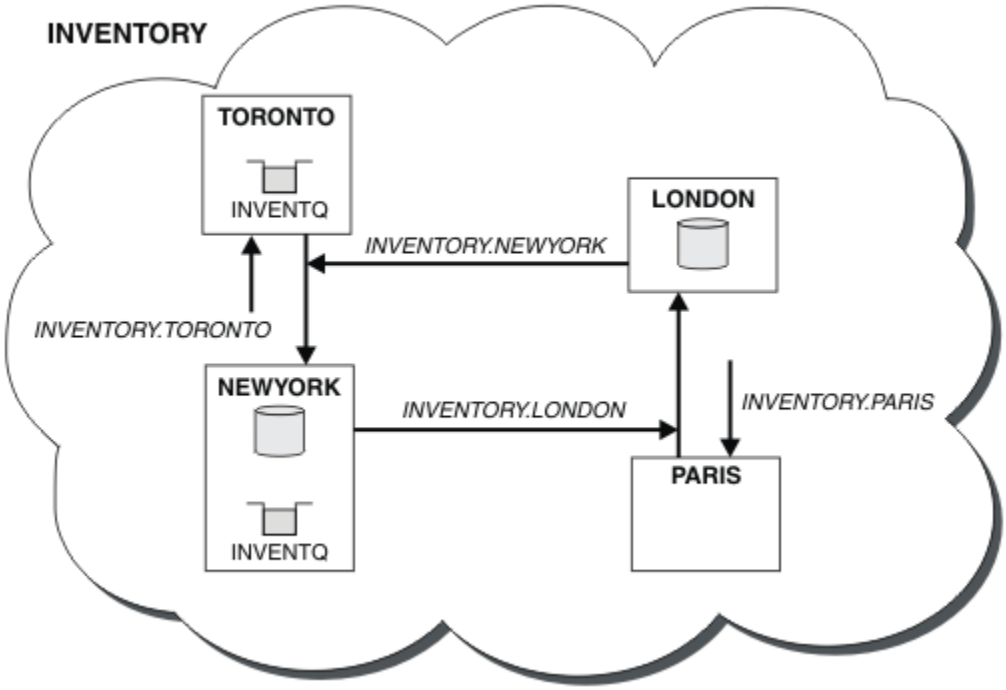


Figura 44. Il cluster INVENTORY con quattro gestori code

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 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.

z/OS Aggiunta di un gruppo di condivisione code ai cluster esistenti

Aggiungere un gruppo di condivisione code su z/OS ai cluster esistenti.

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. I gruppi di condivisione code sono supportati solo su IBM MQ for z/OS. Questa attività non è applicabile ad altre piattaforme.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in “Configurazione di un nuovo cluster” a pagina 287. Contiene due gestori code, LONDON e NEWYORK.
- Si desidera aggiungere un gruppo di condivisione code a questo cluster. Il gruppo, QSGP, comprende tre gestori code, P1, P2e P3. Condividono un'istanza della coda INVENTQ , che deve essere definita da P1.

Informazioni su questa attività

Effettuare le operazioni riportate di seguito per aggiungere nuovi gestori code che ospitano una coda condivisa.

Procedura

1. Decidere a quale repository completo i gestori code fanno riferimento per primi.

   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 particolarmente significativo quale repository completo si sceglie. In questo esempio, scegliere NEWYORK. Una volta che il gruppo di condivisione code si è unito al cluster, comunica con entrambi i repository completi.
2. Definire i canali CLUSRCVR .

   Ogni gestore code in un cluster deve definire un canale ricevente del cluster su cui può ricevere messaggi. In P1, P2e P3, definire:

   ```
   DEFINE CHANNEL(INVENTORY.Pn) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(Pn.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for sharing queue manager')
   ```

   Il canale ricevente del cluster annuncia la disponibilità di ciascun gestore code a ricevere messaggi da altri gestori code nel cluster INVENTORY.
3. Definire un canale CLUSSDR per il gruppo di condivisione code.

   Ogni membro di un cluster deve definire un canale mittente del cluster su cui può inviare messaggi al primo repository completo. In questo caso abbiamo scelto NEWYORK. Uno dei gestori code nel gruppo di condivisione code ha bisogno della seguente definizione di gruppo. La definizione garantisce che ogni gestore code abbia una definizione di canale mittente del cluster.

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) QSGDISP(GROUP)
   DESCR('Cluster-sender channel to repository at NEWYORK')
   ```
4. Definire la coda condivisa.

Definire la coda INVENTQ su P1 come segue:

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY) QSGDISP(SHARED) CFSTRUCT(STRUCTURE)
```

Avviare l'iniziatore di canali e un programma listener sul nuovo gestore code. Il programma listener ascolta le richieste di rete in entrata e avvia il canale ricevente del cluster quando è necessario.

Risultati

Figura 45 a pagina 310 mostra il cluster impostato da questa attività.

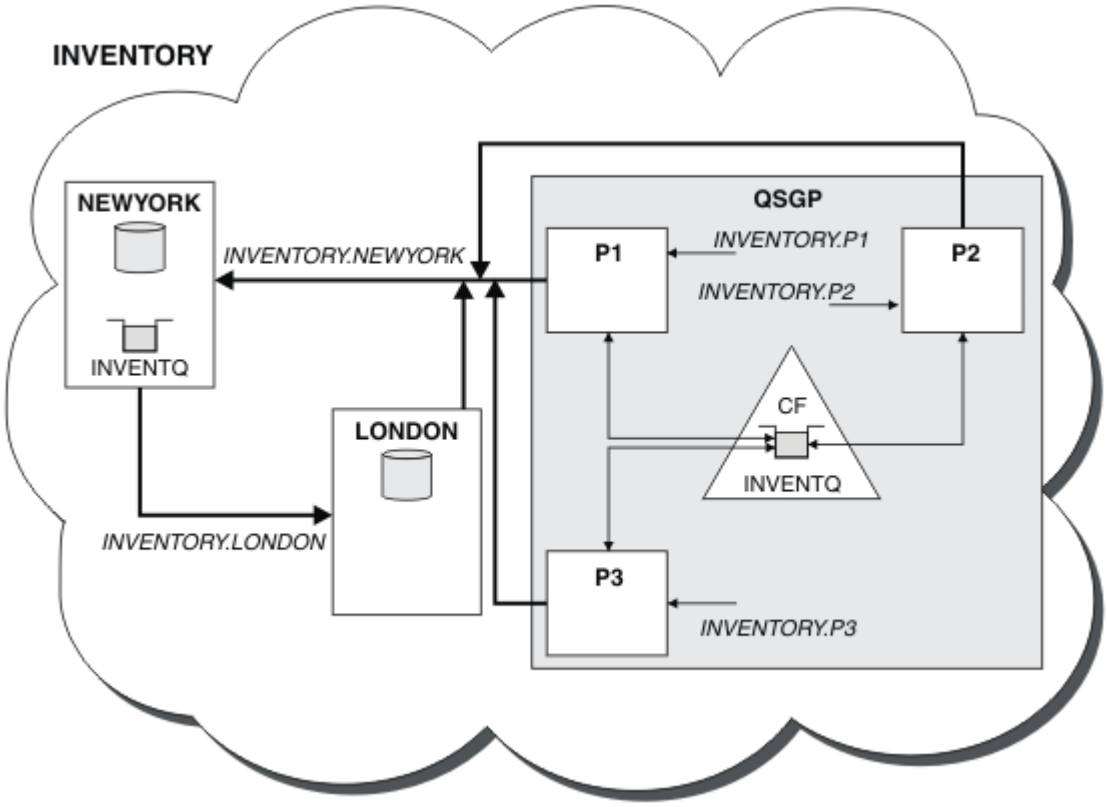


Figura 45. Gruppo di condivisione code e cluster

Ora i messaggi inseriti nella coda INVENTQ da LONDON vengono instradati alternativamente intorno ai quattro gestori code indicati come host della coda.

Operazioni successive

Un vantaggio di avere membri di un gruppo di condivisione code che ospitano una coda cluster è che qualsiasi membro del gruppo può rispondere a una richiesta. In questo caso, è possibile che P1 non sia disponibile dopo aver ricevuto un messaggio sulla coda condivisa. Un altro membro del gruppo di condivisione code può rispondere.

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 299.
- 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 definiti manualmente che puntano a LONDON su tutti i gestori code nel cluster con canali che puntano a NEWYORK o PARIS. Dopo aver eliminato un canale, immettere sempre il comando **start channel** in modo che il cluster possa utilizzare nuovamente i canali automatici. 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 46 a pagina 313 mostra il cluster impostato da questa attività.

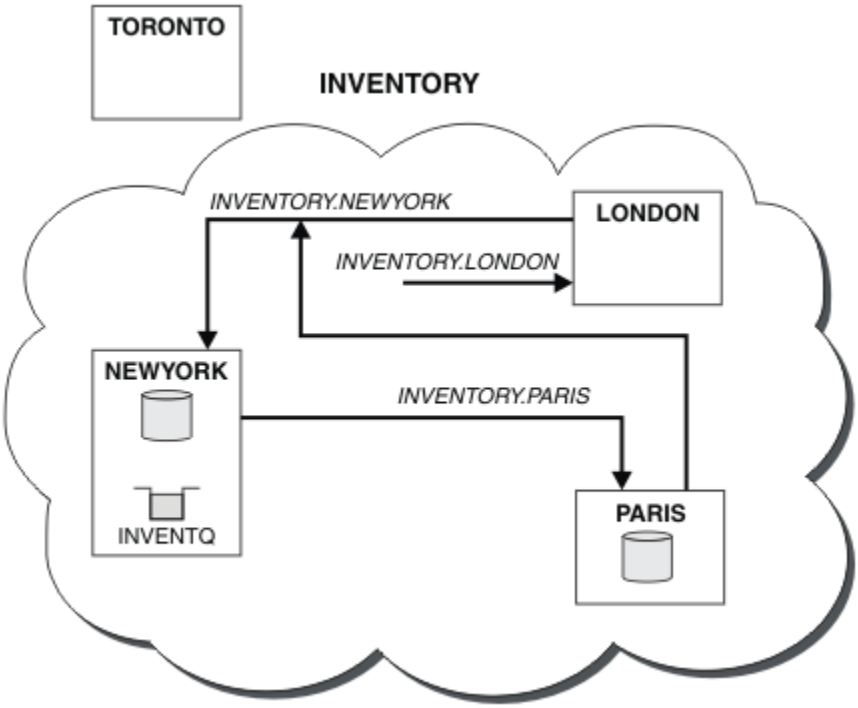


Figura 46. Il cluster INVENTORY con il repository completo è stato spostato in PARIS

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
- Windows 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 IBM MQ , il listener può essere avviato utilizzando il comando **START LISTENER** .

Multi Su sistemi 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`.

z/OS Una porta listener non condivisa (INDISP (QMGR)) deve essere utilizzata per canali CLUSRCVR su z/OS e per canali CLUSSDR su z/OS.

Procedura

1. Avviare l'iniziatore di canali.
   - z/OS Su z/OS, esiste un iniziatore di canali per ogni gestore code e viene eseguito come uno spazio di indirizzo separato. Avviarlo utilizzando il comando **MQSC** `START CHINIT` , che viene immesso come parte dell'avvio del gestore code.
   - ULW Su UNIX, Linux, and Windows, 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** .
   - IBM i Su IBM i, 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.
   - z/OS Su z/OS, utilizzare il programma listener del canale fornito da IBM MQ. Per avviare un listener del canale IBM MQ , utilizzare il **MQSC** comando `START LISTENER`, che viene emesso come parte dell'avvio dell'iniziatore del canale. Ad esempio:

     ```
     START LISTENER PORT(1414) TRPTYPE(TCP)
     ```

     oppure:

     ```
     START LISTENER LUNAME(LONDON.LUNAME) TRPTYPE(LU62)
     ```

     I membri di un gruppo di condivisione code possono utilizzare un listener condiviso invece di un listener per ogni gestore code. Non utilizzare listener condivisi con i cluster. In particolare, non rendere il `CONNAME` del canale `CLUSRCVR` l'indirizzo del listener condiviso del gruppo di condivisione code. In tal caso, i gestori code potrebbero ricevere messaggi per le code per le quali non dispongono di una definizione.
   - IBM i Su IBM i, utilizzare il programma listener del canale fornito da IBM MQ. Per avviare un listener del canale IBM MQ utilizzare il comando **CL** `STRMQMLSR`. Ad esempio:

     ```
     STRMQMLSR MQMNAME(QM1) PORT(1414)
     ```
   - Windows Su Windows, utilizzare il programma listener del canale fornito da IBM MQo le funzioni fornite dal sistema operativo.

     Per avviare il listener del canale IBM MQ utilizzare il comando `RUNMQLSR` . Ad esempio:

     ```
     RUNMQLSR -t tcp -p 1414 -m QM1
     ```
   - Linux UNIX Su UNIX and Linux, utilizzare il programma listener del canale fornito da IBM MQo le funzionalità fornite dal sistema operativo; ad esempio, **inetd** per le comunicazioni TCP.

     Per avviare il listener del canale IBM 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 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 IBM MQ .

Gli aggiornamenti diventano attivi dopo che **inetd** ha riletto i file di configurazione. Immettere i comandi riportati di seguito dall'ID utente root:

AIX Su AIX:

```
refresh -s inetd
```

Solaris Linux Su Solaris o Linux:

a. Individuare l'ID processo di **inetd** con il seguente comando:

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

b. Eseguire il comando appropriato.

Per Solaris 9 e Linux:

```
kill -1 inetd processid
```

Per Solaris 10 o versioni successive:

```
inetconv
```

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 287 tramite “Spostamento di un repository completo in un altro gestore code” a pagina 310 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 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 47 a pagina 316.

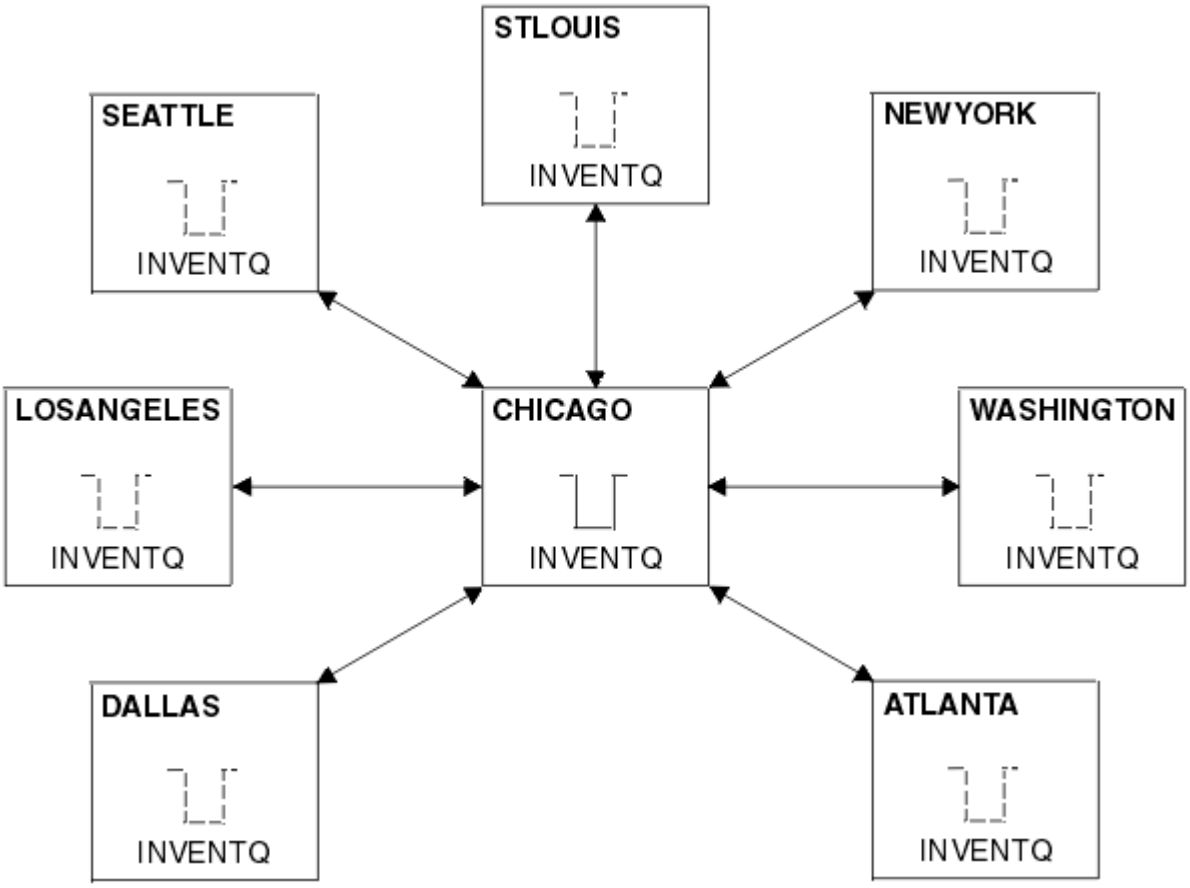


Figura 47. Una rete hub e spoke

- 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_name`* 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 393
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 IBM MQ è stato impostato come descritto in "Conversione di una rete esistente in un cluster" a pagina 315.
- 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 dei 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 è mostrato in Figura 48 a pagina 321.

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.

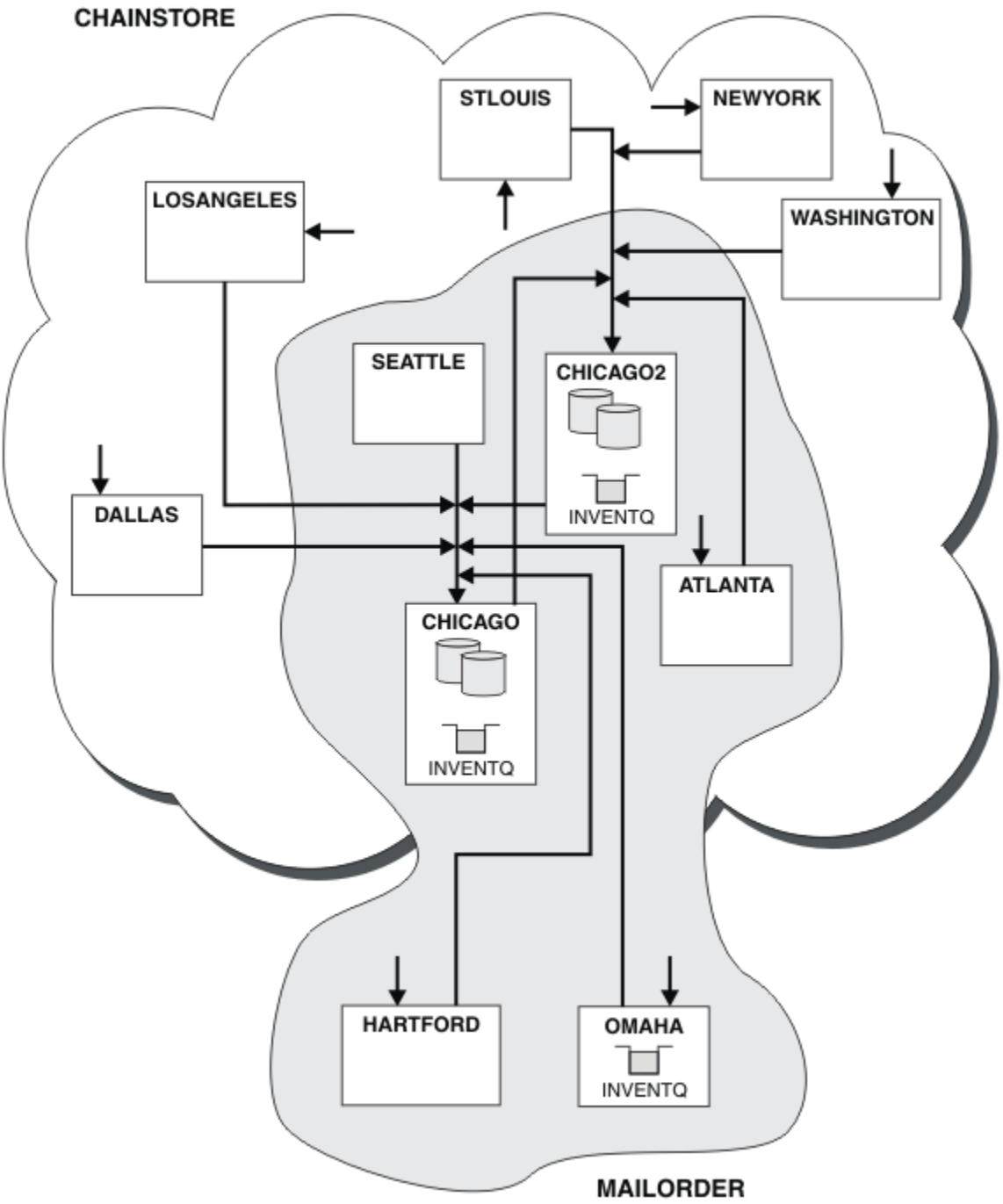


Figura 48. Cluster interconnessi

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.

Attività correlate

Rimozione di una rete cluster
Rimuovere un cluster da una rete e ripristinare la configurazione dell'accodamento distribuito.

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 MQ è stato configurato come descritto in “Conversione di una rete esistente in un cluster” a pagina 315.
- 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 351.

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.

Attività correlate

Aggiunta di un nuovo cluster interconnesso
Aggiungere un nuovo cluster che condivide alcuni gestori code con un cluster esistente.

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 49 a pagina 324. L'esempio è descritto in Cluster: isolamento dell'applicazione utilizzando più code di trasmissione cluster.

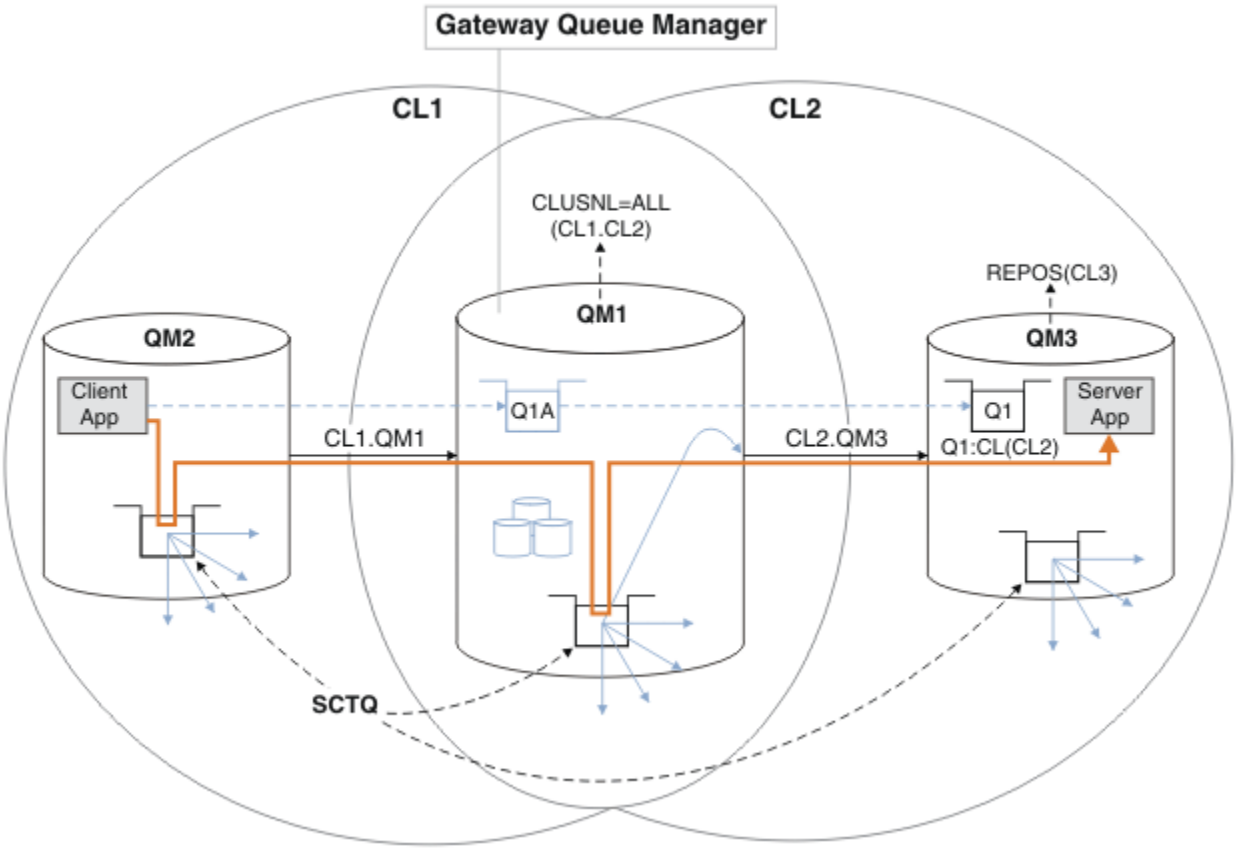


Figura 49. Applicazione client-server distribuita all'architettura hub e spoke utilizzando i cluster IBM MQ

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 Cluster: Pianificazione della configurazione delle code di trasmissione cluster.

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 QM n
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 QM n
DEFINE LISTENER(TCP141 n) TRPTYPE(TCP) IPADDR(hostname) PORT(141 n) CONTROL(QMGR) REPLACE
START LISTENER(TCP141 n)
```

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 seguenti comandi su QM2, QM3, QM4 e QM5, dove *c*, *ne* *m* assumono i valori mostrati in Tabella 27 a pagina 325 per ciascun gestore code:

Tabella 27. 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 QM m
DEFINE CHANNEL(CL c.QM n) CHLTYPE(CLUSSDR) CONNAME('localhost(141 n)') CLUSTER(CL c) REPLACE
DEFINE CHANNEL(CL c.QM m) CHLTYPE(CLUSRCVR) CONNAME('localhost(141 m)') CLUSTER(CL c) REPLACE
```

6. 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.

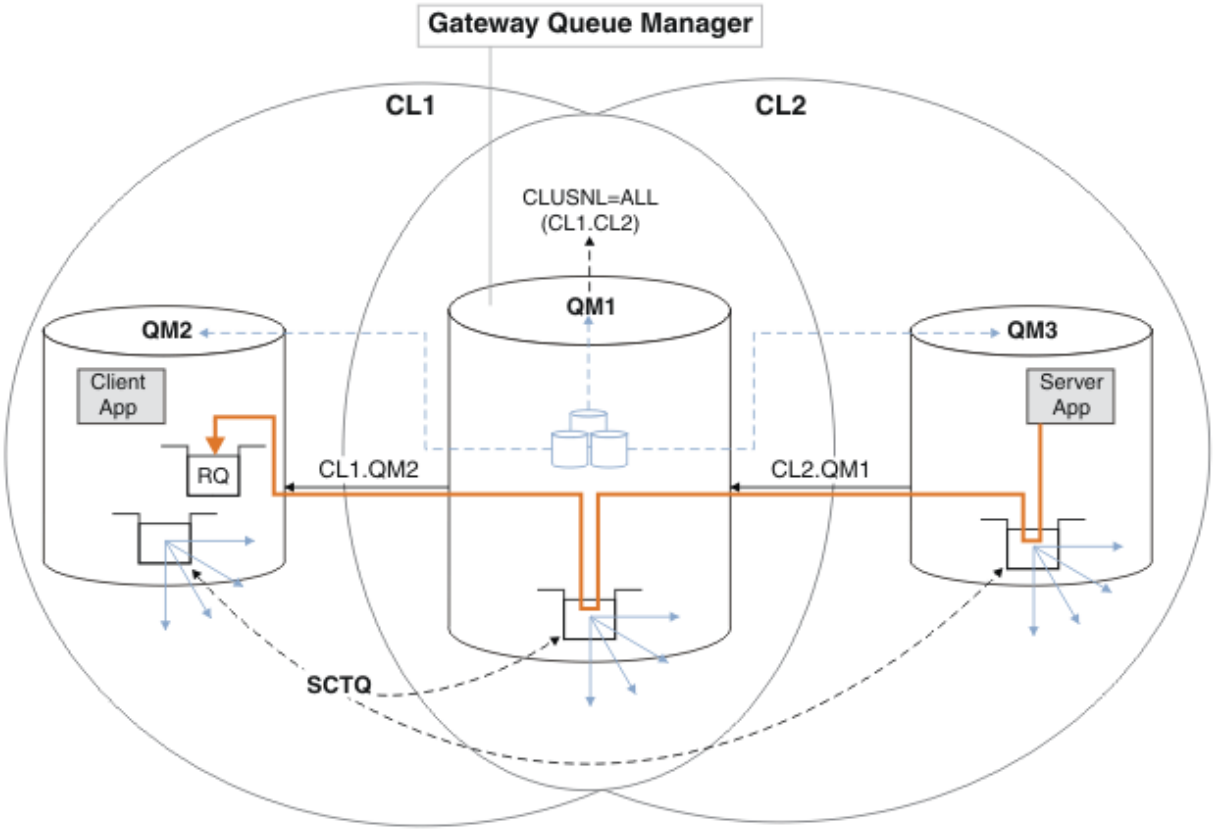


Figura 50. Utilizzo di un alias del gestore code per restituire il messaggio di risposta a un cluster differente

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: IBM 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

Attività correlate

Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster

Clustering: pianificazione della configurazione delle code di trasmissione del cluster

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 301

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 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

Crea i cluster di sovrapposizione mostrati nell' applicazione client - server distribuita all'architettura hub e spoke utilizzando i cluster IBM MQ in “Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 324 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 del 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 51 a pagina 329, 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 331. È inoltre necessario gestire la commutazione da una coda di trasmissione all'altra.

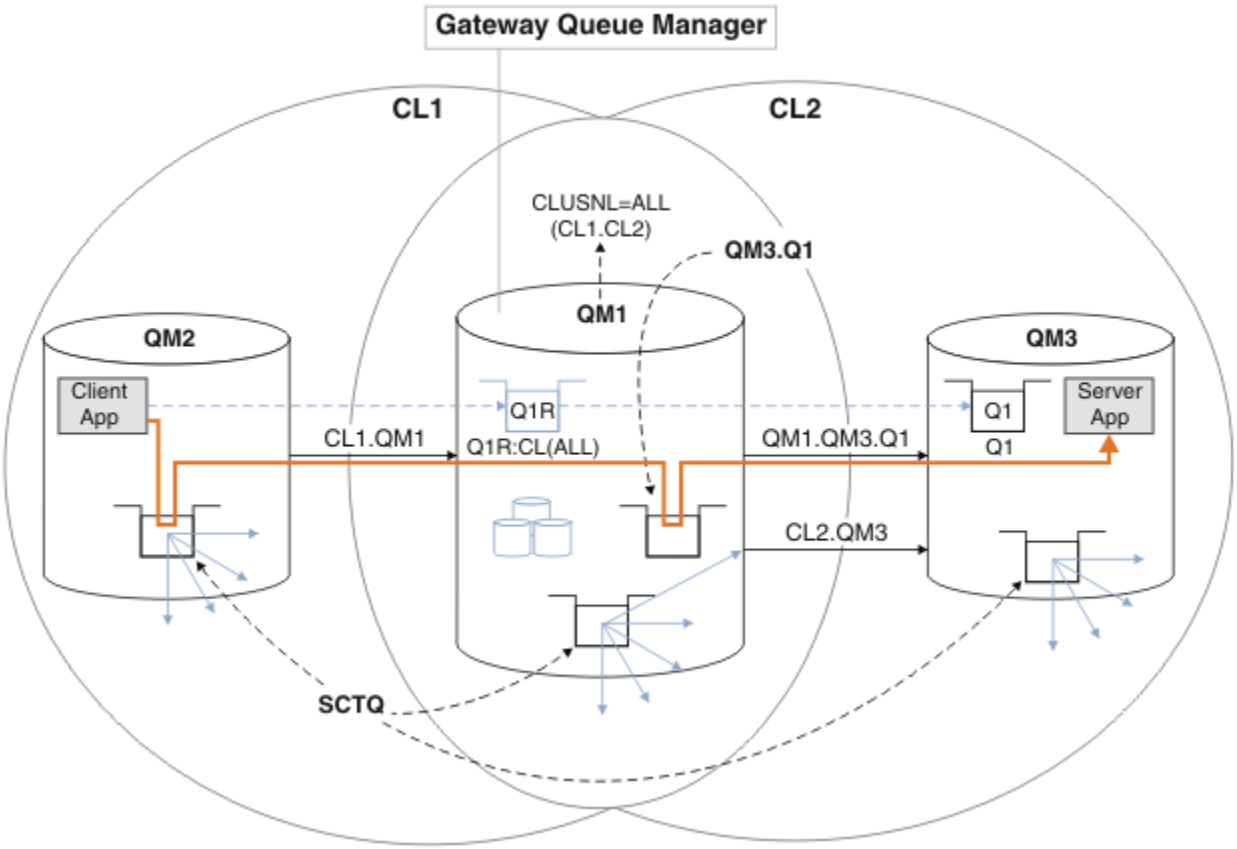


Figura 51. Applicazione client-server distribuita all'architettura del cluster hub e spoke utilizzando definizioni di coda remota

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

Attività correlate

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.

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.

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.

Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster

Clustering: pianificazione della configurazione delle code di trasmissione del cluster

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 301
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

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 IBM WebSphere MQ 7.5o versione successiva.
2. Crea i cluster di sovrapposizione mostrati nell' applicazione client - server distribuita all'architettura hub e spoke utilizzando i cluster IBM MQ in “Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 324 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 52 a pagina 332.

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 328:

- 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 52 a pagina 332 non risulta in un isolamento del traffico così grande come 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 328. 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 52 a pagina 332 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 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 334.

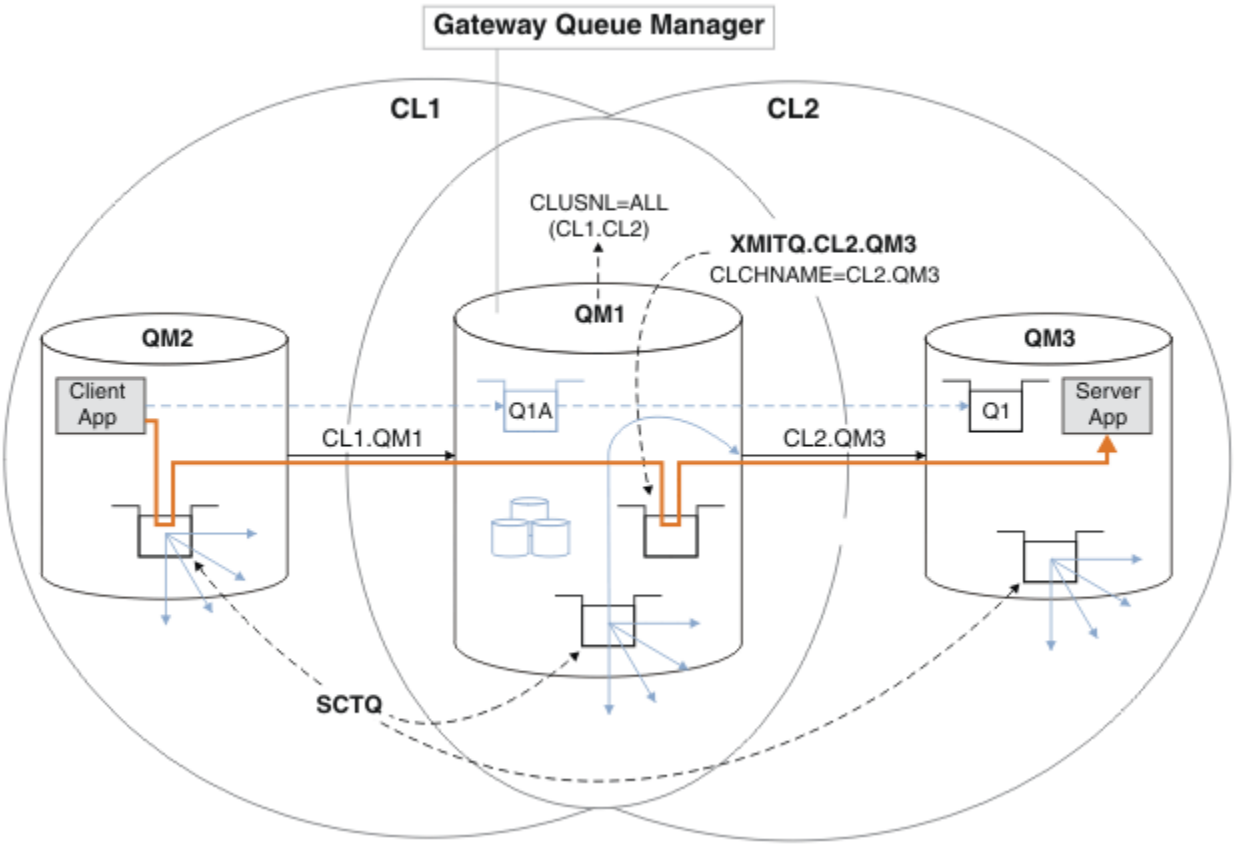


Figura 52. Applicazione client-server distribuita all'architettura hub e spoke utilizzando una coda di trasmissione cluster aggiuntiva.

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 IBM 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 IBM 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

“Utilizzo delle code di trasmissione del cluster e dei canali mittente del cluster” a pagina 281
I messaggi tra i gestori code con cluster vengono memorizzati nelle code di trasmissione cluster e inoltrati dai canali mittenti del cluster. 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. L'elaborazione di questo switch è automatizzata e transazionale.

Attività correlate

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.

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.

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.

Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster

Clustering: pianificazione della configurazione delle code di trasmissione del cluster

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 301
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 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 52 a pagina 332.

1. Il gestore code del gateway deve essere su IBM WebSphere MQ 7.5o versione successiva.
2. Crea i cluster di sovrapposizione mostrati nell' applicazione client - server distribuita all'architettura hub e spoke utilizzando i cluster IBM MQ in “Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 324 seguendo i passi in tale attività.

3. Eseguire i passi in Figura 52 a pagina 332 in “Aggiunta di una coda di trasmissione cluster per isolare il traffico di messaggi cluster inviati da un gestore code gateway” a pagina 331 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 331 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 331 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 53 a pagina 336. 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 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 331 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.

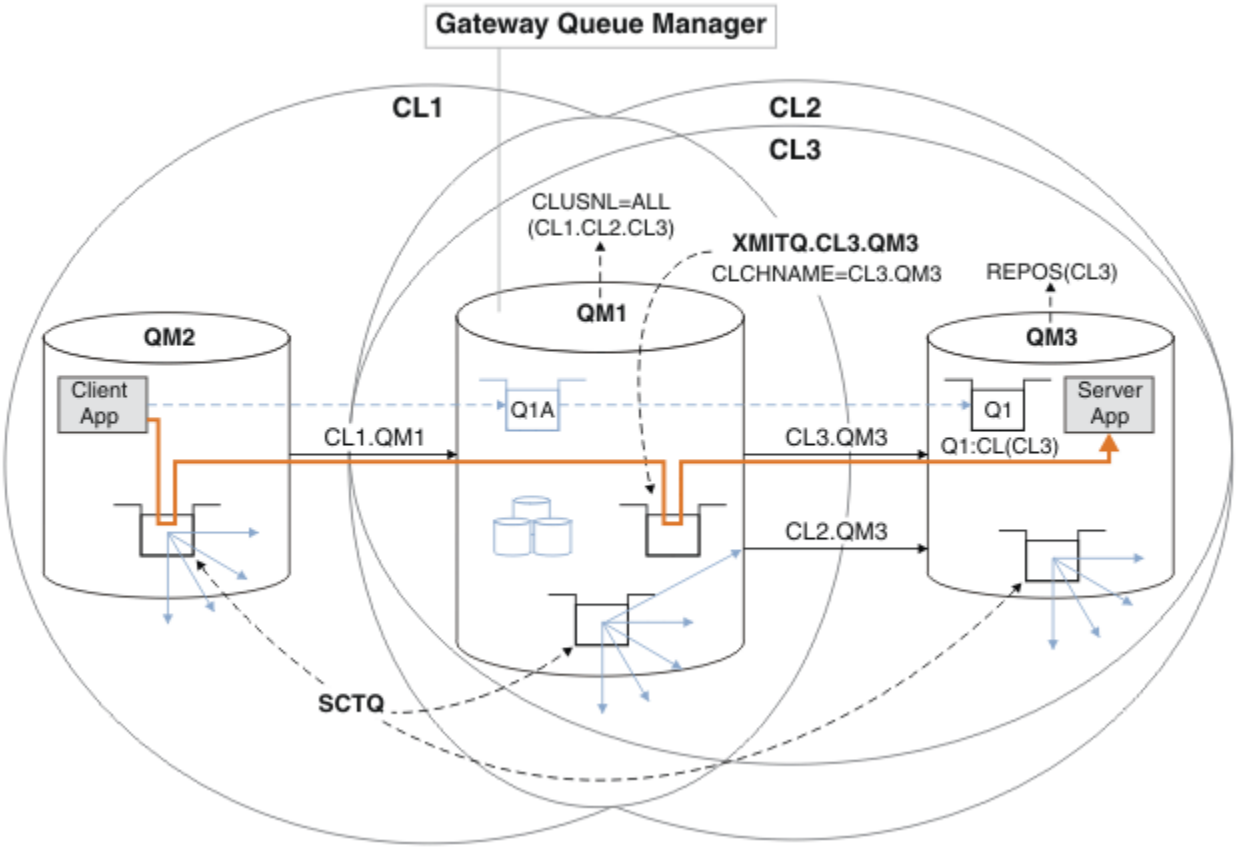


Figura 53. Utilizzo di un ulteriore cluster per separare il traffico di messaggi nel gestore code del gateway che va a una delle diverse code del cluster sullo stesso gestore code

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 MQ trasferisce automaticamente i messaggi da XMITQ.CL2.QM3 alla 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 IBM 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 IBM 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

“Utilizzo delle code di trasmissione del cluster e dei canali mittente del cluster” a pagina 281

I messaggi tra i gestori code con cluster vengono memorizzati nelle code di trasmissione cluster e inoltrati dai canali mittenti del cluster. 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. L'elaborazione di questo switch è automatizzata e transazionale.

Attività correlate

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.

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.

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.

Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster

Clustering: pianificazione della configurazione delle code di trasmissione del cluster

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 301

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.

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 IBM WebSphere MQ 7.5o versione successiva.
2. Crea i cluster di sovrapposizione mostrati nell' applicazione client - server distribuita all'architettura hub e spoke utilizzando i cluster IBM MQ in “Creazione di cluster a due sovrapposizioni con un gestore code del gateway” a pagina 324 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 IBM WebSphere MQ 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 54 a pagina 341. 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 301.

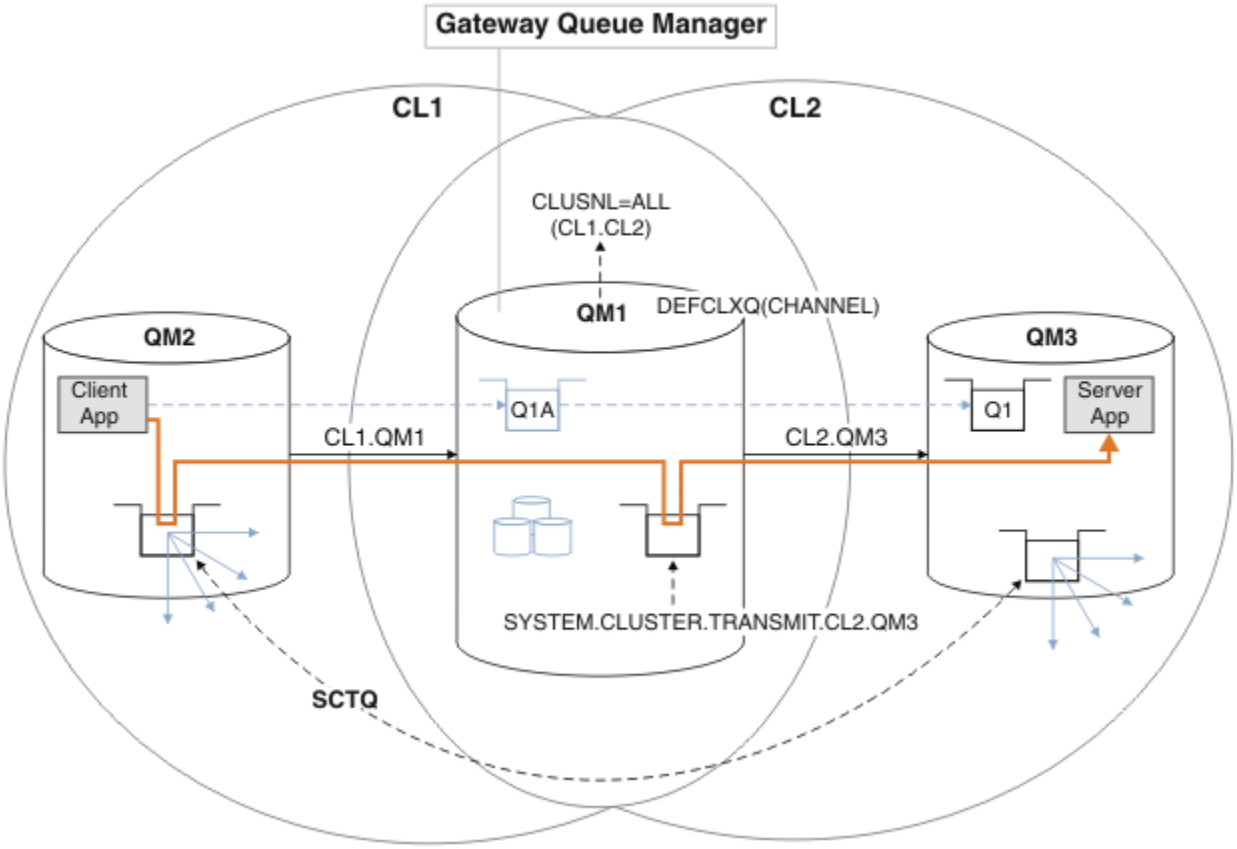


Figura 54. Applicazione client-server distribuita all'architettura hub e spoke con code di trasmissione cluster separate sul gestore code del gateway.

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 IBM 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 IBM 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

Attività correlate

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.

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.

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.

Clustering: isolamento dell'applicazione utilizzando più code di trasmissione cluster

Clustering: pianificazione della configurazione delle code di trasmissione del cluster

“Aggiunta di un gestore code a un cluster: code di trasmissione separate” a pagina 301
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.

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 306. 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, SALESQe 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)
```

Rimozione di un gestore code da un cluster: procedura ottimale

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 349.

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 299e modificato come descritto in “Rimozione di una coda cluster da un gestore code” a pagina 345.

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. Prima di rimuovere il gestore code dal cluster, verificare che il gestore code non ospiti più le risorse richieste dal cluster:
   - Se il gestore code ospita un repository completo, completare i passi da 1 a 6 da “Spostamento di un repository completo in un altro gestore code” a pagina 310. Se la funzionalità del repository completo del gestore code da rimuovere non deve essere spostata in un altro gestore code, è necessario solo completare i passi 5 e 6.
   - 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 345.

- Se il gestore code ospita argomenti cluster, eliminare gli argomenti (ad esempio utilizzando il comando DELETE TOPIC) o spostarli su altri host come descritto in “Spostamento di una definizione di argomento del raggruppamento in un gestore code differente” a pagina 404.

  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.

2. Modificare i canali riceventi del cluster definiti manualmente per rimuoverli dal cluster, sul gestore code LONDON:

```
ALTER CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) CLUSTER(' ')
```

3. 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.

4. 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.PARIS) 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)
```

Se per questo canale era in uso una coda di trasmissione definita manualmente e il pattern CLCHNAME non corrisponde ad altri canali esistenti o pianificati, è possibile eliminare la coda di trasmissione. Ad esempio:

```
DELETE QLOCAL(PARIS.CUSTOM.XMITQ)
```

Nota: Se le code di trasmissione definite automaticamente o il SYSTEM.CLUSTER.TRANSMIT.QUEUE è in uso, questo passo non è richiesto.

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 299. 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 351.

Attività correlate

Rimozione di un gestore code da un cluster (utilizzando IBM MQ Explorer)

Riferimenti correlati

ALTER CHANNEL (modifica impostazioni canale)

DISPLAY CHANNEL (visualizzazione definizione canale)

DISPLAY CHSTATUS (visualizzazione stato canale)

DISPLAY CLUSQMGR (visualizza informazioni sul canale per gestori code cluster)

STOP CHANNEL (arresta canale)

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: procedura ottimale” a pagina 347.

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 299e modificato come descritto in “Rimozione di una coda cluster da un gestore code” a pagina 345.

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. Prima di rimuovere il gestore code dal cluster, verificare che il gestore code non ospiti più le risorse richieste dal cluster:
   - Se il gestore code ospita un repository completo, completare i passi da 1 a 6 da "Spostamento di un repository completo in un altro gestore code" a pagina 310. Se la funzionalità del repository completo del gestore code da rimuovere non deve essere spostata in un altro gestore code, è necessario solo completare i passi 5 e 6.
   - 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 345.
   - Se il gestore code ospita argomenti cluster, eliminare gli argomenti (ad esempio utilizzando il comando DELETE TOPIC) o spostarli su altri host come descritto in "Spostamento di una definizione di argomento del raggruppamento in un gestore code differente" a pagina 404.

     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.
2. 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)
   ```
3. 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.
4. Eliminare i canali cluster definiti manualmente, sul gestore code LONDON:

   ```
   DELETE CHANNEL(INVENTORY.NEWYORK)
   DELETE CHANNEL(INVENTORY.TORONTO)
   ```
5. 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 299. 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 351.

Riferimenti correlati

DELETE CHANNEL (elimina un canale)
DISPLAY CHANNEL (visualizzazione definizione canale)
DISPLAY CHSTATUS (visualizzazione stato canale)
DISPLAY CLUSQMGR (visualizza informazioni sul canale per gestori code cluster)
STOP CHANNEL (arresta canale)
RESET CLUSTER (ripristino di un cluster)

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.

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: procedura ottimale" a pagina 347. 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

Componenti cluster

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.

IBM 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. z/OS Su z/OS, impostare INDXTYPE di una coda di trasmissione cluster su CORRELID.

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 della coda di trasmissione del cluster sia memorizzato su z/OS (ad esempio, z/OS serie di pagine) non diventi pieno.

Informazioni su questa attività

z/OS

La seguente procedura è applicabile solo a z/OS.

Procedura

Impostare INDXTYPE della coda di trasmissione cluster su CORRELID

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 ottimali di REFRESH CLUSTER.

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 MQ garantisce che non si perda alcun dato dalle code.

Informazioni correlate

Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER

Ripristino di un gestore code cluster

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 aggiornamenti sullo 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.

Informazioni correlate

Cluster: utilizzo delle procedure consigliate per REFRESH CLUSTER

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.

  z/OS **SUIBM MQ for z/OS**

  Controllare il problema dell'estremità ricevente del cluster del canale rimanente attivo utilizzando i parametri ADOPTMCA e ADOPTCHK su ALTER QMGR.

  Multi **SUMultipiattaforme**

  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 .

Verifica che i comandi asincroni per le reti distribuite siano terminati

Molti comandi sono asincroni quando utilizzati in una rete distribuita. A seconda del comando e dello stato della rete quando viene emesso, il completamento può richiedere una quantità di tempo

significativa. Il gestore code non emette un messaggio al completamento, quindi sono necessari altri modi per controllare che il comando sia terminato.

Informazioni su questa attività

È probabile che quasi tutte le modifiche di configurazione apportate a un cluster vengano completate in modo asincrono. Ciò è dovuto ai cicli di gestione e aggiornamento interni che operano all'interno dei cluster. Per le gerarchie di pubblicazione / sottoscrizione, è probabile che qualsiasi modifica di configurazione che influisca sulle sottoscrizioni venga completata in modo asincrono. Questo non è sempre ovvio dal nome del comando.

I seguenti comandi MQSC potrebbero essere tutti completati in modo asincrono. Ognuno di questi comandi ha un equivalente PCF e la maggior parte è disponibile anche da IBM MQ Explorer . Quando vengono eseguiti su una rete di piccole dimensioni senza alcun carico di lavoro, questi comandi generalmente vengono completati in pochi secondi. Tuttavia, questo non vale per le reti più grandi e più affollate. Inoltre, il comando **REFRESH CLUSTER** potrebbe richiedere molto più tempo, in particolare quando viene emesso su più gestori code contemporaneamente.

Per avere la certezza che questi comandi siano terminati, verificare che gli oggetti previsti esistano sui gestori code remoti.

Procedura

- ALTER DRG

  Per il comando ALTER QMGR PARENT , utilizzare `DISPLAY PUBSUB TYPE(PARENT) ALL` per tracciare lo stato della relazione principale richiesta.

  Per i comandi ALTER QMGR REPOS e ALTER QMGR REPOSNL , utilizzare `DISPLAY CLUSQMGR QMTYPE` per confermare il completamento.

- DEFINE CHANNEL, ALTER CHANNELe DELETE CHANNEL

  Per tutti i parametri elencati nella tabella Parametri ALTER CHANNEL, utilizzare il comando `DISPLAY CLUSQMGR` per monitorare quando le modifiche sono state propagate al cluster.

- DEFINE NAMELIST, ALTER NAMELISTe DELETE NAMELIST.

  Se si utilizza un **NAMELIST** sull'attributo **CLUSNL** di un oggetto **QMgr** , una coda o un canale cluster potrebbero influire su tale oggetto. Monitorare come appropriato per l'oggetto interessato.

  Le modifiche a `SYSTEM.QPUBSUB.QUEUE.NAMELIST` potrebbero influire sulla creazione o l'annullamento delle sottoscrizioni proxy in una gerarchia di pubblicazione / sottoscrizione. Utilizzare il comando `DISPLAY SUB SUBTYPE(PROXY)` per monitorarlo.

- DEFINE queues, ALTER queuese DELETE queues.

  Per tutti i parametri elencati nella tabella Parametri che possono essere restituiti dal comando DISPLAY QUEUE, utilizzare il comando `DISPLAY QCLUSTER` per monitorare quando le modifiche sono state propagate al cluster.

- DEFINE SUBe DELETE SUB

  Quando si definisce la prima sottoscrizione su una stringa argomento, è possibile creare sottoscrizioni proxy in una gerarchia di pubblicazione / sottoscrizione o in un cluster di pubblicazione / sottoscrizione. Allo stesso modo, quando si elimina l'ultima sottoscrizione su una stringa di argomenti, è possibile annullare le sottoscrizioni proxy in una gerarchia di pubblicazione / sottoscrizione o in un cluster di pubblicazione / sottoscrizione.

  Per verificare che un comando che definisce o elimina una sottoscrizione sia terminato, verificare se la sottoscrizione proxy prevista esiste o meno su altri gestori code nella rete distribuita. Se si sta utilizzando l' *instradamento diretto* in un cluster, verificare che la sottoscrizione proxy prevista esista sugli altri repository parziali nel cluster. Se si sta utilizzando l' *instradamento dell'host argomento* in

un cluster, verificare che la sottoscrizione proxy prevista esista sugli host argomento corrispondenti. Utilizzare il seguente comando MQSC:

```
DISPLAY SUB(*) SUBTYPE(PROXY)
```

Utilizzare lo stesso controllo per le seguenti chiamate MQI di sottoscrizione e annullamento sottoscrizione equivalenti, quando vengono emesse in un cluster o gerarchia:

- Sottoscrivere utilizzando MQSUB.
- Annullare la sottoscrizione utilizzando MQCLOSE con MQCO_REMOVE_SUB.

- DEFINE TOPIC, ALTER TOPICe DELETE TOPIC

  Per verificare che un comando che definisce, modifica o elimina un argomento del cluster sia terminato, visualizzare l'argomento negli altri repository parziali nel cluster (se si utilizza l' *instradamento diretto*) o su altri host argomento (se si utilizza l' *instradamento host argomento*).

  Per tutti i parametri elencati nella tabella Parametri che possono essere restituiti dal comando DISPLAY TOPIC, utilizzare il comando `DISPLAY TCLUSTER` per monitorare quando le modifiche sono state propagate al cluster.

  Nota:

  - Il parametro **CLUSTER** può influenzare la creazione o l'annullamento delle sottoscrizioni proxy in un cluster di pubblicazione / sottoscrizione.
  - I parametri **PROXYSUB** e **SUBSCOPE** possono influenzare la creazione o l'annullamento delle sottoscrizioni proxy in una gerarchia di pubblicazione / sottoscrizione o in un cluster di pubblicazione / sottoscrizione.
  - Utilizzare il comando `DISPLAY SUB SUBTYPE(PROXYSUB)` per monitorarlo.

- Aggiornamento cluster

  Se si sta eseguendo il comando **REFRESH CLUSTER** , eseguire il polling della profondità della coda comandi del cluster. Attendere che raggiunga lo zero, e rimanere a zero, prima di ricercare gli oggetti.

  1. Utilizzare il comando MQSC riportato di seguito per controllare che la profondità della coda comandi del cluster sia zero.

     ```
     DISPLAY QL(SYSTEM.CLUSTER.COMMAND.QUEUE) CURDEPTH
     ```

  2. Ripetere il controllo fino a quando la profondità della coda non raggiunge lo zero e rimane a zero nel successivo controllo.

  Il comando **REFRESH CLUSTER** rimuove e ricrea oggetti e, in configurazioni di grandi dimensioni, può richiedere molto tempo per il completamento. Consultare Considerazioni su REFRESH CLUSTER per i cluster di pubblicazione/sottoscrizione.

- AGGIORNA QMGR TYPE (PROXYSUB)

  Per verificare che il comando **REFRESH QMGR TYPE(PROXYSUB)** sia terminato, verificare che le sottoscrizioni proxy siano state corrette su altri gestori code nella rete distribuita. Se si sta utilizzando l' *instradamento diretto* in un cluster, verificare che le sottoscrizioni proxy siano state corrette sugli altri repository parziali nel cluster. Se si sta utilizzando l' *instradamento host argomento* in un cluster, verificare che le sottoscrizioni proxy previste siano state corrette sugli host argomento corrispondenti. Utilizzare il seguente comando MQSC:

  ```
  DISPLAY SUB(*) SUBTYPE(PROXYSUB)
  ```

- Reimposta cluster

  Per controllare che il comando **RESET CLUSTER** è stato completato, utilizzare `DISPLAY CLUSQMGR`.

- RESET QMGR TYPE (PUBSUB)

Per controllare che il comando **RESET QMGR** è stato completato, utilizzare `DISPLAY PUBSUB TYPE(PARENT|CHILD)`.

Nota: Il comando **RESET QMGR** potrebbe causare l'annullamento delle sottoscrizioni proxy in una gerarchia di pubblicazione / sottoscrizione o in un cluster di pubblicazione / sottoscrizione. Utilizzare il comando `DISPLAY SUB SUBTYPE(PROXYSUB)` per monitorarlo.

- Si potrebbe anche voler monitorare altre code di sistema che, man mano che i comandi vengono completati, tendono ad una profondità di coda pari a zero.

  Ad esempio, si potrebbe voler monitorare la coda `SYSTEM.INTER.QMGR.CONTROL` e la coda `SYSTEM.INTER.QMGR.FANREQ` . Vedi Monitoraggio del traffico di sottoscrizioni proxy nei cluster e Bilanciamento dei produttori e dei consumatori nelle reti di pubblicazione / sottoscrizione.

Operazioni successive

Se questi controlli non confermano che un comando asincrono è terminato, è possibile che si sia verificato un errore. Per esaminare, controllare prima il log del gestore code su cui è stato emesso il comando, quindi (per un cluster) controllare i log del repository completo del cluster.

Riferimenti correlati

z/OS Comportamento asincrono dei comandi CLUSTER su z/OS

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

Confronto tra cluster e accodamento distribuito

Componenti di un cluster

“Cluster e alias del gestore code” a pagina 371
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 375
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 374
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 275
I cluster forniscono un meccanismo per l'interconnessione dei gestori code in modo da semplificare sia la configurazione iniziale che la gestione in corso. È possibile definire componenti cluster e creare e gestire cluster.

“Configurazione di un nuovo cluster” a pagina 287
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 55 a pagina 359 mostra un gestore code denominato QM3 esterno al cluster denominato DEMO. QM3 potrebbe essere un gestore code su un prodotto IBM 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)
```

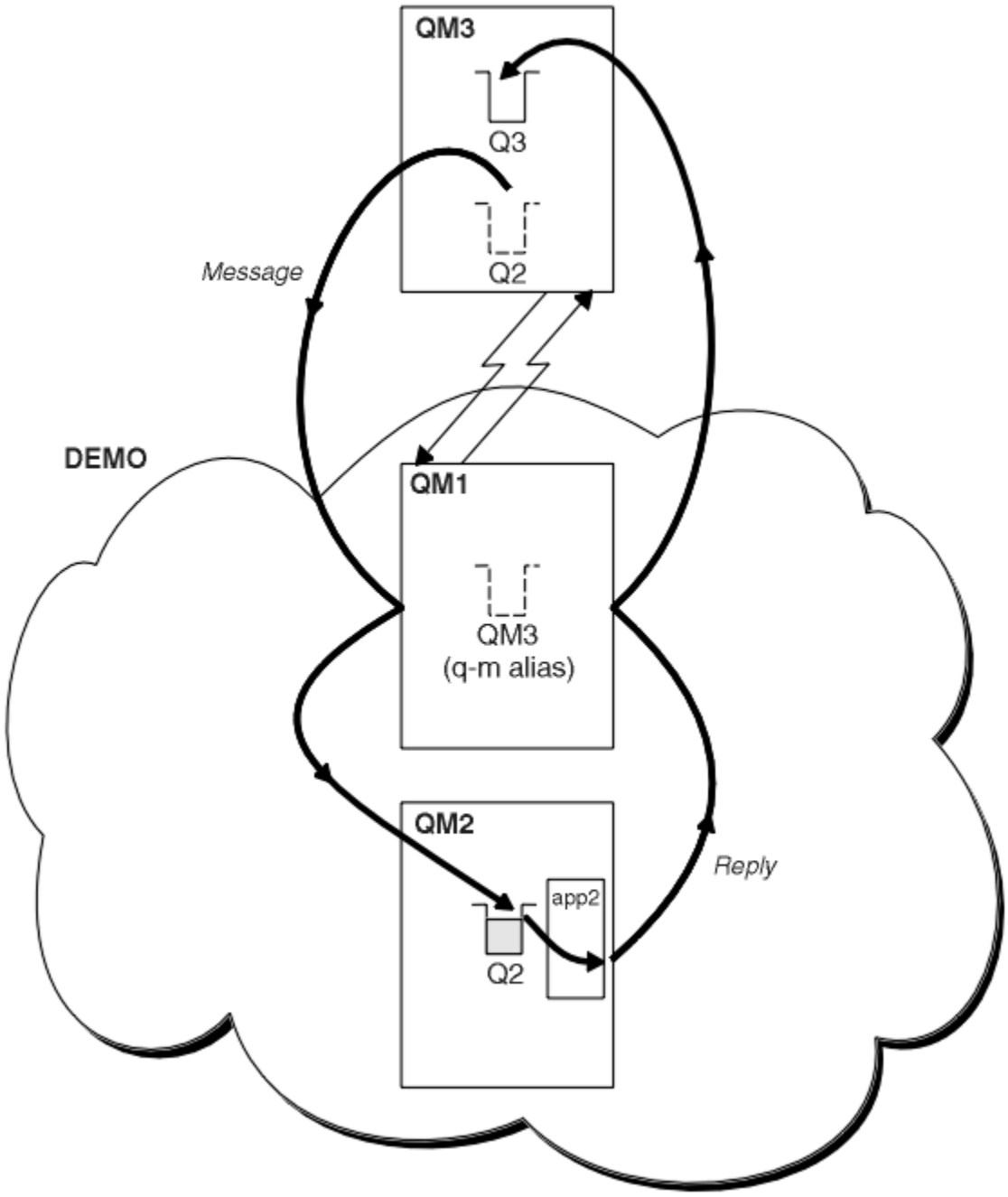


Figura 55. Inserimento da un gestore code esterno al cluster

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 55 a pagina 359.

   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. IBM 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.

Concetti correlati

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.

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.

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.

Attività correlate

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.

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.

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.

“Nascondere il nome di un gestore code di destinazione cluster” a pagina 362

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 362 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 358, per nascondere il nome del gestore code di destinazione all'interno del cluster.

Procedura

Nell'esempio, consultare Figura 56 a pagina 363, definire un alias del gestore code sul gestore code del gateway QM1 denominato DEMO:

```
DEFINE QREMOTE(DEMO) RNAME(' ') RQMNAME(' ')
```

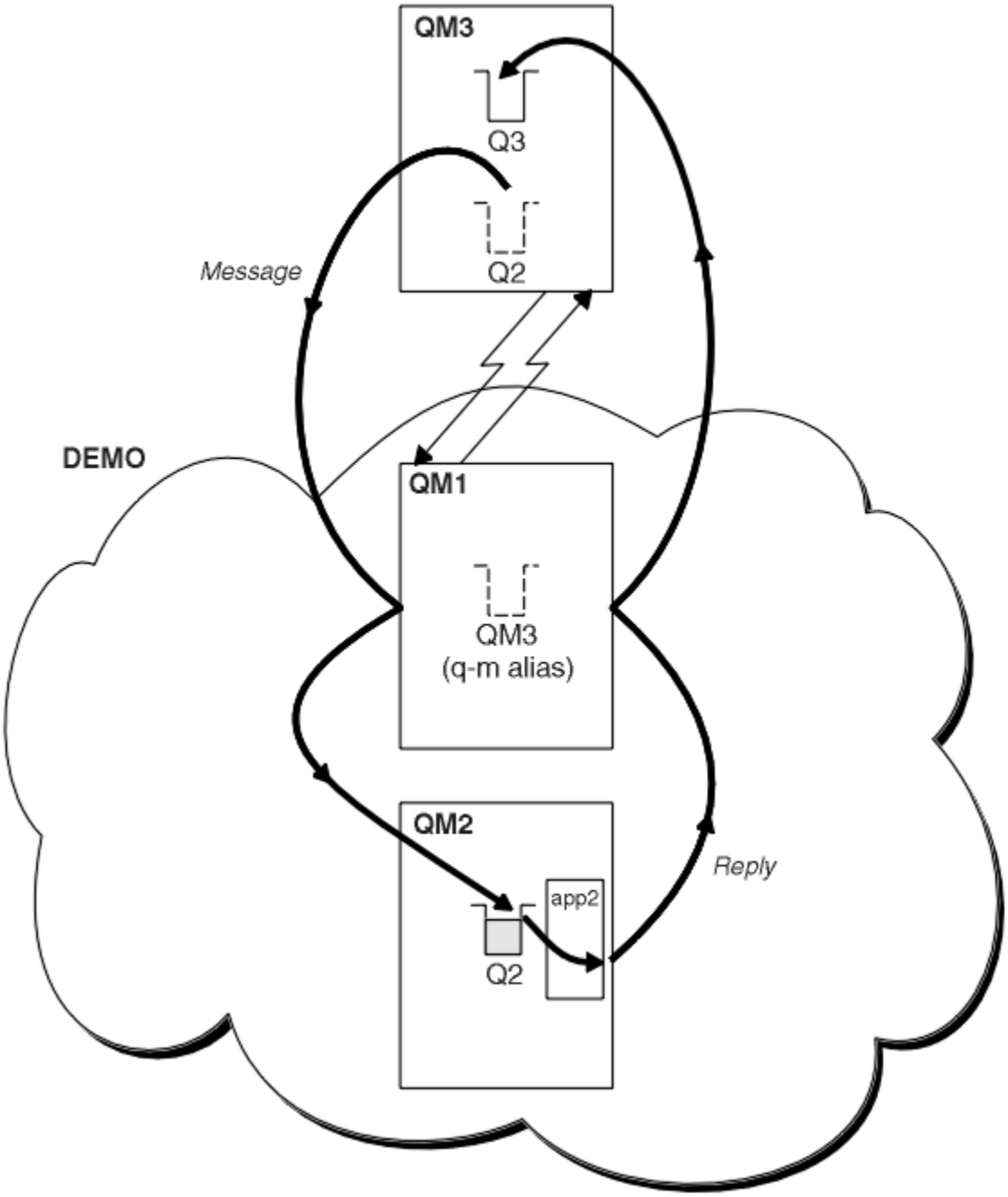


Figura 56. Inserimento da un gestore code esterno al cluster

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) XMIT(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 57 a pagina 365 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.

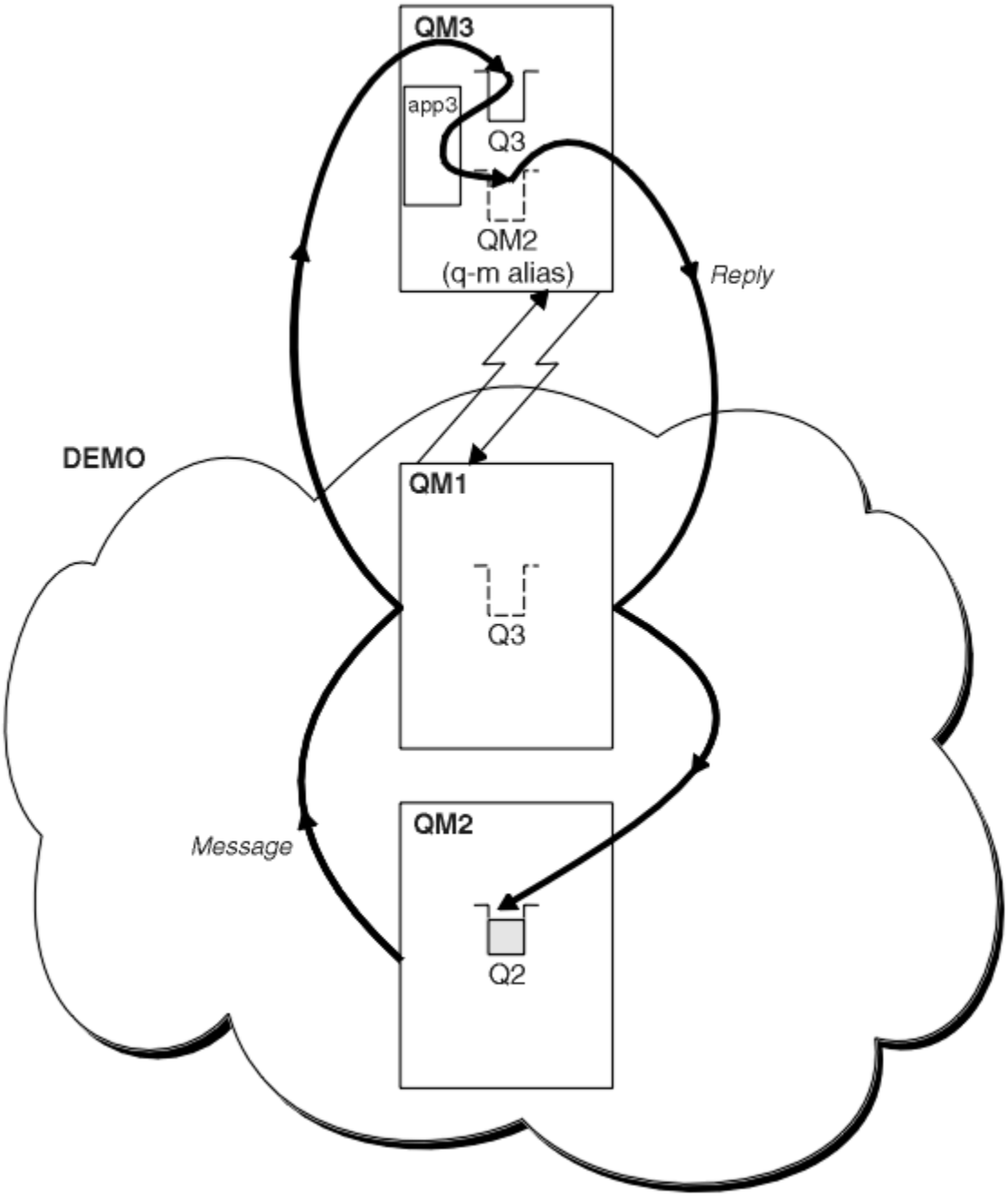


Figura 57. Inserimento in un gestore code all'esterno del cluster

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 57 a pagina 365.

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 anche specificare il nome della coda di trasmissione al gestore code 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.

Concetti correlati

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.

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.

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.

Attività correlate

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.

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.

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.

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 55 a pagina 359 in “Configurazione della richiesta/risposta a un cluster” a pagina 358.

Informazioni su questa attività

In questo scenario, il gestore code all'esterno del cluster, QM3 in Figura 58 a pagina 368, invia richieste alla coda Q2. Q2 è ospitato su due gestori code, QM2 e QM4 all'interno del cluster DEMO. Entrambi i gestori code sono configurati con un'opzione di bind predefinita NOTFIXED per utilizzare il bilanciamento del carico di lavoro. Le richieste provenienti da QM3, il gestore code esterno al cluster, vengono inviate a un'istanza di Q2 tramite QM1.

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 58 a pagina 368.

La procedura estende l'esempio in Figura 55 a pagina 359 in “Configurazione della richiesta/risposta a un cluster” a pagina 358.

Procedura

1. 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.
2. Creare un alias del gestore code Q3 su QM1.

   ```
   DEFINE QREMOTE(Q3) RNAME(' ') RQMNAME(' ')
   ```

   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, ' '
3. Definire una coda locale denominata Q2 su ciascuno di QM2 e QM4.

   ```
   DEFINE QLOCAL(Q2) CLUSTER(DEMO) DEFBIND(NOTFIXED)
   ```
4. QM1, il gestore code del gateway, non ha definizioni speciali.

Risultati

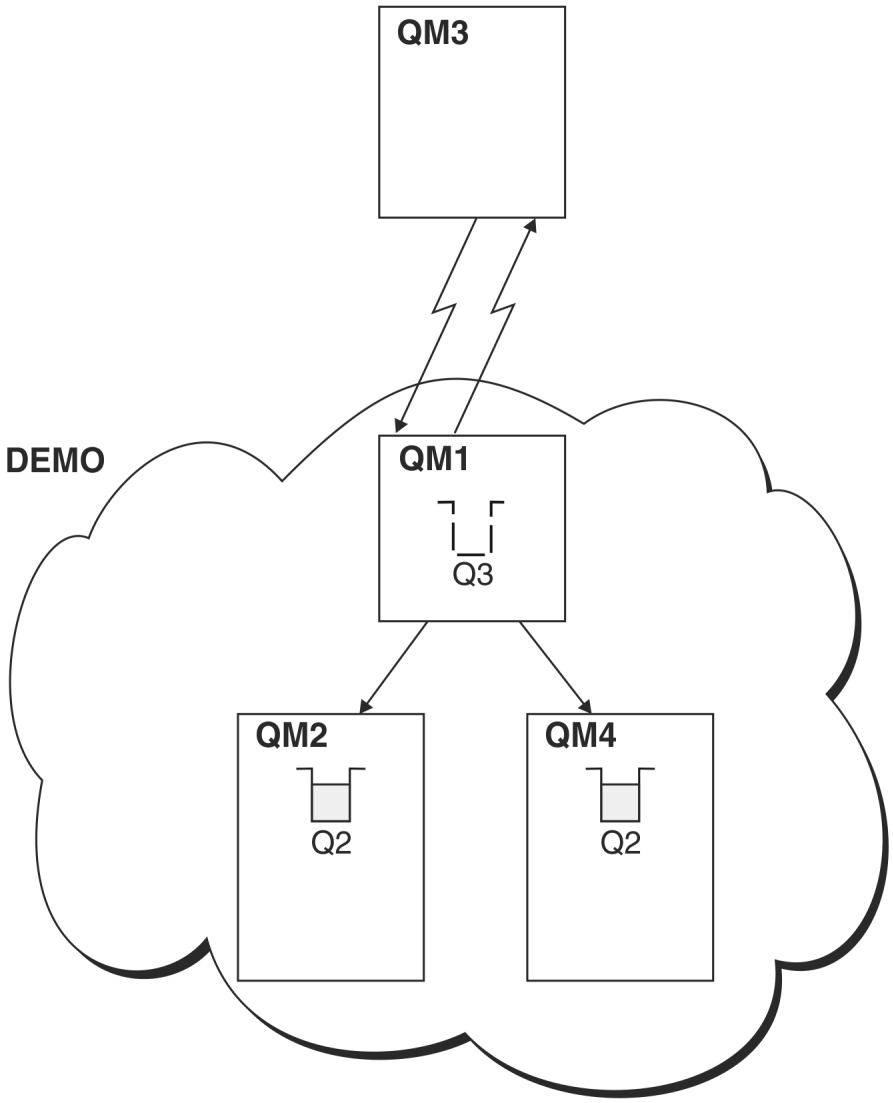


Figura 58. Inserimento da un gestore code esterno al cluster

Quando un'applicazione in QM3 emette una chiamata MQPUT per inserire un messaggio in Q2, la QREMOTE definizione in QM3 fa in modo che il messaggio venga instradato attraverso il gestore code gateway QM1. Quando QM1 riceve il messaggio, è consapevole che il messaggio è ancora destinato a una coda denominata Q2 ed esegue la risoluzione dei nomi. QM1 controlla le relative definizioni locali e non ne trova alcuna per Q2. QM1 , quindi, controlla la configurazione del cluster e rileva due istanze di Q2 nel cluster DEMO. QM1 può ora utilizzare il bilanciamento del carico di lavoro per distribuire i messaggi tra le istanze di Q2 che risiedono su QM2 e QM4.

Concetti correlati

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.

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.

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.

Attività correlate

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.

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.

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 correlate

Risoluzione nome coda

Risoluzione nomi

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. Vedi Cluster sovrapposti. 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.

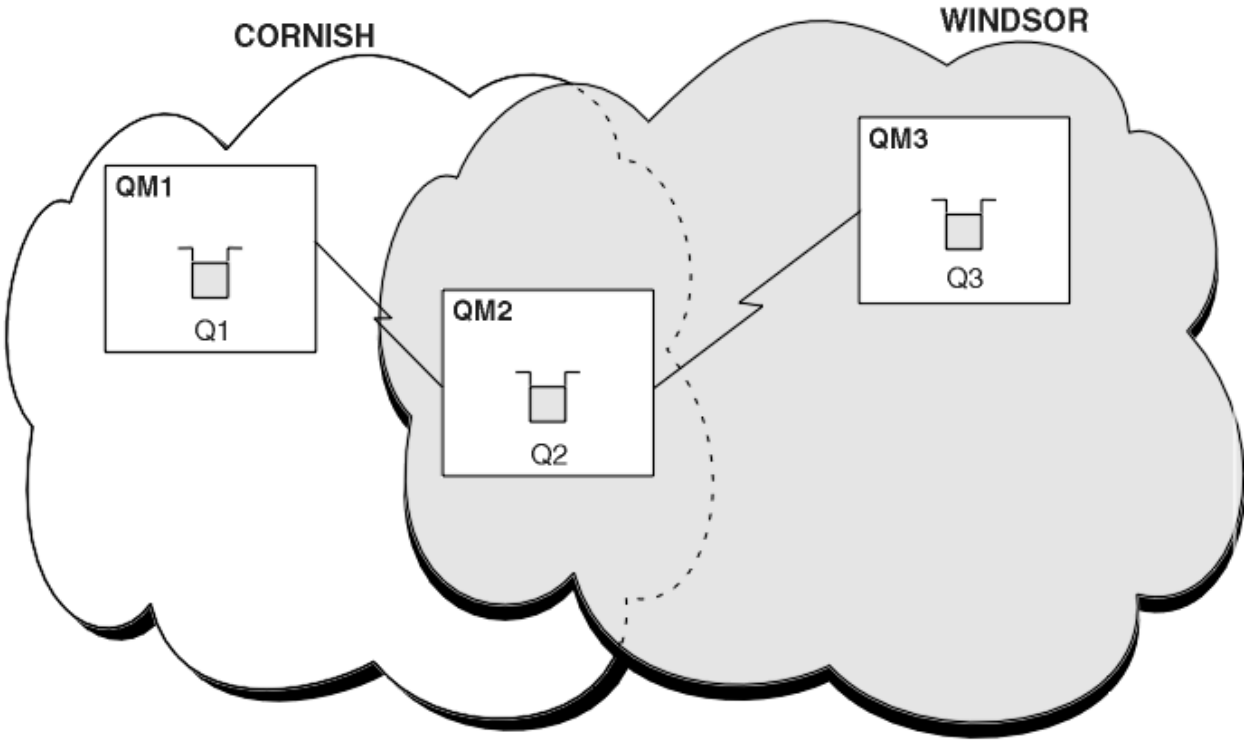


Figura 59. Collegamento tra cluster

Figura 59 a pagina 370 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 59 a pagina 370, 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 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 .

Concetti correlati

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.

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.

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.

Attività correlate

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.

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.

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.

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 dei gestori 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 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 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. Cerca una definizione di alias del gestore code con lo stesso nome del gestore code nell'intestazione di trasmissione. Se ne trova uno, sostituisce RQMNAME dalla definizione dell'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 324, da cui viene preso il flusso di messaggi di risposta 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.

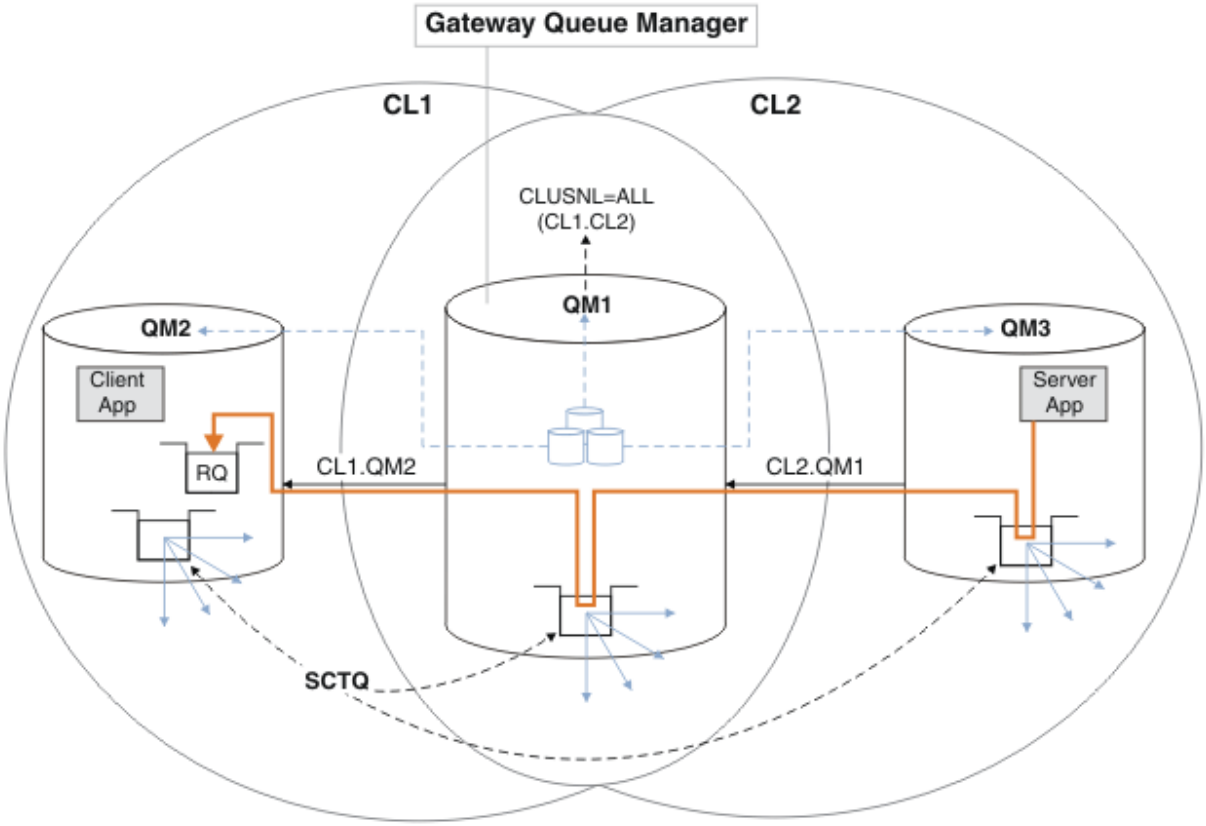


Figura 60. Utilizzo di un alias del gestore code per restituire il messaggio di risposta a un cluster differente

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 366

Concetti correlati

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.

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.

Attività correlate

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.

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.

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.

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.

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.

Concetti correlati

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.

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.

Attività correlate

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.

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.

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.

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.

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.

Concetti correlati

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.

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.

Attività correlate

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.

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.

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.

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.

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.

z/OS Ad esempio, in un sysplex parallelo z/OS le applicazioni clonate potrebbero accedere ai dati in un database VSAM (Virtual Storage Access Method) o Db2 condiviso. È possibile distribuire il workload tra i propri gestori code disponendo di diverse istanze di un'applicazione. Ogni istanza dell'applicazione riceve messaggi e viene eseguita indipendentemente dalle altre.

I vantaggi di utilizzare i cluster in questo modo sono i seguenti:

- Maggiore disponibilità delle code e delle applicazioni.
- Maggiore velocità di trasmissione dei messaggi.
- Distribuzione più uniforme del carico di lavoro nella rete.

Uno qualsiasi dei gestori code che ospita un'istanza di una particolare coda può gestire i messaggi destinati a tale coda e le applicazioni non denominano un gestore code quando inviano i messaggi. Se un cluster contiene più di un'istanza della stessa coda, IBM MQ seleziona un gestore code a cui instradare un messaggio. Le destinazioni adatte vengono scelte in base alla disponibilità del gestore code e della coda

e in base a un certo numero di attributi specifici del carico di lavoro del cluster associati a gestori code, code e canali. Vedi Bilanciamento del carico di lavoro in cluster.

z/OS In IBM MQ for z/OS, i gestori code che si trovano in gruppi di condivisione code possono ospitare code cluster come code condivise. Le code cluster condivise sono disponibili per tutti i gestori code nello stesso gruppo di condivisione code. Ad esempio, in Un cluster con più istanze della stessa coda, uno o entrambi i gestori code QM2 e QM4 possono essere un gestore code condiviso. Ognuno ha una definizione per la coda Q3. Qualsiasi gestore code nello stesso gruppo di condivisione code di QM4 può leggere un messaggio inserito nella coda condivisa Q3. Ogni gruppo di condivisione code può contenere fino a 32 gestori code, ognuno con accesso agli stessi dati. La condivisione della coda aumenta in modo significativo la velocità di trasmissione dei messaggi.

Consultare i seguenti argomenti secondari per ulteriori informazioni sulle configurazioni cluster per la gestione del carico di lavoro:

Concetti correlati

Confronto tra cluster e accodamento distribuito

Accodamento distribuito e cluster

Componenti di un cluster

Canali cluster

Cosa succede se una coda cluster è disabilitata per MQPUT

“Instradamento dei messaggi verso e dai cluster” a pagina 358
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

Scrittura e compilazione delle uscite del carico di lavoro del cluster

“Configurazione di un cluster di gestore code” a pagina 275
I cluster forniscono un meccanismo per l'interconnessione dei gestori code in modo da semplificare sia la configurazione iniziale che la gestione in corso. È possibile definire componenti cluster e creare e gestire cluster.

“Configurazione di un nuovo cluster” a pagina 287
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 del bilanciamento del workload dall'esterno di un cluster” a pagina 366
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.

Riferimenti correlati

Il bilanciamento del carico di lavoro impostato su un canale mittente del cluster non sta funzionando

Programma di esempio Monitoraggio coda cluster (AMQSCLM)

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 61 a pagina 378 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.

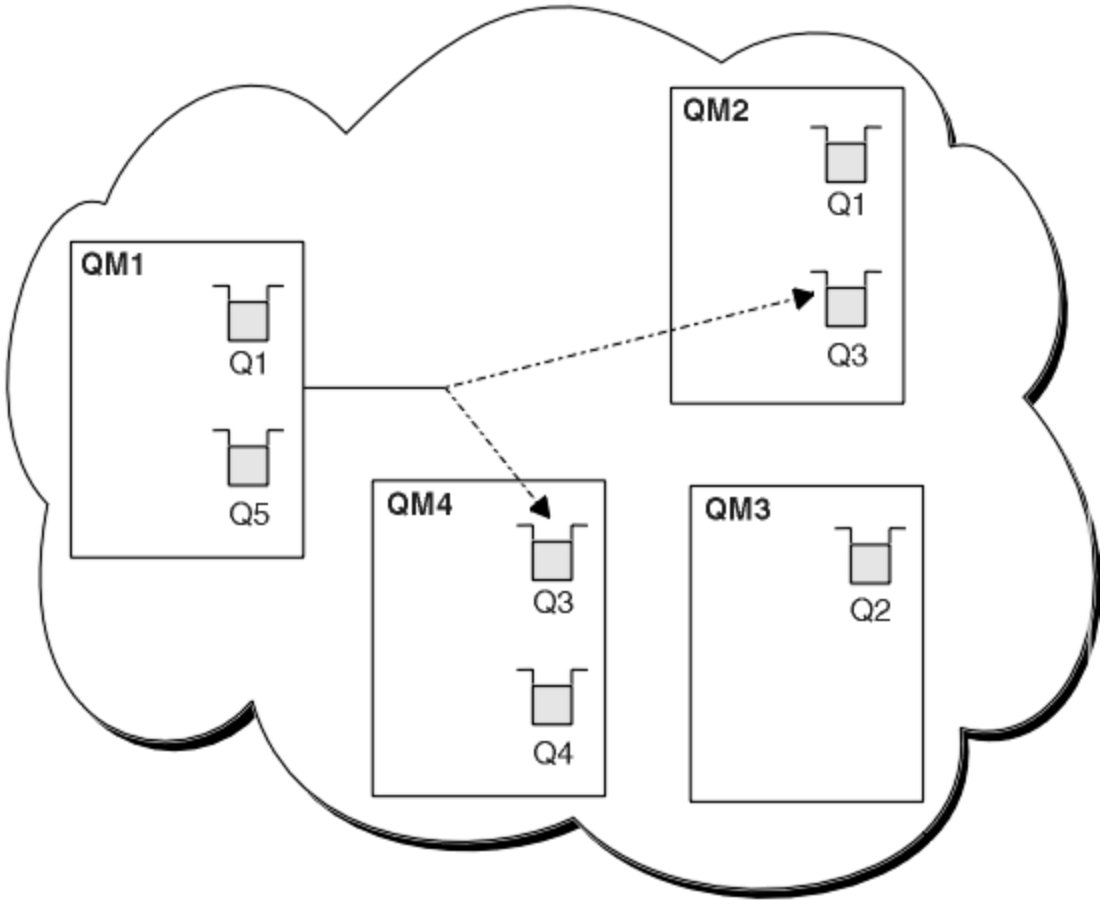


Figura 61. Un cluster con più istanze della stessa coda

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.

z/OS Su IBM MQ for z/OS, il canale non si arresta completamente fino a quando non viene completato il processo di riassegnazione del messaggio. L'interruzione del canale con modalità impostata su FORCE o TERMINATE non interrompe il processo, quindi se si esegue questa operazione, alcuni messaggi BIND_NOT_FIXED potrebbero essere già stati riassegnati a un altro canale oppure i messaggi potrebbero non essere in ordine.

Nota: z/OS

1. Prima di configurare un cluster che abbia più istanze della stessa coda, assicurarsi che i messaggi non abbiano dipendenze tra loro. Ad esempio, deve essere elaborato in una sequenza specifica o dallo stesso gestore code.
2. Rendere identiche le definizioni per istanze differenti della stessa coda. Altrimenti, si ottengono risultati diversi da chiamate MQINQ differenti.

Concetti correlati

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.

Attività correlate

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.

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.

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.

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.

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.

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.

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.

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 già stato fatto, avviare l'iniziatore di canali su IBM MQ for 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 62 a pagina 380 mostra il cluster impostato da questa attività.

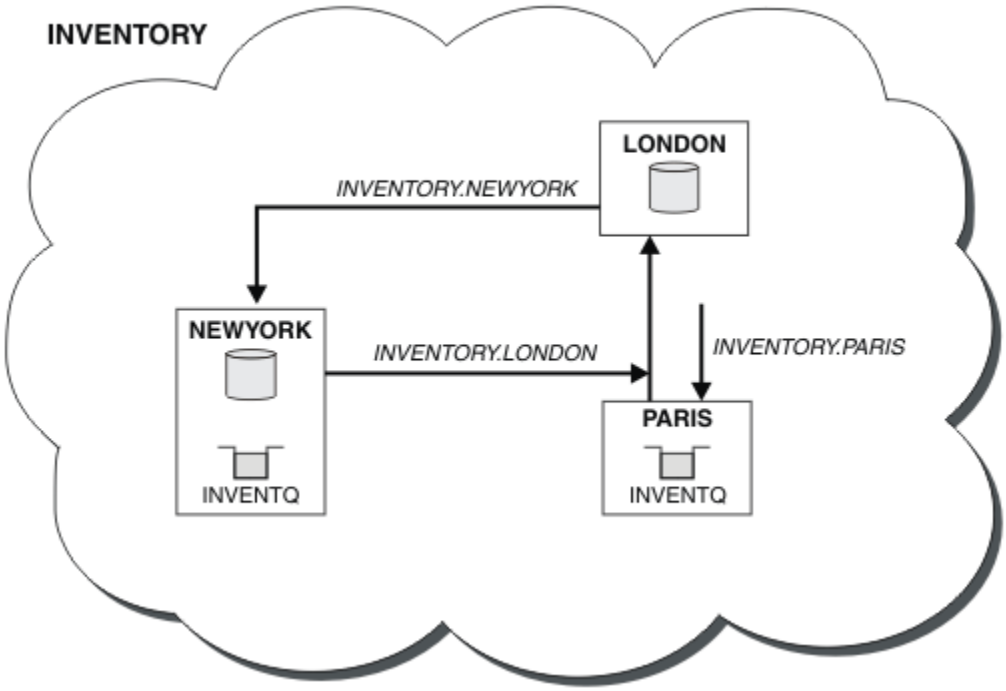


Figura 62. Il cluster INVENTORY , con tre gestori code

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.

Concetti correlati

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.

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.

Attività correlate

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.

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.

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.

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.

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.

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 stato ancora fatto, avviare l'iniziatore di canali su IBM MQ for 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 63 a pagina 383 mostra il cluster impostato da questa attività.

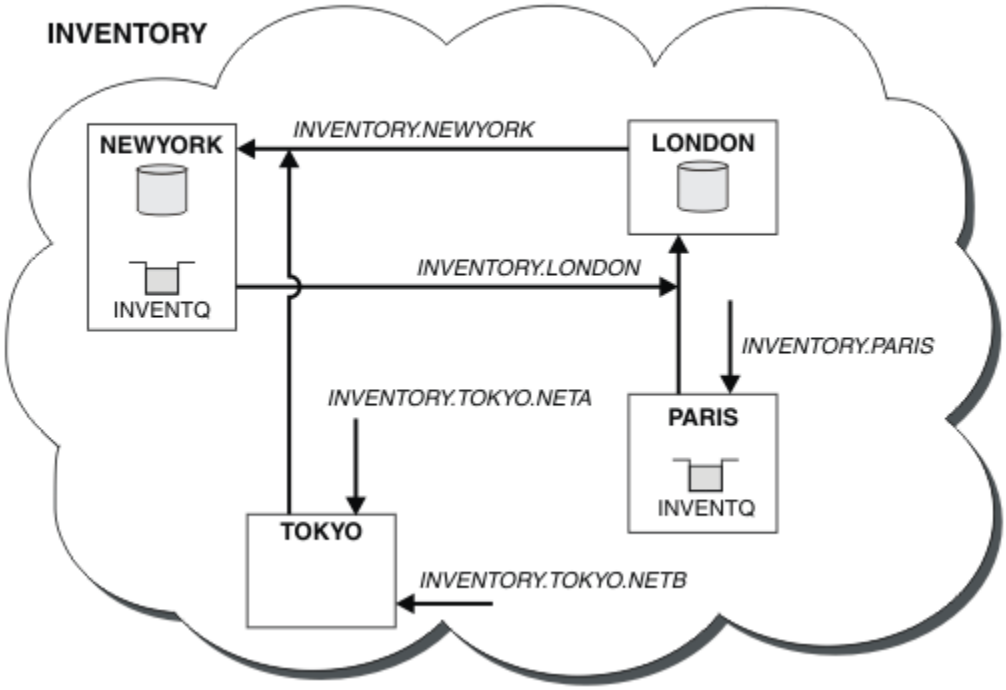


Figura 63. Il cluster INVENTORY , con quattro gestori code

Facendo solo tre definizioni, abbiamo aggiunto il gestore code TOKYO al cluster con due diversi instradamenti di rete disponibili.

Concetti correlati

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.

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.

Attività correlate

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.

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.

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.

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.

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.

“Aggiunta di un gestore code a un cluster” a pagina 299
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 381. 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.

Concetti correlati

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.

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.

Attività correlate

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.

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.

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.

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.

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.

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 299. 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 stato ancora fatto, avviare l'iniziatore di canali su IBM MQ for 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 64 a pagina 386 mostra il cluster impostato da questa attività.

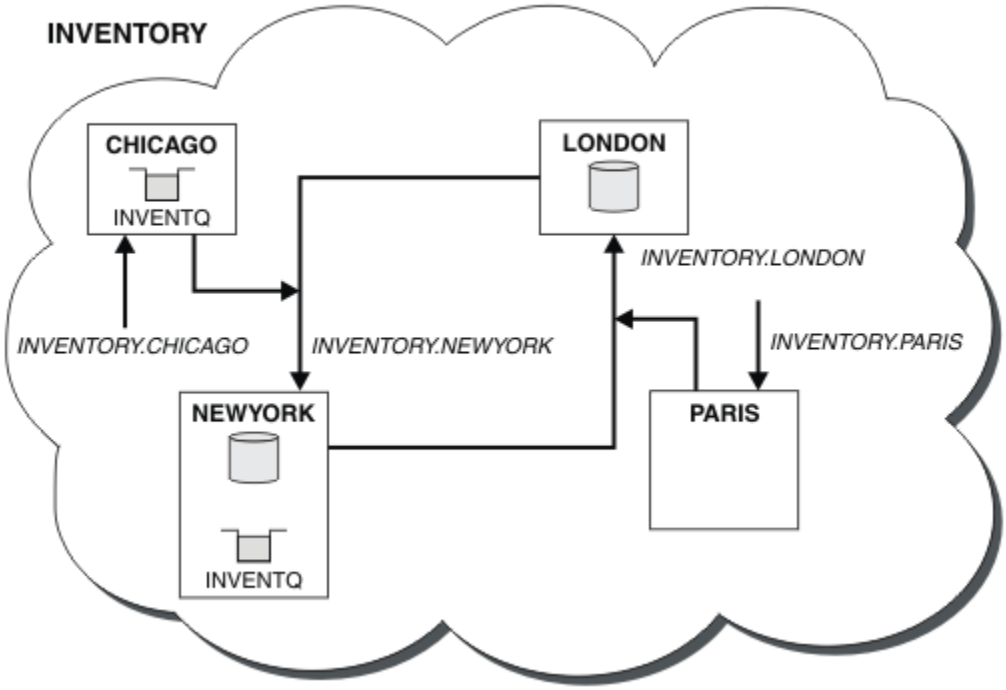


Figura 64. Il cluster INVENTORY, con quattro gestori code

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 degli stati meno preferibili 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.

Concetti correlati

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.

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.

Attività correlate

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.

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.

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.

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.

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.

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 IBM MQ for 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 65 a pagina 389 mostra il cluster impostato da questa attività.

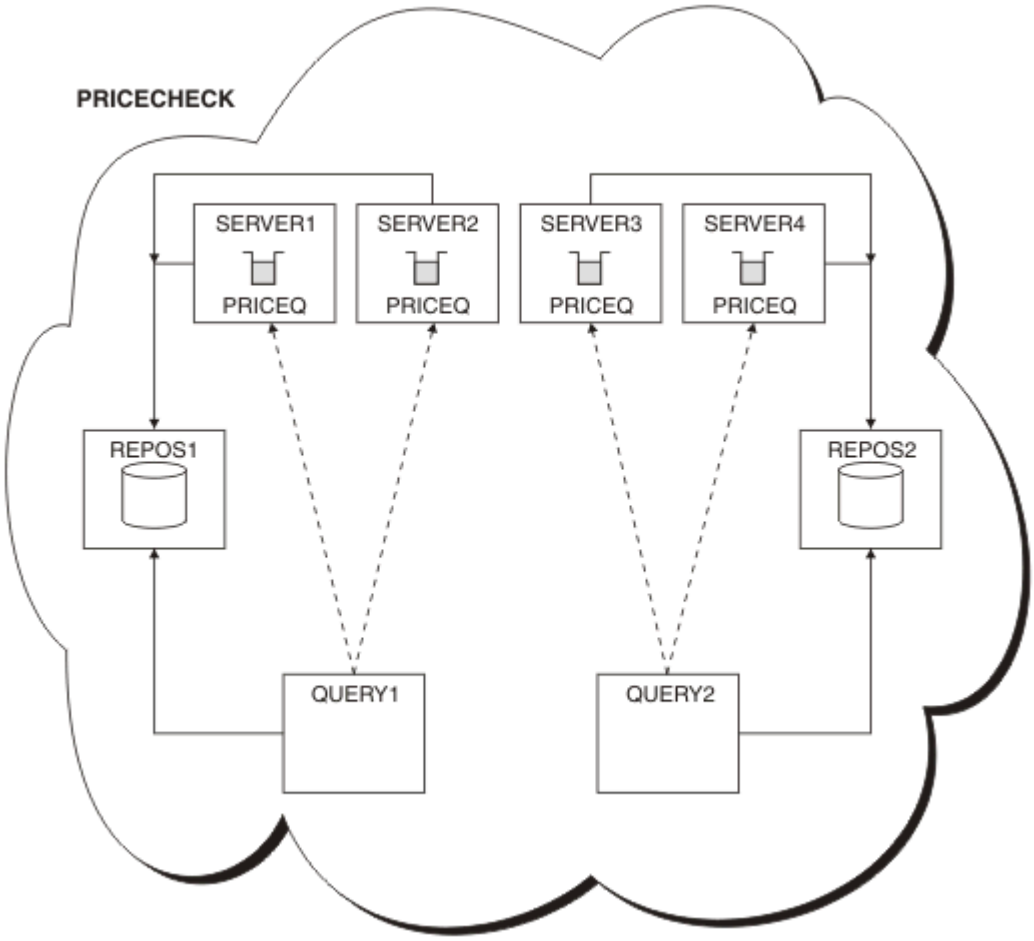


Figura 65. Il cluster PRICECHECK , con quattro gestori code del server, due repository e due gestori code di query

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.

Concetti correlati

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.

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.

Attività correlate

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.

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.

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.

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.

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.

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 299. 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 stato ancora fatto, avviare l'iniziatore di canali su IBM MQ for 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 390 mostra il cluster impostato da questa attività.

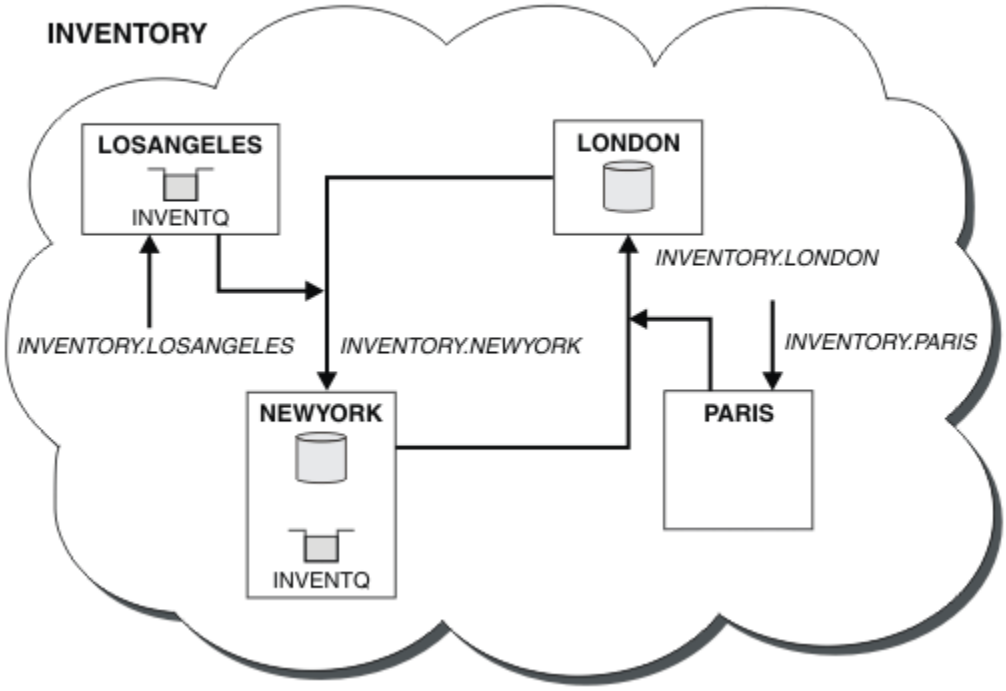


Figura 66. Il cluster INVENTORY con quattro gestori code

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.

Concetti correlati

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.

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.

Attività correlate

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.

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.

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.

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.

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.

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)`.

Concetti correlati

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.

Attività correlate

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.

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.

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.

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.

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.

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.

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.

Configurazione della messaggistica di pubblicazione/sottoscrizione

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.

Procedura

- Consultare i seguenti argomenti secondari per ulteriori informazioni sul controllo della pubblicazione / sottoscrizione accodata:
  - “Impostazione degli attributi dei messaggi di pubblicazione / sottoscrizione accodati” a pagina 396
  - “Avvio della pubblicazione / sottoscrizione accodata” a pagina 398
  - “Arresto della pubblicazione / sottoscrizione in coda” a pagina 398
  - “Aggiunta di uno stream” a pagina 399
  - “Eliminazione di uno stream” a pagina 400
  - “Aggiunta di un punto di sottoscrizione” a pagina 400
  - “Combinazione di spazi argomento nelle reti di pubblicazione / sottoscrizione” a pagina 409

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 28. 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 Esplora risorse di IBM MQ , i 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

Si avvia la pubblicazione / sottoscrizione accodata impostando l'attributo PSMODE del gestore code.

Prima di iniziare

Leggere la descrizione di PSMODE per comprendere le tre modalità di pubblicazione / sottoscrizione:

- COMPAT
- Disabilitato
- Abilitato

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 IBM 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

IBM MQ elabora i comandi di pubblicazione / sottoscrizione accodati e le chiamate MQI (Message Queue Interface) di pubblicazione / sottoscrizione.

Arresto della pubblicazione / sottoscrizione in coda

La pubblicazione / sottoscrizione in coda viene arrestata impostando l'attributo PSMODE del gestore code.

Prima di iniziare

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 IBM MQ Explorer o il comando **runmqsc** per disattivare l'interfaccia di pubblicazione / sottoscrizione in coda.

Esempio

```
ALTER QMGR PSMODE (COMPAT)
```

Aggiunta di uno stream

È possibile aggiungere i flussi manualmente per consentire l'isolamento dei dati tra le applicazioni o per consentire l'interoperatività con le gerarchie di pubblicazione / sottoscrizione IBM WebSphere MQ 6 .

Prima di iniziare

Familiarizzare con il modo in cui operano i flussi di pubblicazione / sottoscrizione. Vedi Stream e argomenti.

Informazioni su questa attività

Utilizzare il comando PCF, **runmqsc**o IBM 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 IBM WebSphere MQ 6 .
2. Definire un argomento locale con lo stesso nome del flusso IBM WebSphere MQ 6 .
3. Aggiungere il nome della coda all'elenco nomi, `SYSTEM.QPUBSUB.QUEUE.NAMELIST`
4. Ripetere le operazioni per tutti i gestori code IBM WebSphere MQ 7.1 o superiori che si trovano nella gerarchia di pubblicazione / sottoscrizione.

Aggiunta `'Sport'`

Nell'esempio di condivisione del flusso `'Sport'`, i gestori code IBM WebSphere MQ 6 e IBM WebSphere MQ 7.1 operano nella stessa gerarchia di pubblicazione / sottoscrizione. I gestori code IBM WebSphere MQ 6 condividono un flusso denominato `'Sport'`. L'esempio mostra come creare una coda e un argomento su IBM WebSphere MQ 7.1 gestori code denominati `'Sport'`, con una stringa di argomenti `'Sport'` condivisa con il flusso IBM WebSphere MQ 6 `'Sport'`.

Un' IBM WebSphere MQ 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 IBM WebSphere MQ 7.1 , i sottoscrittori dell'argomento `'Sport'`, con stringa argomento `'Soccer/Results'` ricevono la pubblicazione.

Su IBM WebSphere MQ 6 gestori code, i sottoscrittori del flusso `'Sport'`, con la stringa argomento `'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: IBM MQ queue created.
define topic('Sport') topicstr('Sport')
     2 : define topic('Sport') topicstr('Sport')
AMQ8690: IBM MQ topic created.
alter namelist(SYSTEM.QPUBSUB.QUEUE.NAMELIST) NAMES('Sport', 'SYSTEM.BROKER.DEFAULT.STREAM',
'SYSTEM.BROKER.ADMIN.STREAM')
     3 : alter namelist(SYSTEM.QPUBSUB.QUEUE.NAMELIST) NAMES('Sport', 'SYSTEM.BROKER.DEFAULT.STREAM',
'SYSTEM.BROKER.ADMIN.STREAM')
AMQ8551: IBM MQ namelist changed.
```

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 alla versione 6, gestirlo come un broker IBM WebSphere MQ 6 . 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 la versione di un broker è 71, è necessario configurare manualmente ciascun gestore code IBM WebSphere MQ 7.1 nella gerarchia.

Eliminazione di uno stream

È possibile eliminare un flusso da un gestore code IBM WebSphere MQ 7.1o successivo.

Prima di iniziare

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.

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

Ripetere i passi da 3 a 5 su tutti gli altri gestori code connessi IBM WebSphere MQ 7.1o successivi che ospitano il flusso.

Aggiunta di un punto di sottoscrizione

Come estendere un'applicazione di pubblicazione / sottoscrizione accodata esistente migrata da una versione precedente di IBM Integration Bus con un nuovo punto di sottoscrizione.

Prima di iniziare

1. Verificare che il punto di sottoscrizione non sia già definito in SYSTEM.QPUBSUB.SUBPOINT.NAMELIST.
2. 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 7.1o successive non utilizzano i punti di sottoscrizione, ma possono interagire con le applicazioni esistenti che utilizzano il meccanismo di migrazione dei punti di sottoscrizione.

Importante: Il meccanismo di migrazione del punto di sottoscrizione è stato rimosso da IBM MQ 8.0. Se è necessario migrare le applicazioni esistenti, è necessario eseguire le procedure descritte nella documentazione per la versione del prodotto, prima di migrare alla versione più recente.

I punti di sottoscrizione non funzionano con i programmi di pubblicazione / sottoscrizione accodati che utilizzano intestazioni MQRFH1 , che sono stati migrati da IBM WebSphere MQ 6o precedenti.

Non è necessario aggiungere punti di sottoscrizione per utilizzare le applicazioni di pubblicazione / sottoscrizione integrate scritte per IBM WebSphere MQ 7.1o versioni successive.

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.

Configurazione delle reti di pubblicazione / sottoscrizione distribuite

I gestori code connessi insieme in una topologia di pubblicazione / sottoscrizione distribuita condividono uno spazio argomenti federato comune. Le sottoscrizioni create su un gestore code possono ricevere messaggi pubblicati da un'applicazione connessa a un altro gestore code nella topologia.

È possibile controllare l'estensione degli spazi argomento creati collegando i gestori code in cluster o gerarchie. In un cluster di pubblicazione / sottoscrizione, un oggetto argomento deve essere 'in cluster' per ogni ramo dello spazio argomento che deve estendersi al cluster. In una gerarchia, ciascun gestore code deve essere configurato per identificare il relativo 'parent' nella gerarchia.

È possibile controllare ulteriormente il flusso di pubblicazioni e sottoscrizioni all'interno della topologia, scegliendo se ciascuna pubblicazione e sottoscrizione è locale o globale. Le pubblicazioni e le sottoscrizioni locali non vengono propagate oltre il gestore code a cui è connesso il publisher o il sottoscrittore.

Concetti correlati

Reti di pubblicazione / sottoscrizione distribuite

Ambito della pubblicazione

Ambito della sottoscrizione

Spazi argomento

Attività correlate

Definizione degli argomenti del cluster

Configurazione di un cluster di pubblicazione / sottoscrizione

Definire un argomento su un gestore code. Per rendere l'argomento un argomento cluster, impostare la proprietà **CLUSTER** . Per scegliere l'instradamento da utilizzare per pubblicazioni e sottoscrizioni per questo argomento, impostare la proprietà **CLROUTE** .

Prima di iniziare

Alcune configurazioni cluster non possono contenere i costi generali della pubblicazione / sottoscrizione instradata diretta. Prima di utilizzare questa configurazione, esplorare le considerazioni e le opzioni dettagliate in Progettazione di cluster di pubblicazione / sottoscrizione.

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.

Vedere anche Instradamento per i cluster di pubblicazione / sottoscrizione: Note sul funzionamento.

Scenario:

- Il cluster INVENTORY è stato configurato come descritto in “Aggiunta di un gestore code a un cluster” a pagina 299. Contiene tre gestori code; LONDON e NEWYORK contengono entrambi repository completi, PARIS contiene un repository parziale.

Informazioni su questa attività

Quando si definisce un argomento su un gestore code in un cluster, è necessario specificare se l'argomento è un argomento cluster e (in tal caso) l'instradamento all'interno del cluster per le pubblicazioni e le sottoscrizioni per questo argomento. Per rendere l'argomento un argomento cluster, configurare la proprietà **CLUSTER** sull'oggetto TOPIC con il nome del cluster. Definendo un argomento cluster su un gestore code nel cluster, l'argomento viene reso disponibile all'intero cluster. Per scegliere l'instradamento del messaggio da utilizzare nel cluster, impostare la proprietà **CLROUTE** sull'oggetto TOPIC su uno dei seguenti valori:

- **DIRECT**
- **TOPICHOST**

Per impostazione predefinita, l'instradamento argomento è **DIRECT**. Questa era l'unica opzione prima di IBM MQ 8.0. Quando si configura un argomento di cluster con instradamento diretto su un gestore code, tutti i gestori code presenti nel cluster sono a conoscenza di tutti gli altri gestori code del cluster. Quando si effettuano operazioni di pubblicazione e sottoscrizione, ogni gestore code può collegarsi direttamente ad ogni altro gestore code nel cluster. Vedere Cluster di pubblicazione / sottoscrizione instradati diretti.

Da IBM MQ 8.0, è invece possibile configurare l'instradamento argomento come **TOPICHOST**. Quando si utilizza l'instradamento all'host argomento, tutti i gestori code presenti nel cluster sono a conoscenza dei gestori code del cluster che ospitano le definizioni dell'argomento instradato (ossia, i gestori code in cui è stato definito l'oggetto dell'argomento). Quando si effettuano operazioni di pubblicazione e sottoscrizione, i gestori code del cluster si connettono soltanto a questi gestori code dell'host argomento

e non direttamente l'uno all'altro. I gestori code dell'host argomento sono responsabili dell'instradamento delle pubblicazioni dai gestori code su cui vengono pubblicate le pubblicazioni ai gestori code con le sottoscrizioni corrispondenti. Consultare Cluster di pubblicazione / sottoscrizione instradati dell'host argomento.

Nota: Una volta che un oggetto argomento è stato raggruppato in cluster (mediante l'impostazione della proprietà **CLUSTER**) non è possibile modificare il valore della proprietà **CLROUTE** . Prima di poter modificare il valore, è necessario rimuovere l'oggetto dal cluster (**CLUSTER** impostato su ' '). La rimozione di un argomento dal cluster converte la definizione dell'argomento in un argomento locale, il che comporta un periodo durante il quale le pubblicazioni non vengono consegnate alle sottoscrizioni sui gestori code remoti; è necessario considerare questo aspetto quando si effettua questa modifica. Consultare Effetto della definizione di un argomento non cluster con lo stesso nome di un argomento cluster di un altro gestore code. Se si tenta di modificare il valore della proprietà **CLROUTE** mentre è in cluster, il sistema genera un'errore MQRCCF_CLROUTE_NOT_ALTERABLE .

Procedura

1. Scegliere un gestore code per ospitare il proprio argomento.

   Qualsiasi gestore code cluster può ospitare un argomento. Scegliere uno dei tre gestori code (LONDON, NEWYORK o PARIS) e configurare le proprietà dell'oggetto TOPIC . Se si prevede di utilizzare l'instradamento diretto, non fa alcuna differenza operativa quale gestore code si sceglie. Se si prevede di utilizzare l'instradamento dell'host argomento, il gestore code scelto ha ulteriori responsabilità per l'instradamento delle pubblicazioni. Pertanto, per l'instradamento dell'host dell'argomento, scegliere un gestore code che sia ospitato su uno dei sistemi più potenti e che disponga di una buona connettività di rete.
2. Definire un argomento su un gestore code.

   Per rendere l'argomento un argomento cluster, includere il nome cluster quando si definisce l'argomento e impostare l'instradamento che si desidera utilizzare per pubblicazioni e sottoscrizioni per questo argomento. Ad esempio, per creare un argomento cluster di instradamento diretto sul gestore code LONDON , creare l'argomento nel modo seguente:

   ```
   DEFINE TOPIC(INVENTORY) TOPICSTR('/INVENTORY') CLUSTER(INVENTORY) CLROUTE(DIRECT)
   ```

   Definendo un argomento cluster su un gestore code nel cluster, l'argomento viene reso disponibile all'intero cluster.

   Per ulteriori informazioni sull'utilizzo di **CLROUTE**, consultare DEFINE TOPIC (CLROUTE) e Instradamento per cluster di pubblicazione / sottoscrizione: Note sul comportamento.

Risultati

Il cluster è pronto a ricevere pubblicazioni e sottoscrizioni per l'argomento.

Operazioni successive

Se è stato configurato un cluster di pubblicazione / sottoscrizione instradato dell'host argomento, è probabile che si desideri aggiungere un secondo host argomento per questo argomento. Consultare “Aggiunta di ulteriori host argomento a un cluster instradato di host argomento” a pagina 406.

Se hai diversi cluster di pubblicazione / sottoscrizione separati, ad esempio perché la tua organizzazione è geograficamente dispersa, potresti voler propagare alcuni argomenti del cluster in tutti i cluster. È possibile eseguire questa operazione connettendo i cluster in una gerarchia. Consultare “Combinazione degli spazi argomento di più cluster” a pagina 412. È inoltre possibile controllare quali pubblicazioni fluiscono da un cluster all'altro. Consultare “Combinazione e isolamento di spazi argomento in più cluster” a pagina 414.

Concetti correlati

Combinazione di ambiti di pubblicazione e sottoscrizione

Da IBM WebSphere MQ 7.0 in poi, la pubblicazione e l'ambito della sottoscrizione funzionano in modo indipendente per determinare il flusso di pubblicazioni tra i gestori code.

Combinazione di spazi argomento nelle reti di pubblicazione / sottoscrizione
Combinare lo spazio argomenti di un gestore code con altri gestori code in una gerarchia o in un cluster di pubblicazione / sottoscrizione. Combinare cluster di pubblicazione / sottoscrizione e cluster di pubblicazione / sottoscrizione con le gerarchie.

Attività correlate

Spostamento di una definizione di argomento del raggruppamento in un gestore code differente
Per l'host argomento instradato o i cluster instradati direttamente, potrebbe essere necessario spostare una definizione dell'argomento del cluster durante la disattivazione di un gestore code o perché un gestore code del cluster ha riportato un errore o non è disponibile per un periodo di tempo significativo.

Aggiunta di ulteriori host argomento a un cluster instradato di host argomento
In un cluster di pubblicazione / sottoscrizione instradato dall'host argomento, è possibile utilizzare più gestori code per instradare le pubblicazioni alle sottoscrizioni definendo lo stesso oggetto argomento in cluster su tali gestori code. Può essere utilizzato per migliorare la disponibilità e il bilanciamento del carico di lavoro. Quando si aggiunge un host argomento supplementare per lo stesso oggetto argomento cluster, è possibile utilizzare il parametro **PUB** per controllare quando le pubblicazioni iniziano ad essere instradate attraverso il nuovo host argomento.

Connessione di un gestore code a una gerarchia di pubblicazione / sottoscrizione
Si connette il gestore code secondario al gestore code principale nella gerarchia. Se il gestore code child è già un membro di un'altra gerarchia o cluster, questa connessione unisce le gerarchie o unisce il cluster alla gerarchia.

Disconnessione di un gestore code da una gerarchia di pubblicazione / sottoscrizione
Disconnettere un gestore code secondario da un gestore code principale in una gerarchia di pubblicazione / sottoscrizione.

Progettazione di cluster di pubblicazione / sottoscrizione

Risoluzione dei problemi di pubblicazione / sottoscrizione distribuita

Blocco della pubblicazione / sottoscrizione in cluster

Spostamento di una definizione di argomento del raggruppamento in un gestore code differente

Per l'host argomento instradato o i cluster instradati direttamente, potrebbe essere necessario spostare una definizione dell'argomento del cluster durante la disattivazione di un gestore code o perché un gestore code del cluster ha riportato un errore o non è disponibile per un periodo di tempo significativo.

Informazioni su questa attività

È possibile disporre di più definizioni dello stesso oggetto argomento cluster in un cluster. Si tratta di uno stato normale per un cluster instradato dell'host argomento e di uno stato insolito per un cluster instradato direttamente. Per ulteriori informazioni, consultare Più definizioni di argomenti cluster con lo stesso nome.

Per spostare una definizione di argomento del cluster in un gestore code differente nel cluster senza interrompere il flusso di pubblicazioni, effettuare le operazioni riportate di seguito. La procedura sposta una definizione dal gestore code `QM1` al gestore code `QM2`.

Procedura

1. Creare un duplicato della definizione dell'argomento cluster su `QM2`.

   Per l'instradamento diretto, impostare tutti gli attributi in modo che corrispondano alla definizione di `QM1`.

Per l'instradamento dell'host argomento, definire inizialmente il nuovo host argomento come PUB(DISABLED). Ciò consente a QM2 di acquisire informazioni sulle sottoscrizioni nel cluster, ma non di avviare le pubblicazioni di instradamento.

2. Attendere la propagazione delle informazioni nel cluster.

   Attendere che la nuova definizione dell'argomento cluster venga propagata dai gestori code del repository completo a tutti i gestori code nel cluster. Utilizzare il comando **DISPLAY CLUSTER** per visualizzare gli argomenti del cluster su ciascun membro del cluster e controllare una definizione originata da QM2.

   Per l'instradamento dell'host argomento, attendi che il nuovo host argomento su QM2 venga a conoscenza di tutte le sottoscrizioni. Confrontare le sottoscrizioni proxy note a QM2 e quelle note a QM1. Un modo per visualizzare le sottoscrizioni proxy su un gestore code è quello di immettere il seguente comando **runmqsc** :

   ```
   DISPLAY SUB(*) SUBTYPE(PROXY)
   ```

3. Per l'instradamento dell'host argomento, ridefinire l'host argomento in QM2 come PUB(ENABLED), quindi ridefinire l'host argomento in QM1 come PUB(DISABLED).

   Ora che il nuovo host argomento su QM2 ha appreso di tutte le sottoscrizioni su altri gestori code, l'host argomento può avviare l'instradamento delle pubblicazioni.

   Utilizzando l'impostazione PUB(DISABLED) per sospendere il traffico di messaggi tramite QM1, si garantisce che nessuna pubblicazione sia in corso tramite QM1 quando si elimina la definizione dell'argomento cluster.

4. Eliminare la definizione dell'argomento cluster da QM1.

   È possibile eliminare la definizione solo da QM1 se il gestore code è disponibile. Altrimenti, è necessario eseguire entrambe le definizioni esistenti fino a quando QM1 non viene riavviato o rimosso in modo forzato.

   Se QM1 rimane non disponibile per un lungo periodo di tempo e durante questo periodo di tempo è necessario modificare la definizione dell'argomento in cluster in QM2, la definizione QM2 è più recente della definizione QM1 e, di conseguenza, prevale.

   Durante questo periodo, se vi sono differenze tra le definizioni su QM1 e QM2, gli errori vengono scritti nei log degli errori di entrambi i gestori code, segnalando all'utente la definizione dell'argomento cluster in conflitto.

   Se QM1 non tornerà mai al cluster, ad esempio a causa di una disattivazione non prevista a seguito di un errore hardware, come ultima possibilità è possibile utilizzare il comando RESET CLUSTER per espellere forzatamente il gestore code. **RESET CLUSTER** elimina automaticamente tutti gli oggetti argomento ospitati sul gestore code di destinazione.

Concetti correlati

Combinazione di ambiti di pubblicazione e sottoscrizione
Da IBM WebSphere MQ 7.0 in poi, la pubblicazione e l'ambito della sottoscrizione funzionano in modo indipendente per determinare il flusso di pubblicazioni tra i gestori code.

Combinazione di spazi argomento nelle reti di pubblicazione / sottoscrizione
Combinare lo spazio argomenti di un gestore code con altri gestori code in una gerarchia o in un cluster di pubblicazione / sottoscrizione. Combinare cluster di pubblicazione / sottoscrizione e cluster di pubblicazione / sottoscrizione con le gerarchie.

Attività correlate

Configurazione di un cluster di pubblicazione / sottoscrizione
Definire un argomento su un gestore code. Per rendere l'argomento un argomento cluster, impostare la proprietà **CLUSTER** . Per scegliere l'instradamento da utilizzare per pubblicazioni e sottoscrizioni per questo argomento, impostare la proprietà **CLROUTE** .

Aggiunta di ulteriori host argomento a un cluster instradato di host argomento

In un cluster di pubblicazione / sottoscrizione instradato dall'host argomento, è possibile utilizzare più gestori code per instradare le pubblicazioni alle sottoscrizioni definendo lo stesso oggetto argomento in cluster su tali gestori code. Può essere utilizzato per migliorare la disponibilità e il bilanciamento del carico di lavoro. Quando si aggiunge un host argomento supplementare per lo stesso oggetto argomento cluster, è possibile utilizzare il parametro **PUB** per controllare quando le pubblicazioni iniziano ad essere instradate attraverso il nuovo host argomento.

Connessione di un gestore code a una gerarchia di pubblicazione / sottoscrizione
Si connette il gestore code secondario al gestore code principale nella gerarchia. Se il gestore code child è già un membro di un'altra gerarchia o cluster, questa connessione unisce le gerarchie o unisce il cluster alla gerarchia.

Disconnessione di un gestore code da una gerarchia di pubblicazione / sottoscrizione
Disconnettere un gestore code secondario da un gestore code principale in una gerarchia di pubblicazione / sottoscrizione.

Aggiunta di ulteriori host argomento a un cluster instradato di host argomento

In un cluster di pubblicazione / sottoscrizione instradato dall'host argomento, è possibile utilizzare più gestori code per instradare le pubblicazioni alle sottoscrizioni definendo lo stesso oggetto argomento in cluster su tali gestori code. Può essere utilizzato per migliorare la disponibilità e il bilanciamento del carico di lavoro. Quando si aggiunge un host argomento supplementare per lo stesso oggetto argomento cluster, è possibile utilizzare il parametro **PUB** per controllare quando le pubblicazioni iniziano ad essere instradate attraverso il nuovo host argomento.

Prima di iniziare

La definizione dello stesso oggetto argomento cluster su diversi gestori code è utile solo dal punto di vista funzionale per un cluster instradato dell'host argomento. La definizione di più argomenti corrispondenti in un cluster instradato direttamente non ne modifica il funzionamento. Questa attività si applica solo ai cluster instradati dell'host argomento.

Questa attività presuppone che sia stato letto l'articolo Più definizioni di argomenti cluster con lo stesso nome, in particolare le seguenti sezioni:

- Più definizioni dell'argomento cluster in un cluster instradato all'host argomento
- Gestione speciale per il parametro PUB

Informazioni su questa attività

Quando un gestore code viene reso un host argomento instradato, deve prima conoscere l'esistenza di tutti gli argomenti correlati sottoscritti nel cluster. Se le pubblicazioni vengono pubblicate in tali argomenti nel momento in cui viene aggiunto un altro host argomento e una pubblicazione viene instradata al nuovo host prima che tale host abbia appreso dell'esistenza di sottoscrizioni su altri gestori code nel cluster, il nuovo host non inoltra tale pubblicazione a tali sottoscrizioni. Ciò fa sì che le sottoscrizioni non perda le pubblicazioni.

Le pubblicazioni non vengono instradate tramite gestore code dell'host argomento che hanno impostato esplicitamente il parametro **PUB** dell'oggetto argomento cluster su `DISABLED`, pertanto è possibile utilizzare questa impostazione per garantire che nessuna sottoscrizione perda le pubblicazioni durante il processo di aggiungere un ulteriore host argomento.

Nota: Mentre un gestore code ospita un argomento del cluster definito come `PUB(DISABLED)`, i publisher connessi a tale gestore code non possono pubblicare i messaggi e le sottoscrizioni corrispondenti su tale gestore code non ricevono le pubblicazioni pubblicate su altri gestori code del cluster. Per questo motivo, è necessario considerare attentamente la definizione degli argomenti instradati dell'host argomento sui gestori code in cui esistono le sottoscrizioni e la connessione delle applicazioni di pubblicazione.

Procedura

1. Configurare un nuovo host argomento e definire inizialmente il nuovo host argomento come PUB(DISABLED).

   Ciò consente al nuovo host argomento di conoscere le sottoscrizioni nel cluster, ma non di avviare le pubblicazioni di instradamento.

   Per informazioni sulla configurazione di un host argomento, consultare "Configurazione di un cluster di pubblicazione / sottoscrizione" a pagina 402.
2. Determinare quando il nuovo host argomento ha appreso tutte le sottoscrizioni.

   A tale scopo, confrontare le sottoscrizioni proxy note al nuovo host argomento e quelle note all'host argomento esistente. Un modo per visualizzare le sottoscrizioni proxy è immettere il seguente comando **runmqsc** : DISPLAY SUB(*) SUBTYPE(PROXY)
3. Ridefinire il nuovo host argomento come PUB(ENABLED).

   Dopo che il nuovo host argomento ha appreso di tutte le sottoscrizioni su altri gestori code, l'argomento può avviare l'instradamento delle pubblicazioni.

Concetti correlati

Combinazione di ambiti di pubblicazione e sottoscrizione
Da IBM WebSphere MQ 7.0 in poi, la pubblicazione e l'ambito della sottoscrizione funzionano in modo indipendente per determinare il flusso di pubblicazioni tra i gestori code.

Combinazione di spazi argomento nelle reti di pubblicazione / sottoscrizione
Combinare lo spazio argomenti di un gestore code con altri gestori code in una gerarchia o in un cluster di pubblicazione / sottoscrizione. Combinare cluster di pubblicazione / sottoscrizione e cluster di pubblicazione / sottoscrizione con le gerarchie.

Attività correlate

Configurazione di un cluster di pubblicazione / sottoscrizione
Definire un argomento su un gestore code. Per rendere l'argomento un argomento cluster, impostare la proprietà **CLUSTER** . Per scegliere l'instradamento da utilizzare per pubblicazioni e sottoscrizioni per questo argomento, impostare la proprietà **CLROUTE** .

Spostamento di una definizione di argomento del raggruppamento in un gestore code differente
Per l'host argomento instradato o i cluster instradati direttamente, potrebbe essere necessario spostare una definizione dell'argomento del cluster durante la disattivazione di un gestore code o perché un gestore code del cluster ha riportato un errore o non è disponibile per un periodo di tempo significativo.

Connessione di un gestore code a una gerarchia di pubblicazione / sottoscrizione
Si connette il gestore code secondario al gestore code principale nella gerarchia. Se il gestore code child è già un membro di un'altra gerarchia o cluster, questa connessione unisce le gerarchie o unisce il cluster alla gerarchia.

Disconnessione di un gestore code da una gerarchia di pubblicazione / sottoscrizione
Disconnettere un gestore code secondario da un gestore code principale in una gerarchia di pubblicazione / sottoscrizione.

Combinazione di ambiti di pubblicazione e sottoscrizione

Da IBM WebSphere MQ 7.0 in poi, la pubblicazione e l'ambito della sottoscrizione funzionano in modo indipendente per determinare il flusso di pubblicazioni tra i gestori code.

Le pubblicazioni possono essere destinate a tutti i gestori code connessi in una topologia di pubblicazione / sottoscrizione o solo al gestore code locale. Allo stesso modo per le sottoscrizioni proxy. Le pubblicazioni corrispondenti a una sottoscrizione sono regolate dalla combinazione di questi due flussi.

Le pubblicazioni e le sottoscrizioni possono essere entrambe nell'ambito di QMGR o ALL. Se un publisher e un sottoscrittore sono entrambi connessi allo stesso gestore code, le impostazioni dell'ambito non influiscono sulle pubblicazioni che il sottoscrittore riceve da tale publisher.

Se il publisher e il sottoscrittore sono connessi a gestori code differenti, entrambe le impostazioni devono essere ALL per ricevere le pubblicazioni remote.

Si supponga che i publisher siano connessi a gestori code differenti. Se si desidera che un sottoscrittore riceva le pubblicazioni da un qualsiasi publisher, impostare l'ambito della sottoscrizione su ALL. È quindi possibile decidere, per ciascun publisher, se limitare l'ambito delle proprie pubblicazioni ai sottoscrittori locali per il publisher.

Si supponga che i sottoscrittori siano connessi a gestori code differenti. Se si desidera che le pubblicazioni da un publisher vengano inviate a tutti i sottoscrittori, impostare l'ambito della pubblicazione su ALL. Se si desidera che un sottoscrittore riceva le pubblicazioni solo da un publisher connesso allo stesso gestore code, impostare l'ambito della sottoscrizione su QMGR.

Esempio: servizio risultati di calcio

Supponiamo che tu sia un membro di una squadra di calcio. Ogni team ha un gestore code connesso a tutti gli altri team in un cluster di pubblicazione / sottoscrizione.

Le squadre pubblicano i risultati di tutte le partite giocate in casa utilizzando l'argomento, `Football/result/`*`Home team name/Away team name`*. Le stringhe in corsivo sono nomi argomento variabili e la pubblicazione è il risultato della corrispondenza.

Ogni club ripubblica i risultati solo per il club utilizzando la stringa di argomento `Football/myteam/`*`Home team name/Away team name`*.

Entrambi gli argomenti vengono pubblicati nell'intero cluster.

Le seguenti sottoscrizioni sono state stabilite dalla lega in modo che i tifosi di qualsiasi squadra possano iscriversi ai risultati in tre modi interessanti.

Nota che puoi configurare gli argomenti del cluster con SUBSCOPE(QMGR). Le definizioni di argomento vengono propagate a ciascun membro del cluster, ma l'ambito della sottoscrizione è solo il gestore code locale. Pertanto, i sottoscrittori a ciascun gestore code ricevono pubblicazioni diverse dalla stessa sottoscrizione.

Ricevi tutti i risultati

```
DEFINE TOPIC(A) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(ALL)
```

Ricevi tutti i risultati a casa

```
DEFINE TOPIC(B) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(QMGR)
```

Poiché la sottoscrizione ha un ambito QMGR , vengono messi in corrispondenza solo i risultati pubblicati a terra.

Ricevi tutti i risultati dei miei team

```
DEFINE TOPIC(C) TOPICSTR('Football/myteam/') CLUSTER SUBSCOPE(QMGR)
```

Poiché la sottoscrizione ha un ambito QMGR , vengono messi in corrispondenza solo i risultati del team locale, ripubblicati localmente.

Concetti correlati

Combinazione di spazi argomento nelle reti di pubblicazione / sottoscrizione
Combinare lo spazio argomenti di un gestore code con altri gestori code in una gerarchia o in un cluster di pubblicazione / sottoscrizione. Combinare cluster di pubblicazione / sottoscrizione e cluster di pubblicazione / sottoscrizione con le gerarchie.

Reti di pubblicazione / sottoscrizione distribuite
Ambito della pubblicazione
Ambito della sottoscrizione

Attività correlate

Configurazione di un cluster di pubblicazione / sottoscrizione
Definire un argomento su un gestore code. Per rendere l'argomento un argomento cluster, impostare la proprietà **CLUSTER** . Per scegliere l'instradamento da utilizzare per pubblicazioni e sottoscrizioni per questo argomento, impostare la proprietà **CLROUTE** .

Spostamento di una definizione di argomento del raggruppamento in un gestore code differente
Per l'host argomento instradato o i cluster instradati direttamente, potrebbe essere necessario spostare una definizione dell'argomento del cluster durante la disattivazione di un gestore code o perché un gestore code del cluster ha riportato un errore o non è disponibile per un periodo di tempo significativo.

Aggiunta di ulteriori host argomento a un cluster instradato di host argomento
In un cluster di pubblicazione / sottoscrizione instradato dall'host argomento, è possibile utilizzare più gestori code per instradare le pubblicazioni alle sottoscrizioni definendo lo stesso oggetto argomento in cluster su tali gestori code. Può essere utilizzato per migliorare la disponibilità e il bilanciamento del carico di lavoro. Quando si aggiunge un host argomento supplementare per lo stesso oggetto argomento cluster, è possibile utilizzare il parametro **PUB** per controllare quando le pubblicazioni iniziano ad essere instradate attraverso il nuovo host argomento.

Connessione di un gestore code a una gerarchia di pubblicazione / sottoscrizione
Si connette il gestore code secondario al gestore code principale nella gerarchia. Se il gestore code child è già un membro di un'altra gerarchia o cluster, questa connessione unisce le gerarchie o unisce il cluster alla gerarchia.

Disconnessione di un gestore code da una gerarchia di pubblicazione / sottoscrizione
Disconnettere un gestore code secondario da un gestore code principale in una gerarchia di pubblicazione / sottoscrizione.

Combinazione di spazi argomento nelle reti di pubblicazione / sottoscrizione

Combinare lo spazio argomenti di un gestore code con altri gestori code in una gerarchia o in un cluster di pubblicazione / sottoscrizione. Combinare cluster di pubblicazione / sottoscrizione e cluster di pubblicazione / sottoscrizione con le gerarchie.

È possibile creare diversi spazi argomenti di pubblicazione / sottoscrizione utilizzando i blocchi di creazione degli attributi **CLUSTER**, **PUBSCOPE** e **SUBSCOPE** , i cluster di pubblicazione / sottoscrizione e le gerarchie di pubblicazione / sottoscrizione.

Partendo dall'esempio del ridimensionamento incrementale da un singolo gestore code a un cluster di pubblicazione / sottoscrizione, i seguenti scenari illustrano diverse topologie di pubblicazione / sottoscrizione.

Concetti correlati

Combinazione di ambiti di pubblicazione e sottoscrizione
Da IBM WebSphere MQ 7.0 in poi, la pubblicazione e l'ambito della sottoscrizione funzionano in modo indipendente per determinare il flusso di pubblicazioni tra i gestori code.

Reti di pubblicazione / sottoscrizione distribuite

Spazi argomento

Attività correlate

Configurazione di un cluster di pubblicazione / sottoscrizione
Definire un argomento su un gestore code. Per rendere l'argomento un argomento cluster, impostare la proprietà **CLUSTER** . Per scegliere l'instradamento da utilizzare per pubblicazioni e sottoscrizioni per questo argomento, impostare la proprietà **CLROUTE** .

Spostamento di una definizione di argomento del raggruppamento in un gestore code differente
Per l'host argomento instradato o i cluster instradati direttamente, potrebbe essere necessario spostare una definizione dell'argomento del cluster durante la disattivazione di un gestore code o perché un gestore code del cluster ha riportato un errore o non è disponibile per un periodo di tempo significativo.

Aggiunta di ulteriori host argomento a un cluster instradato di host argomento
In un cluster di pubblicazione / sottoscrizione instradato dall'host argomento, è possibile utilizzare più gestori code per instradare le pubblicazioni alle sottoscrizioni definendo lo stesso oggetto argomento in

cluster su tali gestori code. Può essere utilizzato per migliorare la disponibilità e il bilanciamento del carico di lavoro. Quando si aggiunge un host argomento supplementare per lo stesso oggetto argomento cluster, è possibile utilizzare il parametro **PUB** per controllare quando le pubblicazioni iniziano ad essere instradate attraverso il nuovo host argomento.

Connessione di un gestore code a una gerarchia di pubblicazione / sottoscrizione
Si connette il gestore code secondario al gestore code principale nella gerarchia. Se il gestore code child è già un membro di un'altra gerarchia o cluster, questa connessione unisce le gerarchie o unisce il cluster alla gerarchia.

Disconnessione di un gestore code da una gerarchia di pubblicazione / sottoscrizione
Disconnettere un gestore code secondario da un gestore code principale in una gerarchia di pubblicazione / sottoscrizione.

Definizione degli argomenti del cluster

Creazione di un singolo spazio argomento in un cluster di pubblicazione / sottoscrizione

Ridimensionare un sistema di pubblicazione / sottoscrizione per l'esecuzione su più gestori code. Utilizzare un cluster di pubblicazione / sottoscrizione per fornire a ciascun publisher e sottoscrittore un singolo spazio argomenti identico.

Prima di iniziare

È stato implementato un sistema di pubblicazione / sottoscrizione su un unico gestore code versione 7.

Creare sempre spazi argomento con i propri argomenti root, piuttosto che affidarsi all'eredità degli attributi di `SYSTEM.BASE.TOPIC`. Se si ridimensiona il sistema di pubblicazione / sottoscrizione fino a un cluster, è possibile definire i propri argomenti root come argomenti cluster, sull'host dell'argomento cluster e quindi tutti gli argomenti vengono condivisi all'interno del cluster.

Informazioni su questa attività

Ora si desidera scalare il sistema per supportare più publisher e sottoscrittori e avere ogni argomento visibile in tutto il cluster.

Procedura

1. Creare un cluster da utilizzare con il sistema di pubblicazione / sottoscrizione.

   Se si dispone di un cluster tradizionale esistente, per motivi di prestazioni è preferibile impostare un nuovo cluster per il nuovo sistema di pubblicazione - sottoscrizione. È possibile utilizzare gli stessi server per i repository cluster di entrambi i cluster
2. Scegliere un gestore code, possibilmente uno dei repository, come host dell'argomento del cluster.
3. Assicurarsi che ogni argomento che deve essere visibile in tutto il cluster di pubblicazione / sottoscrizione si risolva in un oggetto argomento di gestione.
   Impostare l'attributo **CLUSTER** denominando il cluster di pubblicazione / sottoscrizione.

Operazioni successive

Connettere le applicazioni publisher e sottoscrittore a qualsiasi gestore code nel cluster.

Creare oggetti argomento di gestione con l'attributo **CLUSTER** . Gli argomenti vengono anche propagati in tutto il cluster. I programmi di pubblicazione e sottoscrizione utilizzano gli argomenti di gestione in modo che il loro comportamento non venga modificato dalla connessione a gestori code differenti nel cluster

Se è necessario che `SYSTEM.BASE.TOPIC` agisca come un argomento del cluster su ogni gestore code, è necessario modificarlo su ogni gestore code.

Concetti correlati

Reti di pubblicazione / sottoscrizione distribuite

Spazi argomento

Attività correlate

Aggiunta di un gestore code IBM WebSphere MQ 7 o successivo agli spazi argomento IBM WebSphere MQ 6 esistenti
Estendere un sistema di pubblicazione / sottoscrizione IBM WebSphere MQ 6 esistente per interagire con un gestore code IBM WebSphere MQ 7 o successivo, condividendo gli stessi spazi argomento.

Combinazione degli spazi argomento di più cluster
Creare spazi argomento che si estendono su più cluster. Pubblicare in un argomento in un cluster e sottoscriverlo in un'altro.

Combinazione e isolamento di spazi argomento in più cluster
Isolare alcuni spazi argomento in un cluster specifico e combinare altri spazi argomento per renderli accessibili in tutti i cluster connessi.

Pubblicazione e sottoscrizione di spazi argomento in più cluster
Pubblicare e sottoscrivere argomenti in più cluster utilizzando cluster sovrapposti. È possibile utilizzare questa tecnica purché gli spazi argomento nei cluster non si sovrappongano.

Definizione degli argomenti del cluster

Aggiunta di un gestore code IBM WebSphere MQ 7 o successivo agli spazi argomento IBM WebSphere MQ 6 esistenti

Estendere un sistema di pubblicazione / sottoscrizione IBM WebSphere MQ 6 esistente per interagire con un gestore code IBM WebSphere MQ 7 o successivo, condividendo gli stessi spazi argomento.

Prima di iniziare

Si dispone di un sistema di pubblicazione / sottoscrizione IBM WebSphere MQ 6 esistente.

È stato installato IBM WebSphere MQ 7 o versione successiva su un nuovo server e configurato un gestore code.

Informazioni su questa attività

Si desidera estendere il sistema di pubblicazione / sottoscrizione IBM WebSphere MQ 6 esistente per utilizzare i gestori code IBM WebSphere MQ 7 o successivi.

Si è deciso di stabilizzare lo sviluppo del sistema di pubblicazione / sottoscrizione IBM WebSphere MQ 6 che utilizza l'interfaccia di pubblicazione / sottoscrizione accodata. Si intende aggiungere estensioni al sistema utilizzando l'interfaccia MQI IBM WebSphere MQ 7 o successiva. Non si dispone ora di piani per riscrivere le applicazioni di pubblicazione / sottoscrizione accodate.

Si intende aggiornare i gestori code IBM WebSphere MQ 6 a IBM WebSphere MQ 7 o versioni successive in futuro. Per ora, si continua ad eseguire le applicazioni di pubblicazione / sottoscrizione accodate esistenti sui gestori code IBM WebSphere MQ 7 o successivi.

Procedura

1. Creare una serie di canali mittente - destinatario per collegare il gestore code versione 7 o successiva con uno dei gestori code IBM WebSphere MQ 6 in entrambe le direzioni.
2. Creare due code di trasmissione con i nomi dei gestori code di destinazione. Utilizzare gli alias del gestore code se non è possibile utilizzare il nome del gestore code di destinazione come nome della coda di trasmissione per qualche motivo.
3. Configurare le code di trasmissione per attivare i canali mittente.
4. Se il sistema di pubblicazione / sottoscrizione IBM WebSphere MQ 6 utilizza i flussi, aggiungere i flussi al gestore code versione 7 o successiva come descritto in “Aggiunta di uno stream” a pagina 399.
5. Verificare che la versione 7 o successiva del gestore code **PSMODE** sia impostata su ENABLE.
6. Modificare l'attributo **PARENT** in modo che faccia riferimento ad uno dei gestori code IBM WebSphere MQ 6 .
7. Verificare che lo stato della relazione padre - figlio tra i gestori code sia attivo in entrambe le direzioni.

Operazioni successive

Una volta completata l'attività, il gestore code IBM WebSphere MQ 6 e IBM WebSphere MQ 7 o versioni successive condividono gli stessi spazi argomento. Ad esempio, è possibile eseguire tutte le attività riportate di seguito.

- Scambiare le pubblicazioni e le sottoscrizioni tra IBM WebSphere MQ 6 e IBM WebSphere MQ 7 o gestori code successivi.
- Eseguire i programmi di pubblicazione / sottoscrizione IBM WebSphere MQ 6 esistenti sul gestore code IBM WebSphere MQ 7 o successivo.
- Visualizzare e modificare lo spazio argomento sul gestore code IBM WebSphere MQ 6 o IBM WebSphere MQ 7 o versioni successive.
- Scrivere le applicazioni di pubblicazione / sottoscrizione IBM WebSphere MQ 7 o successive ed eseguirle sul gestore code IBM WebSphere MQ 7 o successivo.
- Creare nuove pubblicazioni e sottoscrizioni con le applicazioni IBM WebSphere MQ 7 o successive e scambiarle con le applicazioni IBM WebSphere MQ 6 .

Concetti correlati

Reti di pubblicazione / sottoscrizione distribuite

Spazi argomento

Attività correlate

Creazione di un singolo spazio argomento in un cluster di pubblicazione / sottoscrizione
Ridimensionare un sistema di pubblicazione / sottoscrizione per l'esecuzione su più gestori code. Utilizzare un cluster di pubblicazione / sottoscrizione per fornire a ciascun publisher e sottoscrittore un singolo spazio argomenti identico.

Combinazione degli spazi argomento di più cluster
Creare spazi argomento che si estendono su più cluster. Pubblicare in un argomento in un cluster e sottoscriverlo in un'altro.

Combinazione e isolamento di spazi argomento in più cluster
Isolare alcuni spazi argomento in un cluster specifico e combinare altri spazi argomento per renderli accessibili in tutti i cluster connessi.

Pubblicazione e sottoscrizione di spazi argomento in più cluster
Pubblicare e sottoscrivere argomenti in più cluster utilizzando cluster sovrapposti. È possibile utilizzare questa tecnica purché gli spazi argomento nei cluster non si sovrappongano.

Definizione degli argomenti del cluster

Combinazione degli spazi argomento di più cluster

Creare spazi argomento che si estendono su più cluster. Pubblicare in un argomento in un cluster e sottoscriverlo in un'altro.

Prima di iniziare

Questa attività presuppone che si disponga di cluster di pubblicazione / sottoscrizione instradati direttamente e che si desidera propagare alcuni argomenti del cluster in tutti i cluster.

Nota: Non è possibile eseguire questa operazione per i cluster di pubblicazione / sottoscrizione instradati dell'host argomento.

Informazioni su questa attività

Per propagare le pubblicazioni da un cluster a un altro, è necessario unire i cluster in una gerarchia; consultare Figura 67 a pagina 413. Le connessioni gerarchiche propagano le sottoscrizioni e pubblicazioni tra i gestori code connessi e i cluster propagano gli argomenti del cluster all'interno di ogni cluster, ma non tra i cluster.

La combinazione di questi due meccanismi propaga gli argomenti del cluster tra tutti i cluster. È necessario ripetere le definizioni degli argomenti del cluster in ogni cluster.

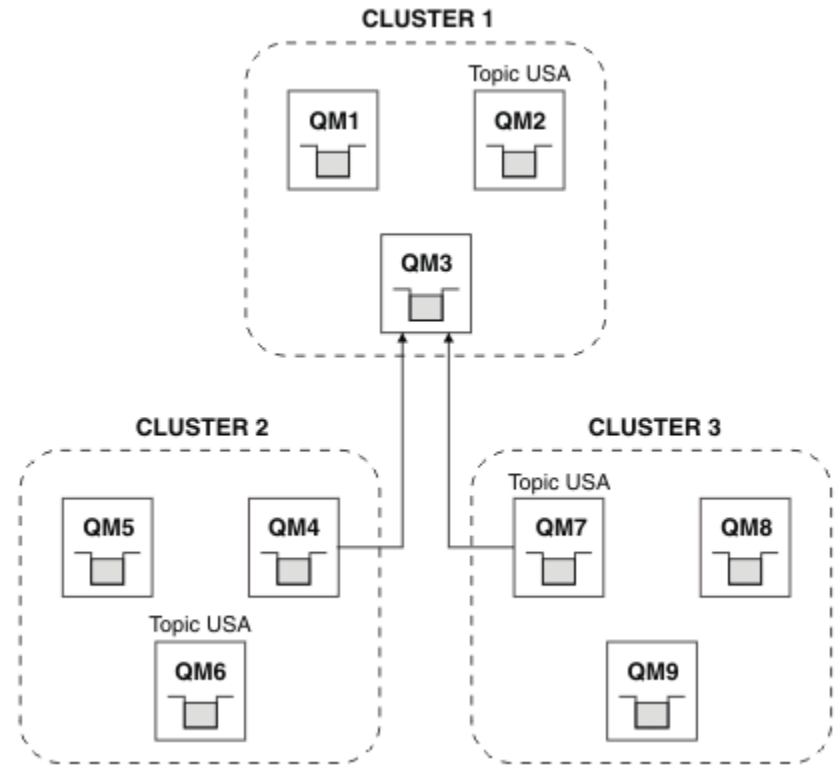


Figura 67. Connessione di cluster mediante gerarchie

La seguente procedura collega i cluster in una gerarchia.

Procedura

1. Creare due serie di canali mittente - ricevente per collegare QM3 e QM4, e QM3 e QM7, in entrambe le direzioni. È necessario utilizzare i canali mittente - destinatario tradizionali e le code di trasmissione, piuttosto che un cluster, per collegare una gerarchia.
2. Creare tre code di trasmissione con i nomi dei gestori code di destinazione. Utilizzare gli alias del gestore code se non è possibile utilizzare il nome del gestore code di destinazione come nome della coda di trasmissione per qualche motivo.
3. Configurare le code di trasmissione per attivare i canali mittente.
4. Verificare che **PSMODE** di QM3, QM4 e QM7 sia impostata su ENABLE.
5. Modificare l'attributo **PARENT** di QM4 e QM7 in QM3.
6. Verificare che lo stato della relazione padre - figlio tra i gestori code sia attivo in entrambe le direzioni.
7. Creare l'argomento di gestione USA con l'attributo **CLUSTER** ('CLUSTER 1'), **CLUSTER** ('CLUSTER 2') e **CLUSTER** ('CLUSTER 3') su ognuno dei tre gestori code dell'argomento del cluster nei cluster 1, 2 e 3. L'host argomento del cluster non deve essere un gestore code connesso gerarchicamente.

Operazioni successive

È ora possibile pubblicare o sottoscrivere l'argomento del cluster USA in Figura 67 a pagina 413. Le sottoscrizioni delle pubblicazioni vengono inviate ai publisher e ai sottoscrittori in tutti e tre i cluster.

Si supponga di non aver creato USA come argomento cluster negli altri cluster. Se USA è definito solo su QM7, le pubblicazioni e le sottoscrizioni a USA vengono scambiate tra QM7, QM8, QM9e QM3. I publisher e i sottoscrittori in esecuzione su QM7, QM8, QM9 ereditano gli attributi dell'argomento di gestione USA. I publisher e i sottoscrittori su QM3 ereditano gli attributi di SYSTEM.BASE.TOPIC su QM3.

Vedi anche “Combinazione e isolamento di spazi argomento in più cluster” a pagina 414.

Concetti correlati

Reti di pubblicazione / sottoscrizione distribuite

Spazi argomento

Attività correlate

Creazione di un singolo spazio argomento in un cluster di pubblicazione / sottoscrizione
Ridimensionare un sistema di pubblicazione / sottoscrizione per l'esecuzione su più gestori code. Utilizzare un cluster di pubblicazione / sottoscrizione per fornire a ciascun publisher e sottoscrittore un singolo spazio argomenti identico.

Aggiunta di un gestore code IBM WebSphere MQ 7 o successivo agli spazi argomento IBM WebSphere MQ 6 esistenti
Estendere un sistema di pubblicazione / sottoscrizione IBM WebSphere MQ 6 esistente per interagire con un gestore code IBM WebSphere MQ 7 o successivo, condividendo gli stessi spazi argomento.

Combinazione e isolamento di spazi argomento in più cluster
Isolare alcuni spazi argomento in un cluster specifico e combinare altri spazi argomento per renderli accessibili in tutti i cluster connessi.

Pubblicazione e sottoscrizione di spazi argomento in più cluster
Pubblicare e sottoscrivere argomenti in più cluster utilizzando cluster sovrapposti. È possibile utilizzare questa tecnica purché gli spazi argomento nei cluster non si sovrappongano.

Definizione degli argomenti del cluster

Combinazione e isolamento di spazi argomento in più cluster

Isolare alcuni spazi argomento in un cluster specifico e combinare altri spazi argomento per renderli accessibili in tutti i cluster connessi.

Prima di iniziare

Esaminare l'argomento “Combinazione degli spazi argomento di più cluster” a pagina 412. Potrebbe essere sufficiente per le tue esigenze, senza aggiungere un ulteriore gestore code come bridge.

Nota: È possibile completare questa attività solo utilizzando cluster di pubblicazione / sottoscrizione instradati diretti. Non è possibile eseguire questa operazione utilizzando i cluster instradati dell'host argomento.

Informazioni su questa attività

Un potenziale miglioramento nella topologia mostrata in Figura 67 a pagina 413 in “Combinazione degli spazi argomento di più cluster” a pagina 412 è quello di isolare gli argomenti del cluster che non sono condivisi tra tutti i cluster. Isolare i cluster creando un gestore code di collegamento che non si trova in nessuno dei cluster; consultare Figura 68 a pagina 415. Utilizzare il gestore code di collegamento per filtrare le pubblicazioni e le sottoscrizioni che possono passare da un cluster all'altro.

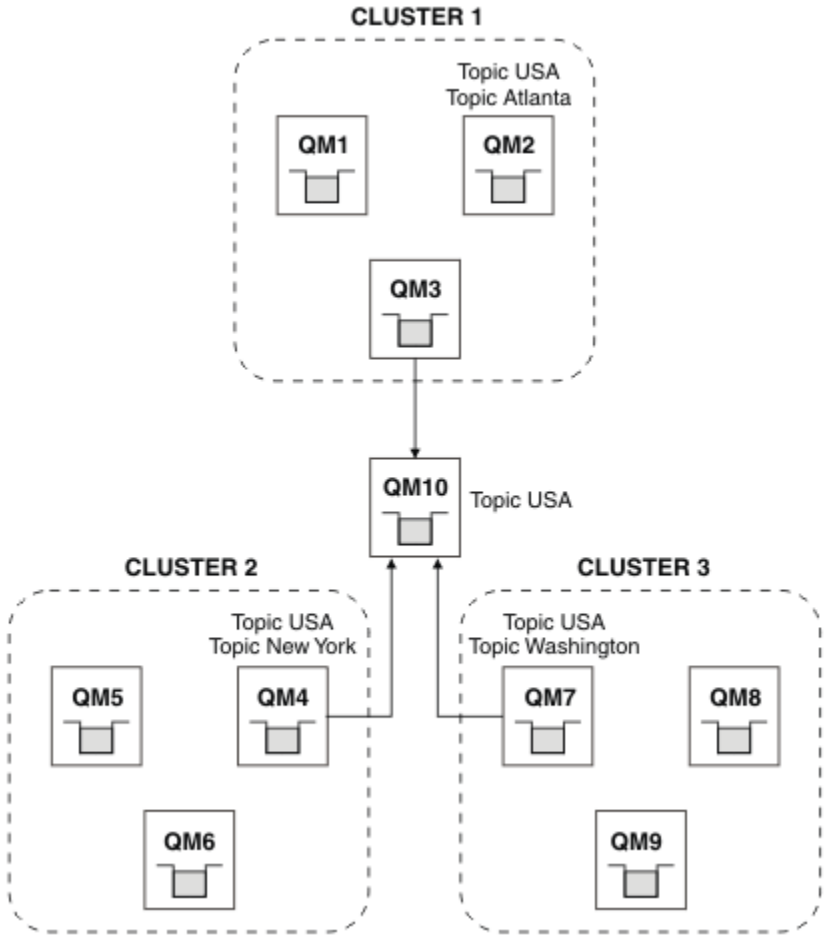


Figura 68. Cluster con bridge

Utilizzare il bridge per isolare gli argomenti del cluster che non si desidera vengano esposti attraverso il bridge sugli altri cluster. In Figura 68 a pagina 415, USA è un argomento cluster condiviso in tutti i cluster e `Atlanta`, `New York` e `Washington` sono argomenti cluster condivisi solo in un cluster ciascuno.

Modellare la propria configurazione utilizzando la seguente procedura:

Procedura

1. Modificare tutti gli oggetti dell'argomento `SYSTEM.BASE.TOPIC` in **SUBSCOPE** (`QMGR`) e **PUBSCOPE** (`QMGR`) su tutti i gestori code.

   Nessun argomento (anche argomenti cluster) viene propagato ad altri gestori code a meno che non si imposti esplicitamente **SUBSCOPE** (`ALL`) e **PUBSCOPE** (`ALL`) sull'argomento root degli argomenti del tuo cluster.
2. Definire gli argomenti sui tre gestori code dell'host del cluster che si desidera condividere in ciascun cluster con gli attributi **CLUSTER** (*clustername*), **SUBSCOPE** (`ALL`) e **PUBSCOPE** (`ALL`).

   Se si desidera che alcuni argomenti del cluster vengano condivisi tra tutti i cluster, definire lo stesso argomento in ciascuno dei cluster. Utilizzare il nome cluster di ciascun cluster come attributo cluster.
3. Per gli argomenti cluster che si desidera condividere tra tutti i cluster, definire di nuovo gli argomenti sul gestore code bridge (`QM10`), con gli attributi **SUBSCOPE** (`ALL`) e **PUBSCOPE** (`ALL`).

Esempio

Nell'esempio in Figura 68 a pagina 415, solo gli argomenti che ereditano da USA si propagano tra tutti i tre cluster.

Operazioni successive

Sottoscrizioni per argomenti definiti sul gestore code del bridge con **SUBSCOPE** (ALL) e **PUBSCOPE** (ALL) sono propagati tra i cluster.

Sottoscrizioni per argomenti definiti all'interno di ciascun cluster con attributi **CLUSTER** (*clustername*), **SUBSCOPE** (ALL) e **PUBSCOPE** (ALL) vengono propagati all'interno di ciascun cluster.

Le altre sottoscrizioni sono locali per un gestore code.

Concetti correlati

Reti di pubblicazione / sottoscrizione distribuite

Spazi argomento

Ambito della pubblicazione

Ambito della sottoscrizione

Attività correlate

Creazione di un singolo spazio argomento in un cluster di pubblicazione / sottoscrizione
Ridimensionare un sistema di pubblicazione / sottoscrizione per l'esecuzione su più gestori code. Utilizzare un cluster di pubblicazione / sottoscrizione per fornire a ciascun publisher e sottoscrittore un singolo spazio argomenti identico.

Aggiunta di un gestore code IBM WebSphere MQ 7 o successivo agli spazi argomento IBM WebSphere MQ 6 esistenti
Estendere un sistema di pubblicazione / sottoscrizione IBM WebSphere MQ 6 esistente per interagire con un gestore code IBM WebSphere MQ 7 o successivo, condividendo gli stessi spazi argomento.

Combinazione degli spazi argomento di più cluster
Creare spazi argomento che si estendono su più cluster. Pubblicare in un argomento in un cluster e sottoscriverlo in un'altro.

Pubblicazione e sottoscrizione di spazi argomento in più cluster
Pubblicare e sottoscrivere argomenti in più cluster utilizzando cluster sovrapposti. È possibile utilizzare questa tecnica purché gli spazi argomento nei cluster non si sovrappongano.

Definizione degli argomenti del cluster

Pubblicazione e sottoscrizione di spazi argomento in più cluster

Pubblicare e sottoscrivere argomenti in più cluster utilizzando cluster sovrapposti. È possibile utilizzare questa tecnica purché gli spazi argomento nei cluster non si sovrappongano.

Prima di iniziare

Creare più cluster tradizionali con alcuni gestori code nelle intersezioni tra i cluster.

Informazioni su questa attività

È possibile che si sia scelto di sovrapporre i cluster per diversi motivi.

1. Si dispone di un numero limitato di server ad alta disponibilità o di gestori code. Si decide di distribuire tutti i repository del cluster e gli host degli argomenti del cluster.
2. Si dispone di cluster di gestori code tradizionali esistenti connessi mediante gestori code gateway. Si desidera distribuire le applicazioni di pubblicazione / sottoscrizione alla stessa topologia cluster.
3. Si dispone di diverse applicazioni di pubblicazione / sottoscrizione autonome. Per motivi di prestazioni, è preferibile mantenere i cluster di pubblicazione / sottoscrizione piccoli e separati dai cluster tradizionali. Si è deciso di distribuire le applicazioni a cluster differenti. Tuttavia, si desidera monitorare anche tutte le applicazioni di pubblicazione / sottoscrizione su un gestore code, poiché si dispone di una sola copia dell'applicazione di controllo. Questo gestore code deve avere accesso alle pubblicazioni per raggruppare gli argomenti in tutti i cluster.

Assicurando che gli argomenti siano definiti in spazi argomento non sovrapposti, è possibile distribuire gli argomenti in cluster di pubblicazione / sottoscrizione sovrapposti, consultare Figura 69 a pagina 417. Se gli spazi argomento si sovrappongono, la distribuzione ai cluster che si sovrappongono causa problemi.

Poiché i cluster di pubblicazione / sottoscrizione si sovrappongono, è possibile pubblicare e sottoscrivere uno qualsiasi degli spazi argomento utilizzando i gestori code nella sovrapposizione.

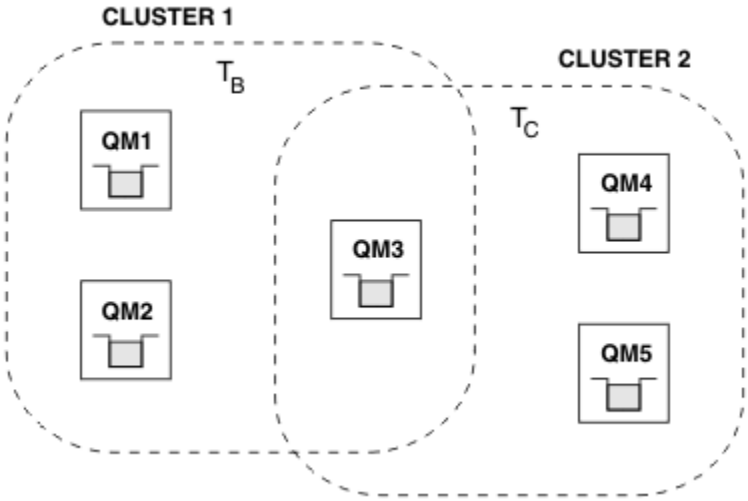


Figura 69. Cluster sovrapposti, spazi argomento non sovrapposti

Procedura

Creare un mezzo per garantire che gli spazi argomento non si sovrappongano.

Ad esempio, definire un argomento root univoco per ciascuno degli spazi argomento. Creare gli argomenti del cluster degli argomenti root.

a) `DEFINE TOPIC(B) TOPICSTR('B') CLUSTER('CLUSTER 1') ...`

b) `DEFINE TOPIC(C) TOPICSTR('C') CLUSTER('CLUSTER 2') ...`

Esempio

In Figura 69 a pagina 417 i publisher e i sottoscrittori collegati a QM3 possono pubblicare o sottoscrivere T_B o T_C

Operazioni successive

Connettere i publisher e i sottoscrittori che utilizzano argomenti in entrambi i cluster ai gestori code nella sovrapposizione.

Connettere i publisher e i sottoscrittori che devono utilizzare solo argomenti in un cluster specifico ai gestori code che non si sovrappongono.

Concetti correlati

Reti di pubblicazione / sottoscrizione distribuite

Spazi argomento

Attività correlate

Creazione di un singolo spazio argomento in un cluster di pubblicazione / sottoscrizione
Ridimensionare un sistema di pubblicazione / sottoscrizione per l'esecuzione su più gestori code.
Utilizzare un cluster di pubblicazione / sottoscrizione per fornire a ciascun publisher e sottoscrittore un singolo spazio argomenti identico.

Aggiunta di un gestore code IBM WebSphere MQ 7 o successivo agli spazi argomento IBM WebSphere MQ 6 esistenti
Estendere un sistema di pubblicazione / sottoscrizione IBM WebSphere MQ 6 esistente per interagire con un gestore code IBM WebSphere MQ 7 o successivo, condividendo gli stessi spazi argomento.

Combinazione degli spazi argomento di più cluster

Creare spazi argomento che si estendono su più cluster. Pubblicare in un argomento in un cluster e sottoscriverlo in un'altro.

Combinazione e isolamento di spazi argomento in più cluster
Isolare alcuni spazi argomento in un cluster specifico e combinare altri spazi argomento per renderli accessibili in tutti i cluster connessi.

Definizione degli argomenti del cluster

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

Si connette il gestore code secondario al gestore code principale nella gerarchia. Se il gestore code child è già un membro di un'altra gerarchia o cluster, questa connessione unisce le gerarchie o unisce il cluster alla gerarchia.

Prima di iniziare

1. I gestori code in una gerarchia di pubblicazione / sottoscrizione devono avere nomi gestore code univoci.
2. Una gerarchia di pubblicazione / sottoscrizione si basa sulla funzionalità del gestore code "pubblicazione / sottoscrizione accodata" . Deve essere abilitato sia sul gestore code principale che su quello secondario. Consultare “Avvio della pubblicazione / sottoscrizione accodata” a pagina 398.
3. La relazione di pubblicazione / sottoscrizione si basa sui canali mittente e destinatario del gestore code. Ci sono due modi per stabilire i canali:
   - Aggiungere i gestori code parent e child a un cluster IBM MQ . Consultare “Aggiunta di un gestore code a un cluster” a pagina 299.
   - Stabilire una coppia di canali mittente / ricevente dal gestore code child al parent e dal parent al child. Ciascun canale deve utilizzare una coda di trasmissione con lo stesso nome del gestore code di destinazione o un alias del gestore code con lo stesso nome del gestore code di destinazione. Per ulteriori informazioni su come stabilire una connessione del canale point-to-point, consultare “Tecniche di accodamento distribuito IBM MQ” a pagina 177.

   Per esempi che configurano una gerarchia su ciascun tipo di configurazione del canale, consultare la seguente serie di scenari della gerarchia di pubblicazione / sottoscrizione:
   - Scenario 1: utilizzo di canali point - to - point con alias del nome gestore code
   - Scenario 2: utilizzo di canali point-to-point con lo stesso nome per la coda di trasmissione e il gestore code remoto
   - Scenario 3: utilizzo di un canale cluster per aggiungere un gestore code

Informazioni su questa attività

Utilizzare il comando ALTER QMGR PARENT (*PARENT_NAME*) **runmqsc** per collegare i figli ai padri. Questa configurazione viene eseguita sul gestore code child, dove *PARENT_NAME* è il nome del gestore code parent.

Procedura

ALTER QMGR PARENT (*PARENT_NAME*)

Esempio

Il primo esempio mostra come collegare il gestore code QM2 come elemento secondario di QM1, quindi interrogare QM2 per confermare che è diventato un elemento secondario con **STATUS** ACTIVE:

```
C:>runmqsc QM2
5724-H72 (C) Copyright IBM Corp. 1994, 2024.  ALL RIGHTS RESERVED.
```

```
Starting MQSC for queue manager QM2
alter qmgr parent(QM1)
     1 : alter qmgr parent(QM1)
AMQ8005: IBM MQ queue manager changed.
display pubsub all
     2 : display pubsub all
AMQ8723: Display pub/sub status details.
   QMNAME(QM2)                             TYPE(LOCAL)
   STATUS(ACTIVE)
AMQ8723: Display pub/sub status details.
   QMNAME(QM1)                             TYPE(PARENT)
STATUS(ACTIVE)
```

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)
```

Se **STATUS** non viene visualizzato come ATTIVO, verificare che i canali tra l'elemento child e l'elemento parent siano correttamente configurati e in esecuzione. Controllare entrambi i log degli errori del gestore code per eventuali errori.

Operazioni successive

Per impostazione predefinita, gli argomenti utilizzati dai publisher e dai sottoscrittori su un gestore code vengono condivisi con i publisher e con i sottoscrittori sugli altri gestori code nella gerarchia. Gli argomenti gestiti possono essere configurati per controllare il livello di condivisione tramite l'utilizzo delle proprietà degli argomenti **SUBSCOPE** e **PUBSCOPE** . Consultare “Configurazione delle reti di pubblicazione / sottoscrizione distribuite” a pagina 401.

Concetti correlati

Combinazione di ambiti di pubblicazione e sottoscrizione
Da IBM WebSphere MQ 7.0 in poi, la pubblicazione e l'ambito della sottoscrizione funzionano in modo indipendente per determinare il flusso di pubblicazioni tra i gestori code.

Combinazione di spazi argomento nelle reti di pubblicazione / sottoscrizione
Combinare lo spazio argomenti di un gestore code con altri gestori code in una gerarchia o in un cluster di pubblicazione / sottoscrizione. Combinare cluster di pubblicazione / sottoscrizione e cluster di pubblicazione / sottoscrizione con le gerarchie.

Stream e argomenti

Pubblicazione/sottoscrizione della messaggistica

Attività correlate

Configurazione di un cluster di pubblicazione / sottoscrizione
Definire un argomento su un gestore code. Per rendere l'argomento un argomento cluster, impostare la proprietà **CLUSTER** . Per scegliere l'instradamento da utilizzare per pubblicazioni e sottoscrizioni per questo argomento, impostare la proprietà **CLROUTE** .

Spostamento di una definizione di argomento del raggruppamento in un gestore code differente
Per l'host argomento instradato o i cluster instradati direttamente, potrebbe essere necessario spostare una definizione dell'argomento del cluster durante la disattivazione di un gestore code o perché un gestore code del cluster ha riportato un errore o non è disponibile per un periodo di tempo significativo.

Aggiunta di ulteriori host argomento a un cluster instradato di host argomento
In un cluster di pubblicazione / sottoscrizione instradato dall'host argomento, è possibile utilizzare più gestori code per instradare le pubblicazioni alle sottoscrizioni definendo lo stesso oggetto argomento in cluster su tali gestori code. Può essere utilizzato per migliorare la disponibilità e il bilanciamento del carico di lavoro. Quando si aggiunge un host argomento supplementare per lo stesso oggetto argomento

cluster, è possibile utilizzare il parametro **PUB** per controllare quando le pubblicazioni iniziano ad essere instradate attraverso il nuovo host argomento.

Disconnessione di un gestore code da una gerarchia di pubblicazione / sottoscrizione
Disconnettere un gestore code secondario da un gestore code principale in una gerarchia di pubblicazione / sottoscrizione.

Riferimenti correlati
VISUALIZZA PUBSUB

Disconnessione di un gestore code da una gerarchia di pubblicazione / sottoscrizione

Disconnettere un gestore code secondario da un gestore code principale in una gerarchia di pubblicazione / sottoscrizione.

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: IBM MQ queue manager changed.
    2 : display pubsub type(child)
AMQ8147: IBM MQ object  not found.
display pubsub type(parent)
    3 : display pubsub type(parent)
AMQ8147: IBM MQ object not found.
```

Operazioni successive

È possibile eliminare tutti i flussi, le code e i canali definiti manualmente che non sono più necessari.

Concetti correlati

Combinazione di ambiti di pubblicazione e sottoscrizione
Da IBM WebSphere MQ 7.0 in poi, la pubblicazione e l'ambito della sottoscrizione funzionano in modo indipendente per determinare il flusso di pubblicazioni tra i gestori code.

Combinazione di spazi argomento nelle reti di pubblicazione / sottoscrizione
Combinare lo spazio argomenti di un gestore code con altri gestori code in una gerarchia o in un cluster di pubblicazione / sottoscrizione. Combinare cluster di pubblicazione / sottoscrizione e cluster di pubblicazione / sottoscrizione con le gerarchie.

Attività correlate

Configurazione di un cluster di pubblicazione / sottoscrizione
Definire un argomento su un gestore code. Per rendere l'argomento un argomento cluster, impostare la proprietà **CLUSTER** . Per scegliere l'instradamento da utilizzare per pubblicazioni e sottoscrizioni per questo argomento, impostare la proprietà **CLROUTE** .

Spostamento di una definizione di argomento del raggruppamento in un gestore code differente

Per l'host argomento instradato o i cluster instradati direttamente, potrebbe essere necessario spostare una definizione dell'argomento del cluster durante la disattivazione di un gestore code o perché un gestore code del cluster ha riportato un errore o non è disponibile per un periodo di tempo significativo.

Aggiunta di ulteriori host argomento a un cluster instradato di host argomento
In un cluster di pubblicazione / sottoscrizione instradato dall'host argomento, è possibile utilizzare più gestori code per instradare le pubblicazioni alle sottoscrizioni definendo lo stesso oggetto argomento in cluster su tali gestori code. Può essere utilizzato per migliorare la disponibilità e il bilanciamento del carico di lavoro. Quando si aggiunge un host argomento supplementare per lo stesso oggetto argomento cluster, è possibile utilizzare il parametro **PUB** per controllare quando le pubblicazioni iniziano ad essere instradate attraverso il nuovo host argomento.

Connessione di un gestore code a una gerarchia di pubblicazione / sottoscrizione
Si connette il gestore code secondario al gestore code principale nella gerarchia. Se il gestore code child è già un membro di un'altra gerarchia o cluster, questa connessione unisce le gerarchie o unisce il cluster alla gerarchia.

ULW Configurazione di più installazioni

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

Informazioni su questa attività

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

Procedura

- Utilizzare le informazioni contenute nei seguenti collegamenti per configurare le installazioni:
  - “Modifica dell'installazione primaria” a pagina 430
  - “Associazione di un gestore code a un'installazione” a pagina 432
  - “Connessione di applicazioni in un ambiente di installazione multiplo” a pagina 421

ULW Connessione di applicazioni in un ambiente di installazione multiplo

Sui sistemi UNIX, Linux, and Windows , se IBM WebSphere MQ 7.1, o versioni successive, vengono caricate le librerie, IBM MQ utilizza automaticamente le librerie appropriate senza che sia necessario intraprendere ulteriori operazioni. IBM MQ utilizza le librerie dell'installazione associate con il 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 MQ:

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

Caricamento
Quando l'applicazione viene eseguita, le librerie IBM 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 delle librerie IBM MQ” a pagina 423.

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

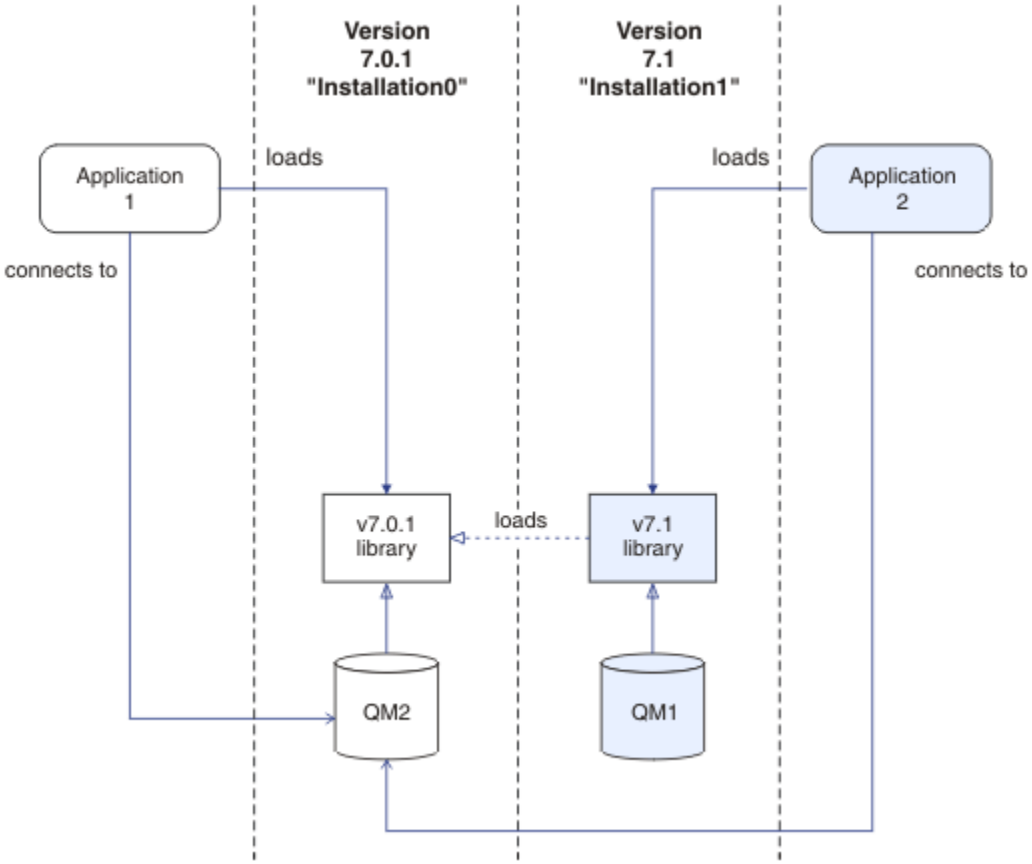


Figura 70. Connessione di applicazioni in un ambiente di installazione multiplo

Ad esempio, Figura 70 a pagina 422 mostra un ambiente di installazione multiplo con un'installazione IBM WebSphere MQ 7.0.1 (`Installation0`) e un'installazione IBM WebSphere MQ 7.1 (`Installation1`). Due applicazioni sono collegate a queste installazioni, ma caricano versioni di librerie differenti.

`Application 1` carica direttamente una libreria IBM WebSphere MQ 7.0.1 . Quando `application 1` si collega a `QM2`, vengono utilizzate le librerie IBM WebSphere MQ 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 IBM WebSphere MQ 7.0.1 non è in grado di caricare altre versioni della libreria. In altre parole, se le librerie IBM WebSphere MQ 7.0.1 vengono caricate direttamente, non è possibile utilizzare un gestore code associato a un'installazione in una versione successiva di IBM MQ.

`Application 2` carica direttamente una libreria IBM WebSphere MQ 7.1 . Quando `application 2` si connette a `QM2`, la libreria IBM WebSphere MQ 7.1 carica e utilizza la libreria IBM WebSphere MQ 7.0.1 . Se `application 2` si connette a `QM1`o se `QM2` è associato a `Installation1`, la libreria IBM WebSphere MQ 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, Linux, and Windows.

Per ulteriori informazioni su come caricare le librerie IBM WebSphere MQ 7.1 , consultare “Caricamento delle librerie IBM MQ” a pagina 423.

Supporto e restrizioni

Se una delle seguenti librerie IBM WebSphere MQ 7.1, o successive, viene individuata e caricata, IBM 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 MQ carica e utilizza automaticamente anche 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, consultare “Limitazioni per le applicazioni che utilizzano più installazioni” a pagina 427.

Concetti correlati

“Limitazioni per le applicazioni che utilizzano più installazioni” a pagina 427
Esistono delle 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 multipla.

“Caricamento delle librerie IBM MQ” a pagina 423
Quando si decide come caricare le librerie IBM 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 MQ e se è probabile che l'ubicazione di IBM MQ cambi.

Attività correlate

Scelta di un'installazione primaria

“Modifica dell'installazione primaria” a pagina 430
È possibile utilizzare il comando **setmqinst** per impostare o annullare l'impostazione di un'installazione come installazione primaria.

“Associazione di un gestore code a un'installazione” a pagina 432
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** .

ULW Caricamento delle librerie IBM MQ

Quando si decide come caricare le librerie IBM 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 MQ e se è probabile che l'ubicazione di IBM MQ cambi.

Queste informazioni si applicano alle librerie IBM WebSphere MQ 7.1, o versione successiva.

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

- Sui sistemi UNIX and Linux , se una copia di IBM WebSphere MQ 7.1, o di una versione successiva, è installata nell'ubicazione predefinita, 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 IBM WebSphere MQ 7.1, o una versione successiva, come installazione primaria oppure creare manualmente i collegamenti simbolici.

- Se IBM WebSphere MQ 7.1, o una versione successiva, è installato in un'ubicazione non predefinita, come nel caso in cui anche IBM WebSphere MQ 7.0.1 è installato, potrebbe essere necessario modificare le applicazioni esistenti in modo che vengano caricate le librerie corrette.

Il modo in cui le librerie IBM MQ possono essere ubicate e caricate dipende anche dal modo in cui le applicazioni esistenti sono configurate per caricare le librerie. Per ulteriori informazioni sul modo in cui è possibile caricare le librerie, consultare "Meccanismi di caricamento della libreria del sistema operativo" a pagina 426.

In modo ottimale, verificare che la libreria IBM MQ , caricata dal sistema operativo, sia quella a cui è associato il gestore code.

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

Tabella 29. Vantaggi e svantaggi delle opzioni per il caricamento delle librerie

Piattaforma	Opzione	Vantaggi	Inconvenienti
Linux UNIX SistemiUNIX 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 relative alla compilazione e al collegamento delle applicazioni, consultare Creazione di un'applicazione procedurale.	• L'ambito della modifica è chiaro.	• È necessario essere in grado di ricompilare e collegare l'applicazione. • Se l'ubicazione di IBM MQ cambia, è necessario modificare RPath.

Tabella 29. 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* , utilizzando setmqenvo crtmqenv, con l'opzione **-k** o **-1** . (AIX Su AIX, questa variabile di ambiente è *LIBPATH*	• Non sono richieste modifiche alle applicazioni esistenti. • Sovrascrive RPath integrati in un'applicazione. • È facile modificare la variabile se l'ubicazione di IBM MQ cambia.	• 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*. • 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 .
Windows SistemiWindows	Impostare la variabile PATH utilizzando setmqo crtmqenv.	• Nessuna modifica richiesta per le applicazioni esistenti. • È facile modificare la variabile se l'ubicazione di IBM MQ cambia.	• Specifico dell'ambiente, deve essere impostato in ogni ambiente in cui viene eseguita l'applicazione. • Possibile impatto su altre applicazioni.
ULW SistemiUNIX, Linux, and Windows	Impostare l'installazione primaria su un'installazione IBM WebSphere MQ 7.1o successiva. Consultare “Modifica dell'installazione primaria” a pagina 430. Per ulteriori informazioni sull'installazione primaria, consultare Scelta di un'installazione primaria.	• Nessuna modifica richiesta per le applicazioni esistenti. • Facile modificare l'installazione primaria se l'ubicazione di IBM MQ cambia. • Fornisce un comportamento simile a quello delle precedenti versioni di IBM MQ.	• Quando IBM WebSphere MQ 7.0.1 è installato, non è possibile impostare l'installazione primaria su IBM WebSphere MQ 7.1o su una versione successiva. • Linux UNIX UNIX and Linux: non funziona se `/usr/lib` non è nel percorso di ricerca predefinito.

Considerazioni sul caricamento della libreria per Linux

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

Solaris

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

Meccanismi di caricamento della libreria del sistema operativo

Sui 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.

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

- Utilizzando la variabile d'ambiente *LD_LIBRARY_PATH* (anche *LIBPATH* su AIX). Se questa variabile è impostata, definisce una serie di directory in cui vengono ricercate le librerie IBM 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 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 7.1 nell'ubicazione predefinita o utilizzare un altro metodo per trovare le librerie.
- Viene utilizzato il percorso libreria predefinito. Se le librerie IBM MQ non vengono trovate dopo la ricerca della variabile *LD_LIBRARY_PATH* e delle 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 AIX: **dump**
- Linux Linux: **readelf**
- Solaris Solaris: **elfdump**

Concetti correlati

“Limitazioni per le applicazioni che utilizzano più installazioni” a pagina 427

Esistono delle 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 multipla.

“Connessione di applicazioni in un ambiente di installazione multiplo” a pagina 421
Sui sistemi UNIX, Linux, and Windows , se IBM WebSphere MQ 7.1, o versioni successive, vengono caricate le librerie, IBM MQ utilizza automaticamente le librerie appropriate senza che sia necessario intraprendere ulteriori operazioni. IBM MQ utilizza le librerie dell'installazione associate con il gestore code a cui si connette l'applicazione.

Attività correlate

Scelta di un'installazione primaria

“Modifica dell'installazione primaria” a pagina 430
È possibile utilizzare il comando **setmqinst** per impostare o annullare l'impostazione di un'installazione come installazione primaria.

“Associazione di un gestore code a un'installazione” a pagina 432
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** .

ULW Limitazioni per le applicazioni che utilizzano più installazioni

Esistono delle 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 multipla.

Librerie server CICS

Se si utilizzano le librerie del server CICS , IBM 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, vedi Creazione di librerie da utilizzare con TXSeries for Multiplatforms versione 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 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 strutture MQIEP , non possono utilizzare un RPATH integrato per individuare le librerie IBM MQ e non possono collegarsi alle librerie IBM MQ . Per ulteriori informazioni, vedere Scrittura di uscite e servizi installabili su UNIX, Linux, and Windows .

Accesso rapido

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

1. Il gestore code deve essere associato alla stessa installazione da cui l'applicazione ha caricato le librerie di runtime di IBM 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 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. Una connessione non ad accesso rapido a un gestore code associato a un'installazione di IBM WebSphere MQ 7.1 o successive non ha alcun effetto sul fatto che un'applicazione possa stabilire una connessione ad accesso rapido.
4. Non è possibile combinare la connessione a un gestore code associato a un'installazione di IBM WebSphere MQ 7.0.1 e il percorso rapido a un gestore code associato a un'installazione di IBM WebSphere MQ 7.1o successiva.

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 essere la stessa da cui sono state caricate le librerie di runtime di IBM 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

ULW Connessione di applicazioni di .NET in un ambiente di installazione multiplo

Per impostazione predefinita, le applicazioni utilizzano gli assembly .NET dell'installazione principale. 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 di IBM MQ inferiore alla versione con cui è stata compilata l'applicazione.

Per informazioni su come aggiornare il file di configurazione dell'applicazione, consultare “Connessione delle applicazioni di .NET utilizzando il file di configurazione dell'applicazione” a pagina 429.

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 430.

Connessione delle applicazioni di .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 specifiche modifiche che devono essere apportate al file di configurazione dell'applicazione per permettere alle applicazioni .NET di connettersi utilizzando particolari assembly:

Tabella 30. Configurazione delle applicazioni per l'utilizzo di particolari assembly

	Applicazioni compilate con una versione precedente di IBM MQ	**Applicazioni compilate con una versione successiva di IBM MQ**
Per eseguire un'applicazione con un'installazione primaria IBM MQ di una versione successiva. (assembly di versioni successive in GAC):	Nessuna modifica necessaria	Nessuna modifica necessaria
Per eseguire un'applicazione con un'installazione primaria IBM MQ di una versione precedente. (assembly di versioni precedenti in GAC):	Nessuna modifica necessaria	Nel file di configurazione dell'applicazione: • Utilizzare la tag *bindingRedirect* per indicare l'utilizzo della versione precedente degli assembly presenti in GAC
Per eseguire un'applicazione con una versione successiva di installazione non primaria IBM MQ . (assembly versione successiva nella cartella di installazione):	Nel file di configurazione dell'applicazione: • Utilizzare la tag *codebase* per puntare all'ubicazione degli assembly delle versioni più recenti • Utilizzare la tag *bindingRedirect* per indicare l'utilizzo degli assembly delle versioni più recenti	Nel file di configurazione dell'applicazione: • Utilizzare la tag *codebase* per puntare all'ubicazione degli assembly delle versioni più recenti
Per eseguire un'applicazione con una versione precedente dell'installazione non primaria IBM MQ . (assembly di versioni precedenti nella cartella di installazione):	Nel file di configurazione dell'applicazione: • Utilizzare la tag *codebase* per puntare all'ubicazione degli assembly della versione precedente • Includere la tag *publisherpolicy Apply=no*	Nel file di configurazione dell'applicazione: • Utilizzare la tag *codebase* per puntare all'ubicazione degli assembly della versione precedente • Utilizzare la tag *bindingRedirect* per indicare l'utilizzo degli assembly della versione precedente • Includere la 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 MQ di qualsiasi installazione non primaria. Il file può anche 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. Per ulteriori informazioni su quando utilizzare questa variabile, consultare la documentazione Microsoft appropriata in *DEVPATH* .

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 421
Sui sistemi UNIX, Linux, and Windows , se IBM WebSphere MQ 7.1, o versioni successive, vengono caricate le librerie, IBM MQ utilizza automaticamente le librerie appropriate senza che sia necessario intraprendere ulteriori operazioni. IBM MQ utilizza le librerie dell'installazione associate con il gestore code a cui si connette l'applicazione.

più installazioni

Attività correlate

Scelta di un'installazione primaria

Utilizzo di .NET

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

Windows Durante il processo di installazione su Windows, è possibile specificare che l'installazione deve essere l'installazione primaria.

Linux UNIX Su sistemi UNIX and Linux , è necessario immettere un comando **setmqinst** dopo l'installazione per impostare l'installazione come primaria.

Procedura

- Per impostare un'installazione come installazione primaria, completare la seguente procedura:
  a) 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 7.1 o successiva.
  b) Se un'installazione esistente di IBM WebSphere MQ 7.1 o successiva è impostata come installazione primaria, annullarla prima di continuare con il passo successivo.

  Se IBM WebSphere MQ 7.0.1 è installato sul sistema, l'installazione primaria non può essere modificata.
  c) Assicurarsi di essere collegati con l'autorizzazione appropriata:
  – UNIX Come root su UNIX and Linux.
  – Linux Come membro del gruppo Amministratori su sistemi Windows .
  d) Immettere uno dei comandi seguenti:
  – 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
```

  e) Windows
  Su sistemi Windows , riavviare il sistema.
- Per annullare l'impostazione di un'installazione come installazione primaria, completare la seguente procedura:
  a) 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 7.1 o successiva.

  Se IBM WebSphere MQ 7.0.1 è l'installazione primaria, non è possibile annullare l'impostazione dell'installazione primaria.
  b) Assicurarsi di essere collegati con l'autorizzazione appropriata:
  – UNIX Come root su UNIX and Linux.
  – Linux Come membro del gruppo Amministratori su sistemi Windows .
  c) Immettere uno dei comandi seguenti:
  – 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 and Linux

Attività correlate

Disinstallazione, aggiornamento e manutenzione dell'installazione primaria

Scelta di un nome di installazione

Riferimenti correlati

setmqinst

ULW 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** .

Informazioni su questa attività

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** generalmente deve essere emesso dall'installazione associata al gestore code. Tuttavia, quando un IBM WebSphere MQ 7.0.1 o un gestore code precedente viene avviato su un'installazione IBM WebSphere MQ 7.1 o successiva 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.

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** .

Quando si desidera associare un gestore code a un'installazione, è possibile utilizzare il comando **setmqm** nei seguenti modi:

- Spostamento di singoli gestori code tra versioni equivalenti di IBM 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 IBM MQ a una versione più recente di IBM MQ. La migrazione dei gestori code tra versioni ha diverse implicazioni di cui è necessario essere consapevoli. Per ulteriori informazioni sulla migrazione, consultare Manutenzione e migrazione.

Procedura

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.

Operazioni successive

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 MQ su un sistema” a pagina 433
Se si dispone di più installazioni IBM MQ su un sistema, è possibile verificare quali versioni sono installate e dove si trovano.

“File di configurazione IBM MQ , mqs.ini” a pagina 84
Il file di configurazione IBM 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

addmqinf
dspmq
dspmqinst
endmqm
setmqm
strmqm

ULW Ricerca di installazioni di IBM MQ su un sistema

Se si dispone di più installazioni IBM 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 IBM 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 IBM WebSphere MQ 7.0.1 .
- Utilizzare gli strumenti di installazione della piattaforma per eseguire una query su dove è stato installato IBM MQ . Quindi, utilizzare il comando **dspmqver** da un'installazione IBM WebSphere MQ 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 MQ :
  - AIX Sui sistemi AIX , è possibile utilizzare il comando **lslpp** :

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

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

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

– Solaris 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
```

– Windows 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
```

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

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

Quindi, utilizzare il comando **dspmqver** da un'installazione IBM WebSphere MQ 7.1 o successiva.

- Windows 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
```

- Windows Su Windowsa 64 bit, immettere il seguente comando:

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

Il comando **reg.exe** visualizza solo le informazioni per le installazioni IBM WebSphere MQ 7.1 o successive.

Concetti correlati
più installazioni
Riferimenti correlati
dspmqver
dspmqinst

Configurazione dell'alta disponibilità, ripristino e riavvio

È possibile rendere le applicazioni altamente disponibili mantenendo la disponibilità della coda in caso di errore di un gestore code e ripristinando i messaggi dopo un errore del server o della memoria.

Informazioni su questa attività

z/OS Su z/OS, l'alta disponibilità è integrata nella piattaforma. È inoltre possibile migliorare la disponibilità delle applicazioni del server utilizzando i gruppi di condivisione code. Vedere Code condivise e gruppi di condivisione code.

Multi Su Multipiattaforme, è possibile migliorare la disponibilità delle applicazioni client utilizzando la riconnessione client per commutare automaticamente un client tra un gruppo di gestori code o alla nuova istanza attiva di un gestore code a più istanze dopo un malfunzionamento del gestore code. La riconnessione automatica del client non è supportata da IBM MQ classes for Java. Un gestore code a più istanze è configurato per essere eseguito come singolo gestore code su più server. Le applicazioni server vengono distribuite a questo gestore code. 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 differente. 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.

Un altro modo per aumentare la disponibilità delle applicazioni server su Multiplatforms è quello di distribuire le applicazioni server a più computer in un cluster di gestori code. Da IBM WebSphere MQ 7.1 in poi, il ripristino da errori del cluster riesegui le operazioni che hanno causato problemi fino a quando i problemi non vengono risolti. Consultare Modifiche al ripristino da errori cluster su server diversi da z/OS. È anche possibile configurare IBM MQ for Multiplatforms come parte di una soluzione di clustering specifica della piattaforma, ad esempio:

- Microsoft Server cluster
- IBM i Cluster HA su IBM i
- Linux UNIX PowerHA per AIX (precedentemente HACMP su AIX) e altre soluzioni di clustering UNIX and Linux

Linux Su sistemi Linux , è possibile configurare i gestori code di dati replicati (RDQM) per implementare soluzioni di alta disponibilità o di ripristino di emergenza. Per l'alta disponibilità, le istanze dello stesso gestore code sono configurate su ciascun nodo in un gruppo di tre server Linux . Una delle tre istanze è l'istanza attiva. I dati del gestore code attivo vengono replicati in modo sincrono nelle altre due istanze, quindi una di queste istanze può assumere il controllo in caso di errore. Per il ripristino di emergenza, un gestore code viene eseguito su un nodo primario su un sito, con un'istanza secondaria di tale gestore code ubicata su un nodo di ripristino su un sito differente. I dati vengono replicati tra l'istanza primaria e l'istanza secondaria, e se il nodo primario viene perso per qualche motivo, l'istanza secondaria può essere creata nell'istanza primaria e avviata.

MQ Appliance Un'altra opzione per una soluzione di ripristino di emergenza o alta disponibilità è quella di distribuire una coppia di dispositivi IBM MQ . Vedi High Availability e Disaster Recovery nella documentazione di IBM MQ Appliance .

Un sistema di messaggistica garantisce che i messaggi immessi nel sistema vengano consegnati alla loro destinazione. IBM 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. IBM MQ conserva i log di recupero 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 recupero*, quando si arresta IBM MQ in modo pianificato.
2. *Ripristino da errore*, quando un errore si arresta IBM 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.

Avvertenza: Non è possibile spostare i log di ripristino su un sistema operativo differente.

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 l'applicazione client per ricreare una connessione utilizzando `MQCONN` o `MQCONNX` e riaprire gli oggetti. La riconnessione automatica del client è adatta a molte ma non a tutte le applicazioni client.

Tabella 31 a pagina 437 elenca il primo release del supporto client IBM 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 32 a pagina 437 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 nonJMS , 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 gestore code di dati replicati o un gestore code HA su IBM MQ Appliance, è possibile specificare un indirizzo IP mobile utilizzato sia dai gestori code attivi che da quelli in standby per semplificare la configurazione.
- Per un client JMS , impostare le opzioni di riconnessione nella configurazione della produzione connessioni. Durante l'esecuzione nel contenitore EJB di un server Java EE , gli MDB possono riconnettersi a IBM MQ utilizzando il meccanismo di riconnessione fornito dalle specifiche di attivazione dell'adattatore di risorse IBM MQ (o le porte listener se in esecuzione in WebSphere Application Server). Tuttavia, se l'applicazione non è un MDB (o è in esecuzione nel contenitore Web), l'applicazione deve implementare la propria logica di riconnessione poiché la riconnessione automatica del client non è supportata in questo scenario. L'adattatore di risorse IBM MQ fornisce questa capacità di riconnessione per la consegna dei messaggi ai bean basati sui messaggi, ma altri elementi Java EE come i servlet devono implementare la propria riconnessione.

Nota: La riconnessione automatica del client non è supportata da IBM MQ classes for Java.

Tabella 31. 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 on 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
	IBM MQ classes for Java	Non supportato	Non supportato
	Client XMS e .NET gestiti: C#, Visual Basic,	7.1	7.1
Altre API	Windows Communication Foundation ([1](#) non gestito)	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 32. Requisiti di configurazione della riconnessione automatica		
Componente	**Requisito**	**Effetto del mancato rispetto dei requisiti**
IBM MQ MQI client installazione	Vedere Tabella 31 a pagina 437	`MQRC_OPTIONS_ERROR`
IBM MQ Installazione server	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`** del factory di connessione.	`MQCC_FAILED` quando una connessione è interrotta o il gestore code termina o non riesce.

La Figura 71 a pagina 438 mostra le interazioni principali tra i componenti coinvolti nella riconnessione client.

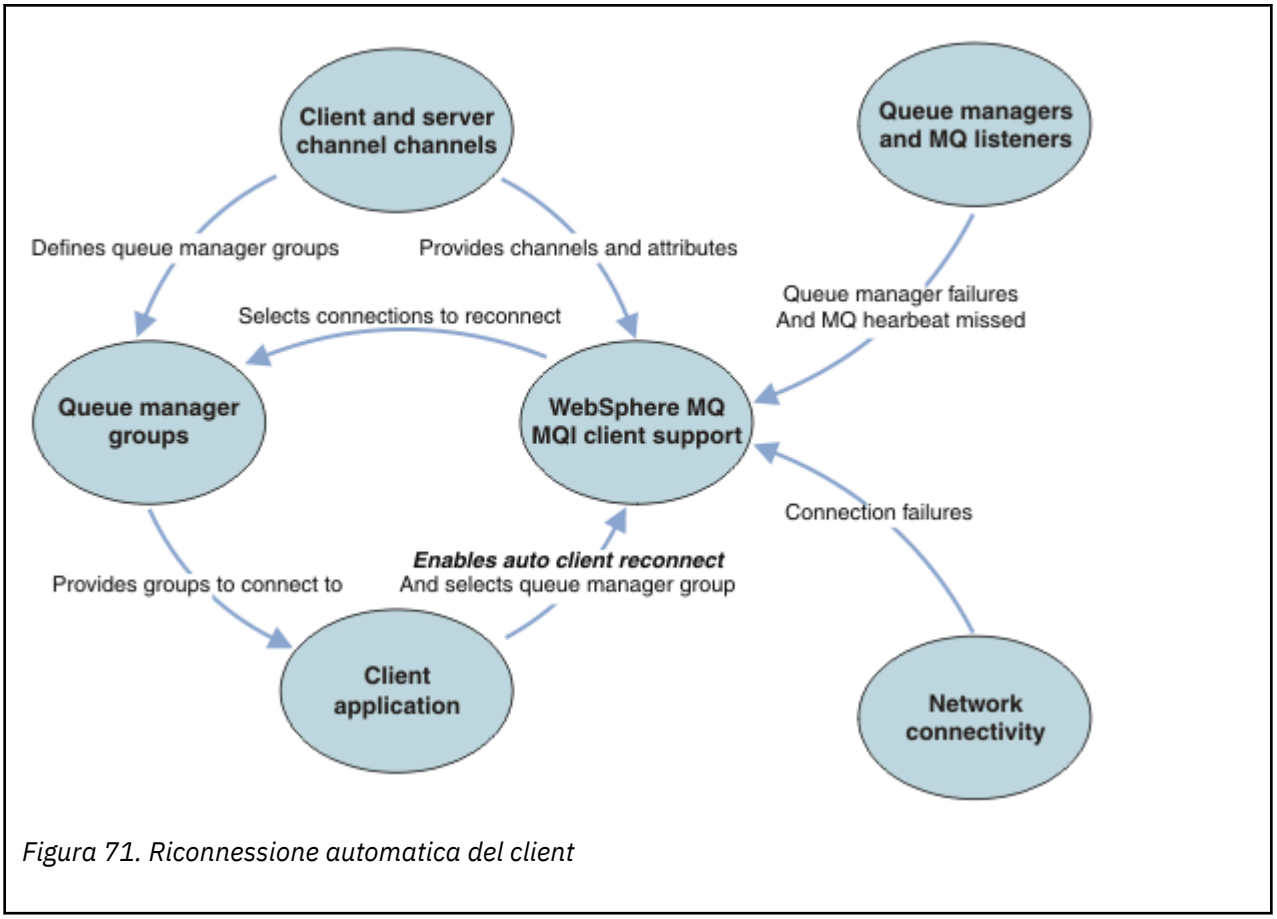


Figura 71. Riconnessione automatica del client

Applicazione client

L'applicazione client è un IBM MQ MQI client. Per dettagli sulla riconnessione automatica del client per un client JMS, consultare Utilizzo della riconnessione automatica del client JMS.

- 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 524.
- 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 ad alta disponibilità

I gestori code ad alta disponibilità hanno un'istanza attiva e una o più istanze in standby di un gestore code. Il gestore code attivo è sincronizzato con i gestori code in standby, in modo che uno standby possa eseguire automaticamente il takeover se l'istanza attiva ha esito negativo. Esistono diverse soluzioni per fornire gestori code ad elevata disponibilità, consultare “Configurazioni HA (High Availability)” a pagina 446.

È possibile semplificare il riavvio delle applicazioni IBM MQ MQI client , dopo che un gestore code ad alta disponibilità ha attivato la propria istanza in standby, utilizzando la riconnessione client automatica.

L'istanza in standby di un gestore code ad alta disponibilità è in genere a un indirizzo di rete differente 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. I gestori code di dati replicati e i gestori code ad alta disponibilità di IBM MQ Appliance supportano gli indirizzi IP mobili, dove si specifica un singolo indirizzo da utilizzare con i gestori code attivi o in standby.

Gruppi gestore code

In genere, IBM MQ MQI clients si riconnette a qualsiasi gestore code in un gruppo di gestori code. A volte si desidera che un IBM MQ MQI client si riconnette solo allo stesso gestore code. Potrebbe avere un'affinità con un 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 del nome 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.

È possibile evitare che un client si riconnette a un gestore code differente. Impostare l'opzione MQCNO , MQCNO_RECONNECT_Q_MGR. IBM MQ MQI client 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 di condivisione code

z/OS 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.

z/OS 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.

z/OS Notare che KAINT si applica solo a z/OS .

KAINT è un heartbeat a livello di rete e HBINT è un heartbeat IBM MQ tra client e 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 a IBM MQ MQI client dalla rete vengono gestiti dalla funzionalità di riconnessione automatica del client.

- Le riconnessioni eseguite automaticamente dal trasporto sono invisibili a IBM MQ.
- L'impostazione HBINT consente di gestire gli errori di rete invisibili a IBM MQ.

Gestori code e listener IBM 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.
- L'arresto di un gestore code utilizzando il comando **endmqm** predefinito non attiva la riconnessione automatica del client. 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.

IBM MQ MQI client supporto di riconnessione automatica

Se si utilizza il supporto di riconnessione client automatica in IBM MQ MQI client, 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
  - Chiusura di un gestore code e specifica dell'opzione `-r`, riconnessione, nel 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 526.
- 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.

Anche se il tempo di riconnessione previsto non è superiore a un minuto, la riconnessione può richiedere più tempo perché un gestore code potrebbe avere numerose risorse da gestire. Durante questo periodo, un'applicazione client potrebbe mantenere dei blocchi che non appartengono alle risorse IBM 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` .

Concetti correlati

Client riconnettibili

Attività correlate

Arresto di un gestore code

z/OS Monitoraggio dei messaggi della console

Su IBM MQ for z/OS, esistono diversi messaggi informativi emessi dal gestore code o dall'iniziatore del canale che dovrebbero essere considerati particolarmente significativi. Questi messaggi non indicano di per sé un problema, ma possono essere utili nella traccia perché indicano un potenziale problema che potrebbe essere necessario risolvere.

La presenza di questi messaggi della console potrebbe anche indicare che un'applicazione utente sta inserendo un numero elevato di messaggi nella serie di pagine, il 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 esegue il GET dei messaggi dalla coda non funziona più.

Messaggi della console da monitorare

Il seguente elenco delinea i messaggi che possono potenzialmente indicare problemi più grandi. Determinare se è necessario tenere traccia di questi messaggi con l'automazione del sistema e fornire la documentazione appropriata in modo che i potenziali problemi possano essere seguiti in modo efficace.

CSQI004I: *csect - name* CONSIDERARE L'INDICIZZAZIONE *nome - coda* BY *tipo - indice* FOR *tipo - connessione* CONNECTION *nome - connessione*, *num-msgs* MESSAGES SKIPPED

- Il gestore code ha rilevato un'applicazione che riceve i messaggi in base all'ID messaggio o all'ID correlazione da una coda che non ha un indice definito.
- Considerare di stabilire un indice per la coda identificata modificando l'oggetto coda locale, *nome - coda*, attributo INDXTYPE per avere il valore *tipo - indice*.

CSQI031I: *nome - csect* LA NUOVA ESTENSIONE DELLA SERIE DI PAGINE *psid* HA FORMATTATO CORRETTAMENTE

- Controllare la profondità corrente delle code assegnate a questa serie di pagine.
- Esaminare la causa dell'errore di elaborazione dei messaggi.

.

CSQI041I: *csect - name* JOB *nomelavoro* USER *idutente* HAD ERROR ACCEDERE ALLA SERIE DI PAGINE *psid*

- Determinare se la serie di pagine è assegnata al gestore code.
- Immettere un comando **DISPLAY USAGE** per determinare lo stato della serie di pagine.
- Controllare la registrazione lavori del gestore code per ulteriori messaggi di errori.

.

CSQI045I: *csect - name* Log RBA ha raggiunto *rba*. Pianificare una reimpostazione del log

- Pianificare l'arresto del gestore code in un momento opportuno e reimpostare i log.

- Se il gestore code utilizza RBA di log a 6 byte, considerare la possibilità di convertire il gestore code in RBA di log a 8 byte.

CSQI046E: *csect - name* Log RBA ha raggiunto *rba*. Eseguire una reimpostazione del log

- Pianificare l'arresto del gestore code in un momento opportuno e reimpostare i log.
- Se il gestore code utilizza RBA di log a 6 byte, considerare la possibilità di convertire il gestore code in RBA di log a 8 byte.

CSQI047E: *csect - name* Log RBA ha raggiunto *rba*. Arrestare il gestore code e reimpostare i log

- Arrestare immediatamente il gestore code e reimpostare i log.
- Se il gestore code utilizza RBA di log a 6 byte, considerare la possibilità di convertire il gestore code in RBA di log a 8 byte.

CSQJ004I: ACTIVE LOG COPY *n* INACTIVE, LOG IN SINGLE MODE, ENDRBA= *ttt*

- Il gestore code ha attivato la modalità di registrazione 'singola'. Questo è spesso indicativo di un problema di offload del log.
- Immettere un comando **DISPLAY LOG** per stabilire le impostazioni per il duplex dei log attivi e di archiviazione. Questo pannello mostra anche il numero di registrazioni attive che richiedono l'elaborazione offload.
- Controllare il log dei lavori del gestore code per ulteriori messaggi di errore

CSQJ031D: *csect - name*, L'INTERVALLO RBA DI LOG DEVE ESSERE REIMPOSTATO. RISPONDERE 'Y' PER CONTINUARE L'AVVIO O ' N' PER CHIUDERE

- Arrestare il gestore code e reimpostare i log il più presto possibile e reimpostare i log.
- Se il gestore code utilizza RBA di log a 6 byte, considerare la possibilità di convertire il gestore code in RBA di log a 8 byte.

CSQJ032E: *csect - name alert - lvl* - AVVICINAMENTO ALLA FINE DELL' INTERVALLO RBA DI LOG DI *max - rba*. CURRENT LOG RBA è *rba corrente*.

- Pianificare l'arresto del gestore code e la reimpostazione dei log non appena possibile.
- Se il gestore code utilizza RBA di log a 6 byte, considerare la possibilità di convertire il gestore code in RBA di log a 8 byte.

CSQJ110E: LAST COPY*n* ACTIVE LOG DATA SET IS *nnn* PERCENT FULL

- Eseguire le operazioni per completare altre attività di scaricamento in attesa eseguendo una richiesta di visualizzazione per determinare le richieste in sospeso relative al processo di scaricamento del log. Eseguire le azioni necessarie per soddisfare le eventuali richieste e consentire all'offload di continuare.
- Considerare se vi sono sufficienti dataset di log attivi. Se necessario, è possibile aggiungere ulteriori dataset di log in modo dinamico utilizzando il comando DEFINE LOG .

CSQJ111A: SPAZIO ESAURITO NEI DATASET DEL LOG ATTIVO

- Eseguire una richiesta di visualizzazione per essere certi che non vi siano richieste in sospeso correlate al processo di offload del log. Eseguire le azioni necessarie per soddisfare le eventuali richieste e consentire all'offload di continuare.
- Considerare se vi sono sufficienti dataset di log attivi. Se necessario, è possibile aggiungere ulteriori dataset di log in modo dinamico utilizzando il comando DEFINE LOG .
- Se il ritardo è stato causato dalla mancanza di una risorsa richiesta per lo scaricamento, la risorsa necessaria deve essere resa disponibile per consentire il completamento dello scaricamento e quindi consentire la registrazione per continuare. Per informazioni sul ripristino da questa condizione, consultare Problemi di registrazione archivio.

CSQJ114I: ERRORE NEL DATASET DI ARCHIVIO, L'OFFLOAD CONTINUA CON LA GENERAZIONE DI UN SOLO DATASET DI ARCHIVIO

- Controllare la registrazione lavori del gestore code per ulteriori messaggi di errori.

- Eseguire una seconda copia del log di archivio e aggiornare manualmente BSDS.

CSQJ115E: OFFLOAD NON RIUSCITO, IMPOSSIBILE ALLOCARE UN DATASET DI ARCHIVIO

Esaminare le informazioni sullo stato dell'errore del messaggio CSQJ103E o CSQJ073E. Correggere la condizione che ha causato l'errore di assegnazione del dataset in modo che, al nuovo tentativo, lo scaricamento possa essere eseguito.

CSQJ136I: IMPOSSIBILE ASSEGNARE L'UNITÀ NASTRO PER LA CONNESSIONE - ID= *xxxx* CORRELAZIONE - ID= *yyyyyy*, *m* ASSEGNATO *n* CONSENTITO

- Controllare la registrazione lavori del gestore code per ulteriori messaggi di errori.

.

CSQJ151I: *nome - csect* ERRORE LETTURA RBA *rrr*, CONNECTION - ID= *xxxx* RELATION - ID= *aaaa* REASON CODE= *ccc*

- Controllare il log dei lavori del gestore code per ulteriori messaggi.
- Immettere un comando **DISPLAY CONN** per determinare quale connessione non sta eseguendo il commit della propria attività.
- Assicurarsi che l'applicazione possa eseguire il commit degli aggiornamenti.

CSQJ160I: LONG RUNNING UOW FOUND, URID= *urid* CONNECTION NAME= *nome*

- Controllare il log dei lavori del gestore code per ulteriori messaggi.
- Immettere un comando **DISPLAY CONN** per determinare quale connessione non sta eseguendo il commit della propria attività.
- Assicurarsi che l'applicazione possa eseguire il commit degli aggiornamenti.

CSQJ161I: UOW NON RISOLTO DOPO *n* OFFLOADS, URID= *urid* CONNECTION NAME= *name*

- Determinare se la serie di pagine è assegnata al gestore code.
- Immettere un comando **DISPLAY USAGE** per determinare lo stato della serie di pagine.
- Controllare il log dei lavori del gestore code per ulteriori messaggi.

CSQP011E: CONNECT ERROR STATUS *ret - code* FOR PAGE SET *psid*

- Controllare la profondità corrente delle code assegnate a questa serie di pagine.
- Esaminare la causa dell'errore nell'elaborazione dei messaggi.

CSQP013I: *csect - name* NEW EXTENT CREATED FOR PAGE SET psid. NUOVA ESTENSIONE VERRÀ ORA FORMATTATA

- Controllare la profondità corrente delle code assegnate a questa serie di pagine.
- Ricercare la causa dell'errore di elaborazione dei messaggi.
- Determinare se le code devono essere riposizionate in un'altra serie di pagine.
- Se il volume è pieno, determinare se è necessario rendere la serie di pagine un dataset a più volumi. Se la serie di pagine è già multi - volume, considerare la possibilità di aggiungere più volumi al gruppo di archiviazione utilizzato. Quando sarà disponibile altro spazio, ritentare l'espansione impostando il metodo **EXPAND** della serie di pagine su **SYSTEM**. Se è richiesto un nuovo tentativo, passare da **EXPAND** a **SYSTEM** e quindi tornare alla propria impostazione normale.

CSQP014E: *csect - name* EXPANSION FAILED FOR PAGE SET psid. LE FUTURE RICHIESTE DI PROROGA SARANNO RESPINTE

- Controllare la profondità corrente delle code assegnate a questa serie di pagine.
- Ricercare la causa dell'errore di elaborazione dei messaggi.
- Determinare se le code devono essere riposizionate in un'altra serie di pagine.

CSQP016E: *csect - name* PAGE SET *psid* HA RAGGIUNTO IL NUMERO MASSIMO DI ESTENSIONI. NON PUÒ ESSERE ESTESO NUOVAMENTE

- Controllare la profondità corrente delle code assegnate a questa serie di pagine.

- Ricercare la causa dell'errore di elaborazione dei messaggi.

CSQP017I: *csect - name* EXPANSION STARTED FOR PAGE SET *psid*
Emettere comandi DISPLAY THREAD per determinare lo stato delle unità di lavoro in IBM MQ.

CSQP047E: Le serie di pagine non disponibili possono causare problemi - intraprendere un'azione per correggere questa situazione

- Seguire la risposta del programmatore di sistema.

CSQQ008I: *nn* unità di recupero ancora in dubbio nel gestore code *qqq*

- Esaminare lo stato della coda dei messaggi non recapitabili. Verificare che la coda dei messaggi non recapitabili non sia disabilitata.
- Assicurarsi che la coda di messaggi non recapitabili non sia al limite MAXMSG.

CSQQ113I: *nome - psb id - regione* Questo messaggio non può essere elaborato

- Controllare il dataset CSQOUTX per determinare la causa dell'errore CSQINPX.
- Alcuni comandi potrebbero non essere elaborati.

CSQX035I: *csect - name* Connessione al gestore code *qmgr - name* in fase di arresto o interrotto, MQCC= *mqcc* MQRC= *mqrc* (*mqrc - text*

- Controllare MQRC per determinare la causa dell'errore.
- Questi codici sono documentati in IBM MQ for z/OS messaggi, codici di completamento e codici di errore.

CSQX032I: *csect - name* Gestore dei comandi di inizializzazione terminato

- Controllare MQRC per determinare la causa dell'errore.
- Questi codici sono documentati in IBM MQ for z/OS messaggi, codici di completamento e codici di errore.

CSQX048I: *csect - name* Impossibile convertire il messaggio per *nome*, MQCC= *mqcc* MQRC= *mqrc* (*mqrc - text*)

- Controllare la registrazione lavoro per determinare la causa dell'errore TCP/IP.
- Verificare la presenza di errori nello spazio di indirizzo TCP/IP.

CSQX234I: *csect - name* Listener arrestato, TRPTYPE= *trptype* INDISCUTI= *disposition*

- Se il listener non si arresta, dopo un comando **STOP** , verificare la presenza di errori nello spazio di indirizzo TCP/IP.
- Seguire la risposta del programmatore di sistema.

CSQX407I: *csect - name* Cluster queue *q - name* definizioni incongruenti

- Più code cluster all'interno del cluster hanno valori incongruenti. Esaminare e risolvere le differenze.

CSQX411I: *csect - name* Repository manager stopped

- Se il gestore repository è stato arrestato a causa di un errore, controllare la registrazione lavori per i messaggi.

CSQX417I: *csect - name* I mittenti del cluster rimangono per il gestore code rimosso *qmgr*

- Seguire la risposta del programmatore di sistema.

CSQX418I: *csect - name* Solo un repository per il cluster *nome_cluster*

- Per aumentare l'alta disponibilità, i cluster devono essere configurati con due repository completi.

CSQX419I: *csect - name* No cluster - receivers for cluster *nome_cluster*

- Seguire la risposta del programmatore di sistema.

CSQX420I: *csect - name* Nessun repository per il cluster *nome_cluster*

- Seguire la risposta del programmatore di sistema.

CSQX448E: *csect - name* Gestore repository arrestato a causa di errori. Riavvia in *n* secondi

- Seguire la risposta del programmatore di sistema.

  Questo messaggio viene emesso ogni 600 secondi (10 minuti) fino a SYSTEM.CLUSTER.COMMAND.QUEUE è abilitato, utilizzando il seguente comando:

  ```
  ALTER QLOCAL(SYSTEM.CLUSTER.COMMAND.QUEUE) GET(ENABLED)
  ```

  Prima di abilitare la coda, potrebbe essere necessario un intervento manuale per risolvere il problema che ha causato l'arresto del gestore repository, prima che venga emesso il primo messaggio CSQX448E .

CSQX548E: *csect - name* Messaggi inviati alla coda di messaggi non instradabili locale, canale *nome - canale* reason=*mqrc* (*mqrc - text*)

- Seguire la risposta del programmatore di sistema.

CSQX788I: *csect - name* DNS lookup for address *address* using function '*func*' ha impiegato *n* secondi

- Seguire la risposta del programmatore di sistema.

CSQY225E: *csect - name* Il gestore code è a corto di memoria locale al di sopra della barra delle azioni

- Il gestore code è in esecuzione a corto di memoria virtuale sopra la barra. È necessario intraprendere un'azione per alleviare la situazione ed evitare la possibile chiusura anomala del gestore code.

CSQ5038I: *csect - name* L'attività di servizio non risponde da hh.mm.ss.nnnnnn. Ricerca di problemi con Db2

- Seguire la risposta del programmatore di sistema.

Configurazioni HA (High Availability)

Se si desidera utilizzare i gestori code IBM MQ in una configurazione HA (High Availability), è possibile impostare i gestori code in modo che funzionino con un gestore HA (High Availability), come ad esempio PowerHA per AIX (in precedenza HACMP) o il servizio cluster Microsoft (MSCS) o con gestori code a più istanze IBM MQ . V 9.1.0 Su sistemi Linux , è possibile anche distribuire i gestori code di dati replicati (RDQM), che utilizzano un gruppo basato sul quorum per fornire l'alta disponibilità.

MQ Appliance Un'altra opzione per una soluzione di ripristino di emergenza o alta disponibilità è quella di distribuire una coppia di dispositivi IBM MQ . Vedi High Availability e Disaster Recovery nella documentazione di IBM MQ Appliance .

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. Da IBM WebSphere MQ 7.1 in poi, il ripristino da errori del cluster riesegui le operazioni che hanno causato problemi fino a quando i problemi non vengono risolti.

Cluster HA
I cluster HA sono gruppi di due o più computer e risorse, ad esempio dischi e reti, connessi e configurati in modo tale che, in caso di errore, un gestore HA (High Availability), ad esempio HACMP (UNIX) o MSCS (Windows) esegue 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 MQ e cluster HA è descritta in “Relazione tra cluster HA e cluster del gestore code” a pagina 448.

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 i gestori code a più istanze per configurare i propri sistemi di messaggistica altamente disponibili basati su IBM 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.

V 9.1.0 **Gestori code di dati replicati ad alta disponibilità (RDQM HA)**

Istanze dello stesso gestore code configurate su ciascun nodo in un gruppo di tre server Linux . Una delle tre istanze è l'istanza attiva. I dati del gestore code attivo vengono replicati in modo sincrono nelle altre due istanze, quindi una di queste istanze può assumere il controllo in caso di errore. Il raggruppamento dei server è controllato da Pacemakere la replica da DRBD.

V 9.1.0 **Gestori code di dati replicati di ripristino di emergenza (RDQM DR)**

Un gestore code viene eseguito su un nodo primario in un sito, con un'istanza secondaria di tale gestore code ubicata su un nodo di recupero in un sito differente. I dati vengono replicati tra l'istanza primaria e l'istanza secondaria, e se il nodo primario viene perso per qualche motivo, l'istanza secondaria può essere creata nell'istanza primaria e avviata. Entrambi i nodi devono essere server Linux . La replica è controllata da DRBD.

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 IBM MQ
- Failover più rapido rispetto al cluster HA
- Configurazione e funzionamento semplici
- Integrazione con IBM 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:

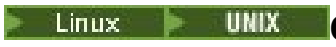
- Sono richiesti ulteriori acquisti di prodotti e competenze
- I dischi che possono essere commutati tra i nodi del cluster sono obbligatori
- La configurazione dei cluster HA è relativamente complessa
- Il failover è piuttosto lento storicamente, ma i prodotti cluster HA recenti stanno migliorando
- 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 forniscono il bilanciamento del carico dei messaggi tra le istanze disponibili delle code del gestore code. Ciò offre una disponibilità superiore rispetto a un singolo gestore code poiché, in caso di errore di un gestore code, le applicazioni di messaggistica possono ancora inviare messaggi e accedere alle istanze rimanenti di una coda del cluster del gestore code. Tuttavia, sebbene i cluster dei gestori code instradino automaticamente i nuovi messaggi ai gestori code disponibili in un cluster, i messaggi attualmente accodati su un gestore code non disponibile non saranno disponibili fino a quando tale gestore code non viene riavviato. Per questo motivo, i cluster di gestori code da soli non forniscono l'alta disponibilità di tutti i dati dei messaggi o forniscono il rilevamento automatico dell'errore del gestore code e l'attivazione automatica del riavvio o del failover del gestore code. I cluster HA (High Availability) forniscono queste funzioni. I due tipi di cluster possono essere utilizzati insieme per un buon effetto. Per un'introduzione ai cluster dei gestori code, consultare Progettazione dei cluster.

Attività correlate

Alta disponibilità per IBM MQ Advanced certified container



Cluster HA su UNIX and Linux

È possibile utilizzare IBM MQ con un cluster HA (high availability) su piattaforme UNIX and Linux : ad esempio, PowerHA per AIX (in precedenza HACMP), Veritas Cluster Server, HP Serviceguard o un cluster Red Hat Enterprise Linux con Red Hat Cluster Suite.

Prima di IBM WebSphere MQ 7.0.1, veniva fornito SupportPac MC91 per assistere nella configurazione dei cluster HA. IBM WebSphere MQ 7.0.1 ha fornito un grado di controllo maggiore rispetto alle precedenti versioni 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 448, la relazione tra i cluster HA e i cluster dei gestori code, “IBM MQ client” a pagina 449e “IBM MQ che opera in un cluster HA” a pagina 449e 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 IBM 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 IBM 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.

IBM MQ client

I client IBM 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. IBM WebSphere MQ 7 ha introdotto funzioni nell'elaborazione di CCDT (Client Channel Definition Table) che aiutano con la disponibilità della connessione e il bilanciamento del carico di lavoro; tuttavia, queste non sono direttamente rilevanti quando si utilizza un sistema di failover.

La funzionalità transazionale consente a IBM MQ MQI client di partecipare a transazioni a due fasi, purché il client sia connesso allo stesso gestore code. La funzionalità transazionale non può utilizzare tecniche, come un programma di bilanciamento del carico IP, per effettuare una selezione da un elenco di gestori code. Quando si utilizza un prodotto HA, un gestore code conserva la propria identità (nome e indirizzo) indipendentemente dal nodo su cui è in esecuzione, quindi è possibile utilizzare la funzionalità transazionale con i gestori code che si trovano sotto il controllo HA.

IBM 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:

- Su 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 IBM 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 anche possibile includere altre risorse IBM 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.

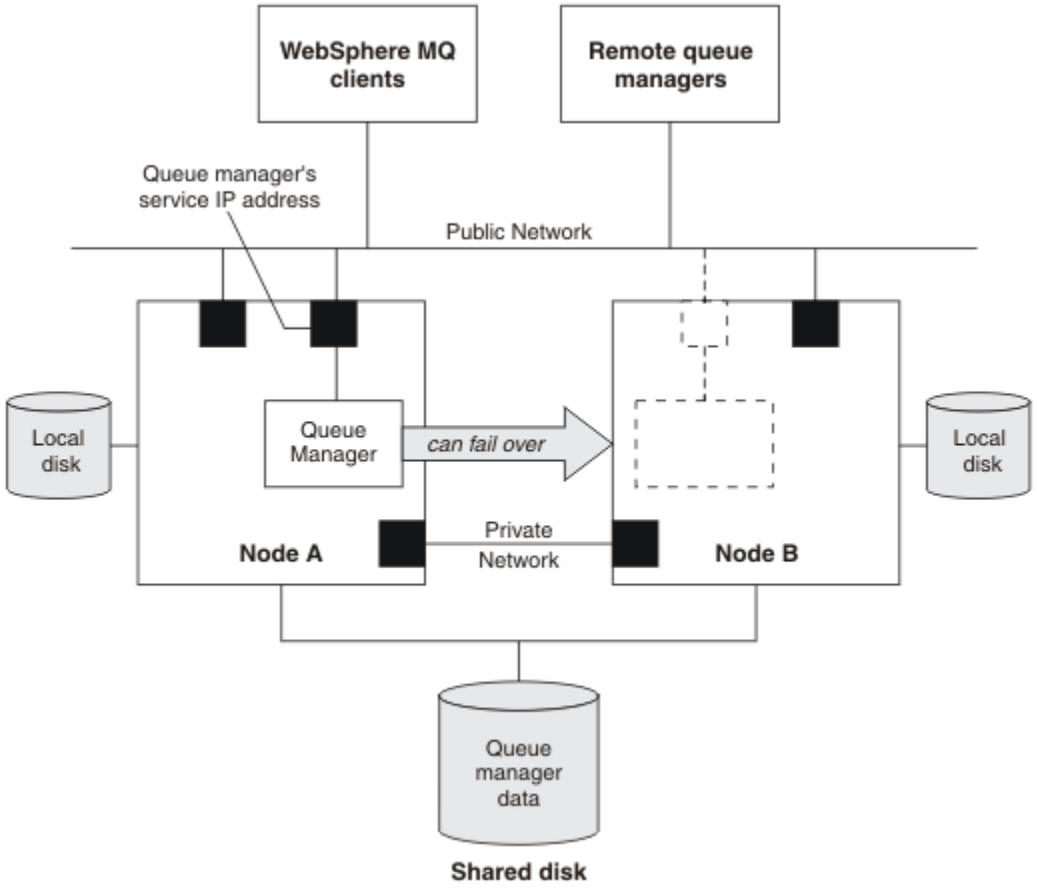


Figura 72. Cluster HA

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. IBM MQ viene eseguito come utente mqm. L'amministrazione di IBM MQ è concessa a membri del gruppo mqm. 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. La gestione di IBM MQ da parte dell'utente root non è consentita; gli script di avvio, arresto o monitoraggio devono passare all'utente mqm.

Nota: IBM MQ deve essere installato correttamente su tutti i nodi; non è possibile condividere i file eseguibili del prodotto.

Linux UNIX *Configurazione dei dischi condivisi su UNIX and Linux*

Un gestore code IBM 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.

Informazioni su questa attività

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.

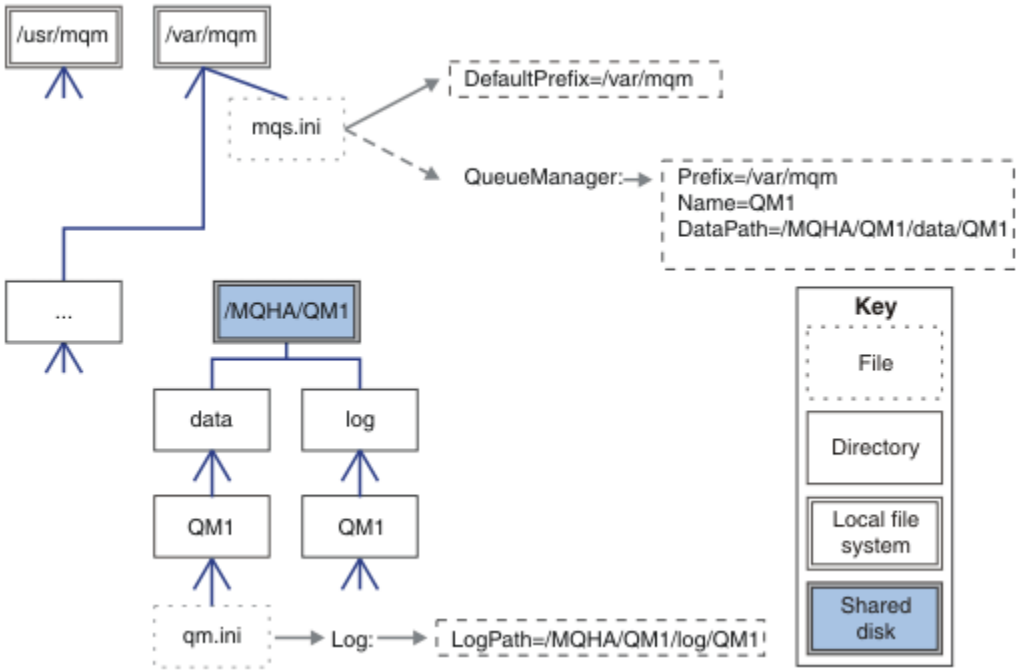


Figura 73. Directory `data` e `log` denominate condivise

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.

Linux UNIX *Creazione di un gestore code cluster HA su UNIX and Linux*

Il primo passo per utilizzare un gestore code in un cluster ad alta disponibilità consiste nel creare il gestore code su uno dei nodi.

Informazioni su questa attività

Per creare un gestore code da utilizzare in un cluster HA, è necessario selezionare prima uno dei nodi nel cluster su cui creare il gestore code, quindi completare la seguente procedura su questo nodo.

Procedura

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** :

   ```
   dspmqinf -o command qmgrname
   ```

   dove `qmgrname` è il nome del gestore code.

   Per ulteriori informazioni sull'utilizzo del comando **addmqinf** , consultare “Aggiunta della configurazione del gestore code ad altri nodi cluster HA su UNIX and Linux” a pagina 452.

   Il comando **addmqinf** viene visualizzato in modo simile al seguente esempio:

   ```
   addmqinf -sQueueManager -vName=qmgrname -vDirectory=qmgrname \
   -vPrefix=/var/mqm -vDataPath=/MQHA/qmgrname/data/qmgrname
   ```

7. Prendere nota del comando visualizzato.
8. Smontare i filesystem del gestore code.

Operazioni successive

Si è ora pronti a completare la procedura descritta in “Aggiunta della configurazione del gestore code ad altri nodi cluster HA su UNIX and Linux” a pagina 452.

Linux UNIX *Aggiunta della configurazione del gestore code ad altri nodi cluster HA su UNIX and Linux*

È necessario aggiungere le informazioni di configurazione del gestore code agli altri nodi nel cluster HA.

Prima di iniziare

Prima di completare questa attività, è necessario aver completato i passi in “Creazione di un gestore code cluster HA su UNIX and Linux” a pagina 451. Una volta creato il gestore code, è necessario aggiungere le informazioni di configurazione per il gestore code a ciascuno degli altri nodi nel cluster HA completando la seguente procedura su ognuno degli altri nodi.

Informazioni su questa attività

Quando si crea un gestore code da utilizzare in un cluster HA, è necessario prima selezionare uno dei nodi nel cluster su cui creare il gestore code, come descritto in “Creazione di un gestore code cluster HA su UNIX and Linux” a pagina 451.

Procedura

1. Montare i filesystem del gestore code.
2. Aggiungere le informazioni di configurazione del gestore code al nodo.

   Esistono due metodi per aggiungere le informazioni di configurazione:

   - Modificando direttamente `/var/mqm/mqs.ini` .
   - Immettendo il comando **addmqinf** visualizzato dal comando **dspmqinf** nel passo 6 in “Creazione di un gestore code cluster HA su UNIX and Linux” a pagina 451.

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 MQ del comando **addmqinf** . Per avviare e arrestare il gestore code da un'installazione diversa da quella attualmente associata al gestore code, 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.

Linux UNIX *Script shell di esempio per l'avvio di un gestore code cluster HA su UNIX and Linux*

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 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.

Linux UNIX *Script di shell di esempio per l'arresto di un gestore code del cluster HA su UNIX and Linux*

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 arrestare immediatamente un gestore code senza fare ipotesi sullo stato corrente del gestore code. Lo 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 è fornito in "Script shell di esempio per l'avvio di un gestore code cluster HA su UNIX and Linux" a pagina 453.)

```
#!/bin/ksh
#
# The script ends the QM by using two phases, initially trying an immediate
# end with a time-out and escalating to a forced stop of remaining
# processes.
#
# The script must be run by the mqm user.
#
# There are two arguments: the queue manager name and a timeout value.
QM=$1
TIMEOUT=$2

if [ -z "$QM" ]
then
  echo "ERROR! No queue manager name supplied"
  exit 1
fi

if [ -z "$TIMEOUT" ]
then
  echo "ERROR! No timeout specified"
  exit 1
fi

for severity in immediate brutal
do
  # End the queue manager in the background to avoid
  # it blocking indefinitely. Run the TIMEOUT timer
  # at the same time to interrupt the attempt, and try a
  # more forceful version. If the brutal version fails,
  # nothing more can be done here.

  echo "Attempting ${severity} end of queue manager '${QM}'"
  case $severity in

  immediate)
    # Minimum severity of endmqm is immediate which severs connections.
    # HA cluster should not be delayed by clients
    endmqm -i ${QM} &
    ;;

  brutal)
    # This is a forced means of stopping queue manager processes.

    srchstr="( |-m)$QM *.*$"
    for process in amqzmuc0 amqzxma0 amqfcxba amqfqpub amqpcsea amqzlaa0 \
                amqzlsa0 runmqchi runmqlsr amqcrsta amqrrmfa amqrmppa \
                amqzfuma amqzmuf0 amqzmur0 amqzmgr0
    do
      ps -ef | tr "\t" " " | grep $process | grep -v grep | \
          egrep "$srchstr" | awk '{print $2}'| \
             xargs kill -9 > /dev/null 2>&1
    done

  esac

  TIMED_OUT=yes
  SECONDS=0
  while (( $SECONDS < ${TIMEOUT} ))
  do
   TIMED_OUT=yes
   i=0
   while [ $i -lt 5 ]
```

```
    do
      # Check for execution controller termination
      srchstr="( |-m)$QM *.*$"
      cnt=`ps -ef | tr "\t" " " | grep amqzxma0 | grep -v grep | \
        egrep "$srchstr" | awk '{print $2}' | wc -l `
      i=`expr $i + 1`
      sleep 1
      if [ $cnt -eq 0 ]
      then
        TIMED_OUT=no
        break
      fi
    done

    if [ ${TIMED_OUT} = "no" ]
    then
      break
    fi

    echo "Waiting for ${severity} end of queue manager '${QM}'"
    sleep 1
  done # timeout loop

  if [ ${TIMED_OUT} = "yes" ]
  then
    continue        # to next level of urgency
  else
    break           # queue manager is ended, job is done
  fi

done # next phase
```

Nota: In base ai processi in esecuzione per un gestore code specifico, l'elenco dei processi del gestore code inclusi in questo script potrebbe non essere completo o potrebbe includere più processi rispetto ai processi in esecuzione per tale gestore code:

```
for process in amqzmuc0 amqzxma0 amqfcxba amqfqpub amqpcsea amqzlaa0 \
               amqzlsa0 runmqchi runmqlsr amqcrsta amqrrmfa amqrmppa \
               amqzfuma amqzmuf0 amqzmur0 amqzmgr0
```

Un processo può essere incluso o escluso da questo elenco in base alla funzione configurata e ai processi in esecuzione per un gestore code specifico. Per un elenco completo di processi e informazioni sull'arresto dei processi in un ordine specifico, consultare Arresto manuale di un gestore code in UNIX e Linux.

Linux UNIX *Controllo di un gestore code cluster HA su UNIX and Linux*

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 IBM WebSphere MQ 7.1, è possibile avere più installazioni di IBM MQ coesistenti su un sistema. Per ulteriori informazioni su più installazioni, consultare Più installazioni. Se si intende utilizzare lo script di monitoraggio in più installazioni, incluse le installazioni in IBM WebSphere MQ 7.1o versioni successive, potrebbe essere necessario eseguire alcune operazioni aggiuntive. Se si dispone di un'installazione primaria o si sta utilizzando lo script con versioni precedenti a IBM WebSphere MQ 7.1, non è necessario specificare *MQ_INSTALLATION_PATH* per utilizzare lo script. In caso contrario, i seguenti passi garantiscono che *MQ_INSTALLATION_PATH* sia identificato correttamente:

1. Utilizzare il comando **crtmqenv** da un'istallazione IBM WebSphere MQ 7.1 per identificare il *MQ_INSTALLATION_PATH* corretto 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 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 “Script shell di esempio per l'avvio di un gestore code cluster HA su UNIX and Linux” a pagina 453):

```
#!/bin/ksh
#
# This script tests the operation of the queue manager.
#
# An exit code is generated by the runmqsc command:
# 0  => Either the queue manager is starting or the queue manager is running and responds.
#       Either is OK.
# >0 => The queue manager is not responding and not starting.
#
# This script must be run by the mqm user.
QM=$1
MQ_INSTALLATION_PATH=$2

if [ -z "$QM" ]
then
  echo "ERROR! No queue manager name supplied"
  exit 1
fi

if [ -z "$MQ_INSTALLATION_PATH" ]
then
  # No path specified, assume system primary install or MQ level < 7.1.0.0
  echo "INFO: Using shell default value for MQ_INSTALLATION_PATH"
else
  echo "INFO: Prefixing shell PATH variable with $MQ_INSTALLATION_PATH/bin"
  PATH=$MQ_INSTALLATION_PATH/bin:$PATH
fi

# Test the operation of the queue manager. Result is 0 on success, non-zero on error.
echo "ping qmgr" | runmqsc ${QM} > /dev/null 2>&1
pingresult=$?

if [ $pingresult -eq 0 ]
then # ping succeeded

  echo "Queue manager '${QM}' is responsive"
  result=0

else # ping failed

  # Don't condemn the queue manager immediately, it might be starting.
  srchstr="( |-m)$QM *.*$"
  cnt=`ps -ef | tr "\t" " " | grep strmqm | grep "$srchstr" | grep -v grep \
              | awk '{print $2}' | wc -l`
  if [ $cnt -gt 0 ]
```

```
  then
    # It appears that the queue manager is still starting up, tolerate
    echo "Queue manager '${QM}' is starting"
    result=0
  else
    # There is no sign of the queue manager starting
    echo "Queue manager '${QM}' is not responsive"
    result=$pingresult
  fi

fi

exit $result
```

Linux UNIX *Inserimento del gestore code sotto il controllo del cluster HA su UNIX and Linux*

È necessario configurare il gestore code, sotto il controllo del cluster HA, con l'indirizzo IP del gestore code e i dischi condivisi.

Informazioni su questa attività

Per mettere il gestore code sotto il controllo di un cluster HA, è necessario definire un gruppo di risorse che contenga il gestore code e tutte le risorse associate.

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.

Linux UNIX *Eliminazione di un gestore code del cluster HA su UNIX and Linux*

Si potrebbe voler rimuovere un gestore code da un nodo che non è più richiesto per eseguire il gestore code.

Informazioni su questa attività

Per rimuovere il gestore code da un nodo in un cluster HA, è necessario rimuovere le informazioni di configurazione.

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*
3. Opzionale: Per eliminare completamente il gestore code, utilizzare il comando **dltmqm** .

   Importante: Tenere presente che l'eliminazione del gestore code utilizzando il comando **dltmqm** elimina completamente i dati e i file di log 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.

Windows Supporto del servizio cluster Microsoft (MSCS)

Introduzione e configurazione di MSCS per supportare il failover di server virtuali.

Queste informazioni si applicano solo a IBM MQ for Windows .

MSCS (Microsoft Cluster Service) consente di collegare i server in un *cluster*, fornendo una maggiore disponibilità di dati e applicazioni e rendendo più semplice 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 458
- “Impostazione di IBM MQ per il clustering MSCS” a pagina 459

Quindi indica come configurare IBM MQ per il clustering MSCS, nelle sezioni seguenti:

- “Creazione di un gestore code da utilizzare con MSCS” a pagina 461
- “Spostamento di un gestore code nella memoria MSCS” a pagina 462
- “Inserimento di un gestore code sotto il controllo di MSCS” a pagina 463
- “Rimozione di un gestore code dal controllo MSCS” a pagina 470

Quindi, fornisce alcuni utili suggerimenti sull'utilizzo di MSCS con IBM MQe dettagli sui programmi di utilità di supporto MSCS IBM MQ , nelle seguenti sezioni:

- “Suggerimenti e consigli sull'utilizzo di MSCS” a pagina 471
- “Supporto per programmi di utilità MSCS” a pagina 474

Windows *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.

“Configurazioni HA (High Availability)” a pagina 446 contiene un confronto tra cluster MSCS, gestori code a più istanze e cluster IBM 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 IBM 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. C'è anche un altro disco condiviso, che deve essere un array ridondante di dischi indipendenti (*RAID*) Livello 1, per l'uso esclusivo di MSCS; 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 mostrata in Figura 74 a pagina 459.

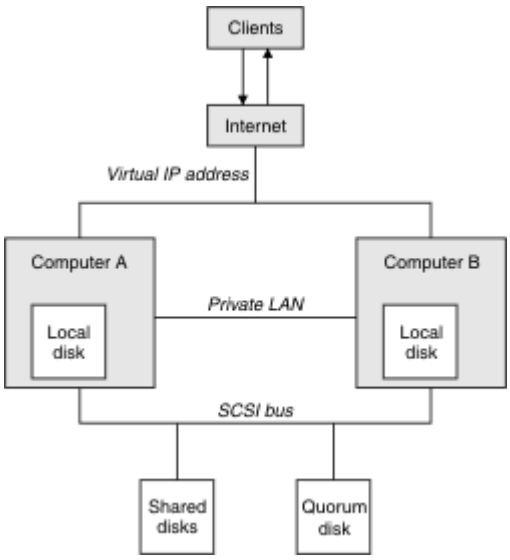


Figura 74. cluster MSCS a due computer

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.

Windows *Impostazione di IBM MQ per il clustering MSCS*

Configurare IBM 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 MQ su ogni computer del cluster.

Poiché il gestore code è associato con il nome di installazione IBM MQ , il nome di installazione di IBM 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 MQ; consultare “Spostamento di un gestore code nella memoria MSCS” a pagina 462. Se si desidera creare nuovi gestori code da utilizzare con MSCS, consultare “Creazione di un gestore code da utilizzare con MSCS” a pagina 461.

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 463.

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 470.

Windows *Imposta simmetria e MSCS*

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, assicurarsi che tutto il software richiesto installato sui due elaboratori 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 460.

Windows *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 hai già un dominio e gli account rilevanti per IBM 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 IBM MQ MSCS garantisce che tutti i file che contengono gli 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.

Puoi utilizzare un account di dominio per eseguire il servizio IBM MQ . Assicurarsi che esista nel gruppo mqm locale su ciascun computer nel cluster.

Windows *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.

Windows *Modalità cluster e MSCS*

Esistono due modalità in cui è possibile eseguire un sistema cluster con IBM MQ su Windows: Attivo / Passivo o Attivo / Attivo.

Nota: Se si utilizza MSCS insieme a COM + (Microsoft Transaction Server), 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 IBM MQ ciò significa che è possibile, ad esempio, eseguire due gestori code, uno su ciascuno di A e B, con ciascuno che sfrutta la potenza completa 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.

Windows *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 IBM 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. (Il IBM MQ Explorer avvia automaticamente un nuovo gestore code e lo imposta all'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:\IBM 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 IBM 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 462.

Creazione di un gestore code utilizzando IBM MQ Explorer

Attenersi alla seguente procedura per creare un gestore code utilizzando IBM MQ Explorer, da utilizzare con MSCS:

1. Avviare IBM MQ Explorer dal menu Start.
2. Nella vista Navigator , espandere i nodi della struttura ad albero per trovare i nodi della struttura ad albero `Gestori code` .
3. Fare clic con il pulsante destro del mouse sul nodo `Gestori code` e selezionare**Nuovo** > **Gestore code**. Viene visualizzato il pannello Crea gestore code.
4. Completare la finestra di dialogo (Passo 1), quindi fare clic su **Avanti>**.
5. Completare la finestra di dialogo (Passo 2), quindi fare clic su **Avanti>**.
6. Completare la finestra di dialogo (Passo 3), verificando che `Avvia gestore code` e `Crea canale di connessione server` non siano selezionati, quindi fare clic su **Avanti>**.
7. Completare la finestra di dialogo (passo 4), quindi fare clic su **Fine**.
8. Procedere con "Spostamento di un gestore code nella memoria MSCS" a pagina 462.

Windows *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`*.

Attenzione: Non provare a trasferire i file manualmente; utilizzare il programma di utilità fornito come parte del supporto IBM MQ MSCS come descritto in questo argomento.

Se il gestore code che viene spostato utilizza le connessioni TLS e il repository delle chiavi TLS 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 repository chiavi TLS, SSLKEYR, viene 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 livello superiore in cui è installato IBM 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 MQ Explorer o MQSC `ALTER QMGR`, per puntare al nuovo file del repository delle chiavi TLS.

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 463.
3. Eseguire un backup completo dei file di coda e dei file di log e archiviare il backup in un luogo sicuro (consultare "File di log del gestore code" a pagina 472 per il motivo 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: \
```

```
IBM MQ " /ld " e: \
IBM MQ \log"
```

sostituire il nome del gestore code con *qmname*, la lettera dell'unità disco condivisa per *e*e la directory scelta per *IBM MQ*. Le directory vengono create se non esistono già.

8. Verificare che il gestore code funzioni, utilizzando IBM MQ Explorer. Ad esempio:
   a. fare clic con il tastino destro del mouse sul nodo della struttura ad albero del gestore code, quindi selezionare **Avvia**. Il gestore code viene avviato.
   b. Fare clic con il pulsante destro del mouse sul nodo della struttura ad albero Code , quindi selezionare **Nuovo** > **Coda locale ...**, e assegnare un nome alla coda.
   c. Fare clic su **Fine**.
   d. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Inserisci messaggio di prova ...**. Viene visualizzato il pannello Inserisci messaggio di prova.
   e. Immettere del testo del messaggio, quindi fare clic su **Inserisci messaggio di prova**e chiudere il pannello.
   f. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Sfoglia messaggi ...**. Viene visualizzato il pannello Browser messaggi.
   g. Assicurarsi che il proprio messaggio sia sulla coda, quindi fare clic su **Chiudi**. Il pannello Browser messaggi viene chiuso.
   h. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Cancella messaggi ...**. I messaggi sulla coda vengono eliminati.
   i. Fare clic con il pulsante destro del mouse sulla coda, quindi selezionare **Elimina ...**. 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 **Arresta ...**. Viene visualizzato il pannello Fine gestore code.
   k. Fare clic su **OK**. Il gestore code viene arrestato.
9. Come amministratore di IBM MQ , assicurarsi che l'attributo di avvio del gestore code sia impostato su manuale. In IBM MQ Explorer, 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 463.

Windows *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 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 MQ per il clustering MSCS" a pagina 459.
2. Utilizzare il programma di utilità **haregtyp** per registrare IBM MQ come un tipo di risorsa MSCS su tutti i nodi cluster. Consultare "Supporto per programmi di utilità MSCS" a pagina 474 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 461.
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 462.
5. Arrestare il gestore code, se è in esecuzione, utilizzando un prompt dei comandi o IBM 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

Per inserire 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 **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 MQSeries MSCS necessita di ulteriore configurazione:
   a. Selezionare il nuovo servizio definito che contiene una risorsa denominata 'Nuovo 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'identificazione del gestore code a cui è destinato.
      - `Run in a separate Resource Monitor` ; per un migliore isolamento
      - `Possible owners` ; imposta 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 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 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, fare riferimento a "Comando PostOnlinee comando PreOfflinein MSCS" a pagina 473.
  - `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, fare riferimento a "Comando PostOnlinee comando PreOfflinein MSCS" a pagina 473.

    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 "Polling looksAlive e isAlive su MSCS" a pagina 469.

d. Facoltativamente, impostare un nodo preferito (ma notare i commenti in "Utilizzo dei nodi preferiti in MSCS" a pagina 473)

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 MQ . Ad esempio:

   a. Fare clic con il pulsante destro del mouse sul nodo della struttura ad albero `Code` , quindi selezionare **Nuovo** > **Coda locale ...**, e assegnare un nome alla coda.

   b. Fare clic su **Fine**. La coda viene creata e visualizzata nella vista Contenuto.

   c. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Inserisci messaggio di prova ...**. Viene visualizzato il pannello Inserisci messaggio di prova.

   d. Immettere del testo del messaggio, quindi fare clic su **Inserisci messaggio di prova**e chiudere il pannello.

   e. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Sfoglia messaggi ...**. Viene visualizzato il pannello Browser messaggi.

   f. Assicurarsi che il proprio messaggio sia nella coda, quindi fare clic su **Chiudi**. Il pannello Browser messaggi viene chiuso.

   g. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Cancella messaggi ...**. I messaggi sulla coda vengono eliminati.

   h. Fare clic con il pulsante destro del mouse sulla coda, quindi selezionare **Elimina ...**. 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 462. 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.

Server Windows 2008

Per posizionare un gestore code sotto il controllo di MSCS su Windows Server 2008, utilizzare la procedura riportata di seguito:

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 **MQSeries MSCS** sul pannello **Seleziona tipo risorsa** .
   f. Completare i passi rimanenti nella procedura guidata.
5. Prima di portare la risorsa in linea, la risorsa MQSeries MSCS necessita di ulteriore configurazione:
   a. Selezionare il nuovo servizio definito che contiene una risorsa denominata 'Nuovo 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'identificazione del gestore code a cui è destinato.
      - `Run in a separate Resource Monitor` ; per un migliore isolamento
      - `Possible owners` ; imposta 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 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 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, fare riferimento a “Comando PostOnlinee comando PreOfflinein MSCS” a pagina 473.
  - `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, fare riferimento a “Comando PostOnlinee comando PreOfflinein MSCS” a pagina 473.

    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 “Polling looksAlive e isAlive su MSCS” a pagina 469.

d. Facoltativamente, impostare un nodo preferito (ma notare i commenti in “Utilizzo dei nodi preferiti in MSCS” a pagina 473)

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 MQ . Ad esempio:

   a. Fare clic con il pulsante destro del mouse sul nodo della struttura ad albero `Code` , quindi selezionare **Nuovo** > **Coda locale ...**, e assegnare un nome alla coda.

   b. Fare clic su **Fine**. La coda viene creata e visualizzata nella vista Contenuto.

   c. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Inserisci messaggio di prova ...**. Viene visualizzato il pannello **Inserisci messaggio di prova** .

   d. Immettere del testo del messaggio, quindi fare clic su **Inserisci messaggio di prova**e chiudere il pannello.

   e. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Sfoglia messaggi ...**. Viene visualizzato il pannello **Browser messaggi** .

   f. Assicurarsi che il proprio messaggio sia nella coda, quindi fare clic su **Chiudi**. Il pannello **Browser messaggi** viene chiuso.

   g. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Cancella messaggi ...**. I messaggi sulla coda vengono eliminati.

   h. Fare clic con il pulsante destro del mouse sulla coda, quindi selezionare **Elimina ...**. 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 462. 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 posizionare un gestore code sotto il controllo di MSCS su 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 460.

   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 MQ MSCS*. La procedura guidata richiede diversi elementi, tra cui:

   - `Name` ; scegliere un nome che facilita l'identificazione del gestore code a cui è destinato.
   - `Add to group` ; utilizzare il gruppo creato
   - `Run in a separate Resource Monitor` ; per un migliore isolamento
   - `Possible owners` ; imposta 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 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 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, fare riferimento a “Comando PostOnlinee comando PreOfflinein MSCS” a pagina 473.

– `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, fare riferimento a “Comando PostOnlinee comando PreOfflinein MSCS” a pagina 473.

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 “Polling looksAlive e isAlive su MSCS” a pagina 469.

8. Facoltativamente, impostare un nodo preferito (ma notare i commenti in “Utilizzo dei nodi preferiti in MSCS” a pagina 473)
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 MQ . Ad esempio:
    a. Fare clic con il pulsante destro del mouse sul nodo della struttura ad albero `Code` , quindi selezionare **Nuovo** > **Coda locale ...**, e assegnare un nome alla coda.
    b. Fare clic su **Fine**. La coda viene creata e visualizzata nella vista Contenuto.
    c. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Inserisci messaggio di prova ...**. Viene visualizzato il pannello **Inserisci messaggio di prova** .
    d. Immettere del testo del messaggio, quindi fare clic su **Inserisci messaggio di prova**e chiudere il pannello.
    e. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Sfoglia messaggi ...**. Viene visualizzato il pannello **Browser messaggi** .
    f. Assicurarsi che il proprio messaggio sia nella coda, quindi fare clic su **Chiudi**. Il pannello **Browser messaggi** viene chiuso.
    g. Fare clic con il tasto destro del mouse sulla coda, quindi selezionare **Cancella messaggi ...**. I messaggi sulla coda vengono eliminati.
    h. Fare clic con il pulsante destro del mouse sulla coda, quindi selezionare **Elimina ...**. 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 462. 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 *Polling looksAlive e isAlive su MSCS*

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.

Windows *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 viene rimosso utilizza connessioni TSL, è necessario modificare l'attributo del gestore code, SSLKEYR, utilizzando il comando IBM MQ Explorer o MQSC `ALTER QMGR`, per puntare al file del repository delle chiavi TLS 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 470
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 470.
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 `Groupso Role` se si sta utilizzando Windows 2012 e 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* IBM 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 provare a spostare i file manualmente; utilizzare il programma di utilità **hamvmqm** fornito come parte del supporto IBM MQ MSCS:

1. Eseguire un backup completo dei file di coda e dei file di log e archiviare il backup in un luogo sicuro (consultare "File di log del gestore code" a pagina 472 per il motivo per cui ciò è importante).
2. 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).
3. 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.
4. Eseguire il programma di utilità per spostare il gestore code nel modo seguente:

```
hamvmqm /m qmname /dd " c:\
```

```
IBM MQ " /ld "c:\
IBM MQ \log"
```

sostituire il nome del gestore code con *qmname*, la lettera dell'unità disco locale per *c*e la directory scelta per *IBM MQ* (le directory vengono create se non esistono già).

5. Verificare il funzionamento del gestore code (come descritto in “Spostamento di un gestore code nella memoria MSCS” a pagina 462).

Windows *Suggerimenti e consigli sull'utilizzo di MSCS*

Questa sezione contiene alcune informazioni generali che consentono di utilizzare in modo efficace il supporto IBM MQ per MSCS.

Questa sezione contiene alcune informazioni generali che consentono di utilizzare in modo efficace il supporto IBM MQ per MSCS.

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.

Windows *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 461 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.

Windows *Avvio manuale e MSCS*

Per un gestore code gestito da MSCS, è necessario impostare l'attributo di avvio su manuale. Ciò garantisce che il supporto MSCS IBM MQ possa riavviare MQSeries Service senza avviare immediatamente il gestore code.

Il supporto MSCS di IBM 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, consultare “Spostamento di un gestore code nella memoria MSCS” a pagina 462.

Windows *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 clustering funzioni con IBM 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 462ed 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 predefinito; IBM 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 “Supporto per programmi di utilità MSCS” a pagina 474 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 74 a pagina 459). 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 461
- “Spostamento di un gestore code nella memoria MSCS” a pagina 462
- “Inserimento di un gestore code sotto il controllo di MSCS” a pagina 463

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 462).

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

IBM MQ Il supporto MSCS consente di eseguire più gestori code su ciascuna macchina e di porre singoli gestori code sotto il controllo di MSCS.

Windows *Utilizza sempre MSCS per gestire i cluster*

Non tentare di eseguire operazioni di avvio e di arresto direttamente su qualsiasi gestore code sotto il controllo di MSCS, utilizzando i comandi di controllo o IBM 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.

Windows *Lavorare in modalità Attiva / Attiva in MSCS*

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 IBM MQ con MSCS e COM +:

- I componenti dell'applicazione che utilizzano il supporto IBM MQ COM + devono essere eseguiti sullo stesso computer del 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.

Windows *Comando PostOnlinee comando PreOfflinein MSCS*

Utilizzare questi comandi per integrare il supporto IBM MQ MSCS con altri sistemi. È possibile utilizzarli per immettere comandi IBM MQ , con alcune limitazioni.

Specificare questi comandi nei parametri per una risorsa di tipo `IBM MQ MSCS`. È possibile utilizzarli per integrare il supporto MSCS IBM MQ 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 richiamati questi comandi vengono eseguiti, per impostazione predefinita, dalla directory di sistema Windows . Poiché IBM MQ utilizza un processo di controllo delle risorse a 32 bit, su sistemi Windows a 64 bit, questa è la directory `\Windows\SysWOW64` anziché la directory `\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 utente utilizzato per eseguire il Servizio cluster MSCS; e vengono richiamati in modo asincrono; il supporto IBM MQ MSCS non li attende per 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 IBM 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.

Windows *Utilizzo dei nodi preferiti in MSCS*

Può essere utile quando si utilizza la modalità Attiva / Attiva in MSCS 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` .

Windows *Errori COM + durante l'installazione su MSCS*

Quando si installa IBM 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 IBM MQ su un ambiente MSCS (Microsoft Cluster Server) quando Microsoft Distributed Transaction Coordinator (MSDTC) non è stato configurato per l'esecuzione in tale ambiente. Per informazioni sulla configurazione di MSDTC in un ambiente con cluster, fare riferimento alla documentazione Microsoft .

Windows *Supporto per programmi di utilità MSCS*

Un elenco del supporto IBM MQ per i programmi di utilità MSCS che è possibile eseguire in una richiesta comandi.

Il supporto IBM 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 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 l'amministratore del cluster MSCS, 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 470.
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 MQ.

Spostare un gestore code nella memoria MSCS
`hamvmqm.exe`

Consultare “Spostamento di un gestore code nella memoria MSCS” a pagina 462.

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 Esplora risorse di IBM MQ 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 dell'impostazione del supporto MSCS IBM MQ , come potrebbe essere richiesto se si chiama il supporto IBM . È disponibile un'opzione per salvare i dettagli in un file.

Multi 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.

Esempio di configurazione del gestore code a più istanze

Figura 75 a pagina 475 mostra un esempio di configurazione a più istanze per il gestore code QM1. IBM 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.

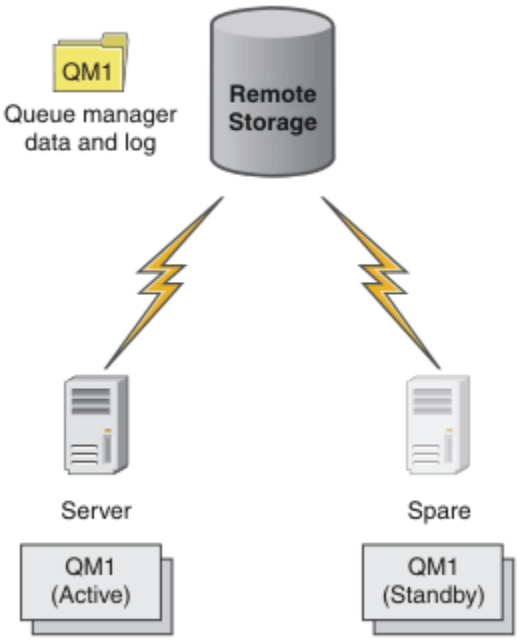


Figura 75. gestore code a più istanze

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 IBM MQ, che quindi arresta 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.

Componenti aggiuntivi necessari per creare una soluzione alta disponibilità

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 il trasferimento di connessioni IBM MQ al computer che assume il controllo dell'esecuzione dell'istanza del gestore code attiva.
- 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 particolare attenzione al comportamento delle applicazioni transazionali e alle applicazioni che sfogliano le code IBM 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.

IBM MQ MQI clients e i canali 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 da IBM MQ classes for Java.

Piattaforme supportate

È possibile creare un gestore code a più istanze su qualsiasi piattaforma nonz/OS supportata da IBM WebSphere MQ 7.0.1 e successive.

La riconnessione automatica del client è supportata per client MQI da IBM WebSphere MQ 7.0.1 e versioni successive.

Crea un gestore code a più istanze

Creare un gestore code a più istanze, creare il gestore code su un server e configurare IBM MQ su un altro server. I gestori code a più istanze condividono 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 `uid` e `gid` di `mqm` uguali 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.

Su Microsoft Windows, l'ID utente che sta eseguendo i processi del gestore code deve disporre 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 “Protezione dei dati del gestore code condiviso e delle directory di log e dei file su Windows” a pagina 504. 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, “Creazione di un gestore code a più istanze su workstation o server di dominio su Windows” a pagina 479, 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, “Creazione di un gestore code a più istanze su controller di dominio Windows” a pagina 494, 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 MQ per ciascun server. Ogni server deve avere la stessa versione di IBM MQ installata a un livello di correzioni 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 517, “Creazione di un gestore code a più istanze su workstation o server di dominio su Windows” a pagina 479e “Creazione di un gestore code a più istanze su controller di dominio Windows” a pagina 494 sono esempi che mostrano come configurare un gestore code a più istanze.

Su sistemi Windows, UNIX and Linux , è possibile condividere un singolo file `mqs.ini` inserendolo 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 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 MQ . IBM i Ad esempio, la condivisione di rete configurata su un server Linux potrebbe contenere log e dati del gestore code separati per gestori code UNIX and Linux , ma non potrebbe contenere i dati del gestore code utilizzati da IBM i.

   IBM i È possibile creare più condivisioni sulla stessa memoria di rete per sistemi IBM i e UNIX purché le condivisioni siano diverse. È possibile assegnare diverse condivisioni a diversi proprietari. La restrizione è una conseguenza dei diversi nomi utilizzati per utenti e gruppi IBM MQ tra UNIX e IBM i. Il fatto che l'utente e il gruppo possono avere gli stessi `uid` e `gid` non allentano la limitazione.
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 .
7. z/OS z/OS non supporta gestori code a più istanze. Utilizzare i gruppi di condivisione code.

   I client ricollegabili funzionano con i gestori code z/OS .

Windows *Domini Windows e gestori code a più istanze*

Un gestore code a più istanze su Windows richiede che i relativi dati e log siano condivisi. 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 507 e “Protezione dei dati del gestore code condiviso e delle directory di log e dei file su Windows” a pagina 504 per esaminare come controllare l'accesso a dati del gestore code e file di log. Gli argomenti sono didattici; se si desidera passare direttamente alla configurazione delle directory condivise per un gestore code a più istanze in un dominio Windows , consultare “Creazione di un gestore code a più istanze su workstation o server di dominio su Windows” a pagina 479.

Eseguire un gestore code a più istanze su server o workstation di dominio

Da IBM WebSphere MQ 7.1, i gestori code a più istanze vengono eseguiti su una workstation o su un server membro di un dominio. 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 parametro `-a` del comando **`crtmqm`** . 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.

Consultare “Creazione di un gestore code a più istanze su workstation o server di dominio su Windows” a pagina 479 per i dettagli sulla creazione di un gestore code a più istanze.

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 di come i processi del gestore code siano autorizzati ad accedere ai relativi 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 507. 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 509 e “Lettura e scrittura dei dati e dei file di log autorizzati da un gruppo di sicurezza locale alternativo” a pagina 513. Un altro argomento, “Protezione dei dati del gestore code condiviso e delle directory di log e dei file su Windows” a pagina 504, 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 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 su Windows” a pagina 482.
2. “Installazione di IBM MQ su un server o su una stazione di lavoro in un dominio Windows” a pagina 486.
3. “Creazione di una directory condivisa per i file di log e i dati del gestore code su Windows” a pagina 489.
4. “Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo” a pagina 491.

È quindi possibile eseguire l'attività, “Creazione di un gestore code a più istanze su workstation o server di dominio su Windows” a pagina 479, 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

I dati del gestore code potrebbero essere protetti con il gruppo `mqm` del dominio. Come spiegato nell'argomento “Protezione dei dati del gestore code condiviso e delle directory di log e dei file su Windows” a pagina 504 , 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 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, “Creazione di un gestore code a più istanze su controller di dominio Windows” a pagina 494 per configurare un gestore code a più istanze sui controller di dominio.

Informazioni correlate

Gestione dell'autorizzazione e del controllo degli accessi

Come utilizzare i nodi cluster di Windows Server come controller di dominio

Windows *Creazione di un gestore code a più istanze su workstation o server di dominio su Windows*

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 MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
Un Windows Server 2008 utilizzato come secondo server IBM 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. Su 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 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 su Windows” a pagina 482.
2. “Installazione di IBM MQ su un server o su una stazione di lavoro in un dominio Windows” a pagina 486.
3. “Creazione di una directory condivisa per i file di log e i dati del gestore code su Windows” a pagina 489.
4. “Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo” a pagina 491.

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 MQ for Windows.
   a) Effettuare le operazioni riportate nell'attività “Installazione di IBM MQ su un server o su una stazione di lavoro in un dominio Windows” a pagina 486 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 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 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 491per 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:\ProgramData\IBM\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:\ProgramData\IBM\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:\ProgramData\IBM\MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

```
IBM 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:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
```

```
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

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:

   ```
   IBM MQ queue manager 'QMGR' starting.
   The queue manager is associated with installation 'Installation1'.
   A standby instance of queue manager 'QMGR' has been started.
   The active instance is running elsewhere.
   ```

2. Su *venus* eseguire il comando **endmqm** :

   ```
   endmqm -r -s -i QMGR
   ```

   La risposta del sistema su *venus*:

   ```
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ended, permitting switchover to
   a standby instance.
   ```

   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 “Verifica del gestore code a più istanze su Windows” a pagina 502.

Windows *Creazione di un dominio Active Directory e DNS su Windows*

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 MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
Un Windows Server 2008 utilizzato come secondo server IBM 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 dell'attività sono congruenti con 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 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 478.

Per l'attività il nome host del controller di dominio è *sun*e i due server IBM 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 successivo, dall'elenco di **Livelli funzionali dell'insieme di strutture** > **Avanti**.

   Il livello più vecchio di Windows Server supportato da IBM MQ è Windows Server 2003.
6. Opzionale: Nella finestra Imposta livello funzionale del dominio, selezionare **Windows Server 2003**o successivo dall'elenco di **Livelli funzionali del 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 MQ" in una workstation o in un server del dominio. La procedura guidata "Prepara IBM MQ" aggiunge automaticamente il gruppo `Domain mqm` al gruppo locale `mqm` in ogni nuova installazione di IBM 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 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 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 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**.

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 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 MQ " configura automaticamente `Domain mqm` come membro del gruppo `mqm` locale in cui viene eseguita la procedura guidata.
È necessario fornire un altro utente per eseguire il servizio IBM MQ per ciascuna installazione di IBM 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 MQ come servizio.

Se è necessario eseguire IBM MQ come un servizio e fornire all'utente del dominio (ottenuto dall'amministratore del dominio) l'accesso per l'esecuzione 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 Windows , immettere il nome utente e la password di un utente o di un responsabile dell'account con autorizzazione sufficiente e fare clic su **OK> Applica> OK**.

Chiudere la finestra Politica di sicurezza locale.

Nota: Su Windows Server 2008 e Windows Server 2012, l'UAC (User Account Control) è abilitato 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 MQ su un server o su una stazione di lavoro in un dominio Windows" a pagina 486.

Attività correlate

Windows Installazione di IBM MQ su un server o su una stazione di lavoro in un dominio Windows

Windows Creazione di una directory condivisa per i file di log e i dati del gestore code su Windows

Windows Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo

Windows *Installazione di IBM MQ su un server o su una stazione di lavoro in un dominio Windows*

In questa attività, si installerà e si configurerà IBM MQ su un server o su una stazione di lavoro 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 MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
Un Windows Server 2008 utilizzato come secondo server IBM 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 su Windows" a pagina 482 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 sui sistemi Windows per altre versioni Windows su cui è possibile eseguire IBM MQ .

Informazioni su questa attività

In questa attività è possibile configurare un server Windows 2008, denominato *mars*, come membro del dominio *wmq.example.com* . Si installa IBM 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 478.

Per l'attività il nome host del controller di dominio è *sun*e i due server IBM 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 elementi 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 MQ for Windows su *mars*.

   Per ulteriori informazioni sull'esecuzione della procedura guidata di installazione di IBM MQ for Windows , consultare Installazione del server IBM MQ su Windows .
   a) Su *mars*, accedere come amministratore locale, *mars*\Administrator.
   b) Eseguire il comando **Setup** sul supporto di installazione IBM MQ for Windows .

      Viene avviata l'applicazione IBM 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 su Windows” a pagina 482, configura un ID utente di dominio per questa serie di attività.

e) Fare clic su **IBM MQ Installazione**, selezionare una lingua di installazione e fare clic su Avvia IBM 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 MQ è installato e il programma di installazione avvia la procedura guidata "Prepara IBM MQ " .

Importante: Non eseguire ancora la procedura guidata.

5. Configurare l'utente che eseguirà il servizio IBM MQ con il diritto **Esegui come servizio** .

Scegliere se configurare il gruppo `mqm` locale, il gruppo `Domain mqm` o l'utente che eseguirà il servizio IBM 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 MQ " .

Per ulteriori informazioni sull'esecuzione della procedura guidata "Prepara IBM MQ " , consultare Configurazione di IBM MQ con la procedura guidata Prepara IBM MQ.

a) Il programma di installazione IBM MQ esegue automaticamente "Prepara IBM MQ " .

Per avviare manualmente la procedura guidata, individuare il collegamento a "Prepara IBM MQ " nella cartella **Avvia** > **Tutti i programmi** > **IBM MQ** . Selezionare il collegamento che corrisponde all'installazione di IBM 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 MQ for Windows per gli utenti del dominio Windows .

d) Nella seconda finestra Configurazione di IBM 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 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 509, per verificare che l'installazione e la configurazione stiano funzionando correttamente.
2. Eseguire l'attività, “Creazione di una directory condivisa per i file di log e i dati del gestore code su Windows” a pagina 489, per impostare una condivisione file per memorizzare i dati e i file di log di un gestore code a più istanze.

Attività correlate

Windows Creazione di un dominio Active Directory e DNS su Windows

Windows Creazione di una directory condivisa per i file di log e i dati del gestore code su Windows

Windows Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo

Riferimenti correlati

Diritti utente richiesti per un servizio IBM MQ Windows

Windows *Creazione di una directory condivisa per i file di log e i dati del gestore code su Windows*

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 MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
: Un Windows Server 2008 utilizzato come secondo server IBM 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 attività esattamente come documentato, effettuare le operazioni riportate nell'attività, “Creazione di un dominio Active Directory e DNS su Windows” a pagina 482, 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 478.

Nell'attività, viene creata una condivisione contenente una directory di dati e log e un gruppo globale per autorizzare l'accesso alla condivisione. Si passa il nome del gruppo globale che autorizza la condivisione al comando **crtmqm** nel relativo 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 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 MQ . Pertanto, *wmquser1* e *wmquser2* sono membri del gruppo `mqm` locale su entrambi i IBM MQ server.

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 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 gli 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 MQ . Controllare l'ID utente di servizio IBM 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 491.

Attività correlate

Windows Creazione di un dominio Active Directory e DNS su Windows

Windows Installazione di IBM MQ su un server o su una stazione di lavoro in un dominio Windows

Windows Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo

Windows *Lettura e scrittura di dati condivisi e file di log autorizzati da un gruppo di sicurezza globale alternativo*

Questa sezione illustra come utilizzare l'indicatore `-a` nel comando **`crtmqm`** . L'indicatore `-a` fornisce al gestore code l'accesso ai relativi file di log e dati su una condivisione file remota utilizzando il gruppo di protezione 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 MQ . Contiene un'istanza del gestore code a più istanze denominato *QMGR*.

venus
Un Windows Server 2008 utilizzato come secondo server IBM 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 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 su Windows" a pagina 482.
2. "Installazione di IBM MQ su un server o su una stazione di lavoro in un dominio Windows" a pagina 486.
3. "Creazione di una directory condivisa per i file di log e i dati del gestore code su Windows" a pagina 489.

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 478.

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 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:

```
IBM MQ queue manager created.
Directory '\\sun\wmq\data\QMGR' created.
The queue manager is associated with installation '1'
Creating or replacing default objects for queue manager 'QMGR'
Default objects statistics : 74 created. 0 replaced.
Completing setup.
Setup completed.
```

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:

   ```
   IBM MQ queue manager 'QMGR' starting.
   The queue manager is associated with installation '1'.
   5 log records accessed on queue manager 'QMGR' during the log
   replay phase.
   Log replay for queue manager 'QMGR' complete.
   Transaction manager state recovered for queue manager 'QMGR'.
   IBM MQ queue manager 'QMGR' started using V7.1.0.0.
   ```

2. 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: IBM 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:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended.
```

6. Eliminare il gestore code.

```
dltmqm QMGR
```

La risposta del sistema:

```
IBM 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
```

Attività correlate

Windows Creazione di un dominio Active Directory e DNS su Windows

Windows Installazione di IBM MQ su un server o su una stazione di lavoro in un dominio Windows

Windows Creazione di una directory condivisa per i file di log e i dati del gestore code su Windows

Windows *Creazione di un gestore code a più istanze su controller di dominio Windows*

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 è basato su Windows Server 2008. La procedura potrebbe differire su altre versioni di Windows Server.

La configurazione utilizza il concetto di mini - dominio o "domainlet" ; vedere Windows 2000, Windows Server 2003 e Windows Server 2008 nodi cluster come controller di dominio. Per aggiungere gestori code a più istanze a un dominio esistente, consultare “Creazione di un gestore code a più istanze su workstation o server di dominio su Windows” a pagina 479.

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 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. Su Windows, le verifiche hanno sempre esito positivo.
2. Eseguire le operazioni in “Creazione di un dominio Active Directory e DNS su Windows” a pagina 482 per creare il primo controller di dominio.
3. Eseguire le operazioni in “Aggiunta di un secondo controller di dominio Windows a un dominio di esempio” a pagina 498 per aggiungere un secondo controller di dominio, installare IBM MQ for Windows su entrambi i controller di dominio e verificare le installazioni.
4. Effettuare le operazioni riportate in “Installazione di IBM MQ su controller di dominio di Windows in un dominio di esempio” a pagina 500 per installare IBM 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 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 Sicurezza 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 Sicurezza 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:

```
IBM MQ queue manager created.
Directory '\\mars\wmq\data\QMGR' created.
The queue manager is associated with installation 'Installation1'.
Creating or replacing default objects for queue manager 'QMGR'.
Default objects statistics : 74 created. 0 replaced. 0 failed.
Completing setup.
Setup completed.
```

4. Avviare il gestore code su *sun*, consentendo un'istanza in standby.

```
strmqm -x QMGR
```

La risposta del sistema:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

5. 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:\ProgramData\IBM\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:\ProgramData\IBM\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
```

```
IBM MQ configuration information added.
```

6. Avviare l'istanza in standby del gestore code in *earth*.

```
strmqm -x QMGR
```

La risposta del sistema:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
A standby instance of queue manager 'QMGR' has been started. The active
instance is running elsewhere.
```

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*:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
```

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended, permitting switchover to
a standby instance.
```

2. 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 “Verifica del gestore code a più istanze su Windows” a pagina 502.

Attività correlate

“Aggiunta di un secondo controller di dominio Windows a un dominio di esempio” a pagina 498

“Installazione di IBM MQ su controller di dominio di Windows in un dominio di esempio” a pagina 500

Informazioni correlate

Nodi cluster Windows 2000, Windows Server 2003 e Windows Server 2008 come controller di dominio

Windows *Aggiunta di un secondo controller di dominio Windows a un dominio di esempio*

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 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 su Windows” a pagina 482 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 server Windows 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 478.

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 elementi 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 MQ ; consultare “Installazione di IBM MQ su controller di dominio di Windows in un dominio di esempio” a pagina 500.

Attività correlate

Windows Installazione di IBM MQ su controller di dominio di Windows in un dominio di esempio

“Creazione di un dominio Active Directory e DNS su Windows” a pagina 482

Windows *Installazione di IBM MQ su controller di dominio di Windows in un dominio di esempio*

Installare e configurare le installazioni di IBM 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 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 su Windows” a pagina 482 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 Windows a un dominio di esempio” a pagina 498 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 sistemi Windows per altre versioni Windows su cui è possibile eseguire IBM MQ .

Informazioni su questa attività

Installare e configurare le installazioni di IBM MQ su entrambi i controller di dominio nel dominio *wmq.example.com* .

Procedura

1. Installare IBM MQ su *sun* e *earth*.

   Per ulteriori informazioni sull'esecuzione della procedura guidata di installazione di IBM MQ for Windows , consultare Installazione del server IBM 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 MQ for Windows .

Viene avviata l'applicazione IBM 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 **IBM MQ Installazione**, selezionare una lingua di installazione e fare clic su Avvia IBM 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 MQ è installato e il programma di installazione avvia la procedura guidata "Prepara IBM MQ " .

L'installazione di IBM MQ for Windows configura un gruppo locale di dominio `mqm`e 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 MQ " .

Per ulteriori informazioni sull'esecuzione della procedura guidata "Prepara IBM MQ " , consultare Configurazione di IBM MQ con la procedura guidata Prepara IBM MQ.

a) Il programma di installazione IBM MQ esegue automaticamente "Prepara IBM MQ " .

Per avviare manualmente la procedura guidata, individuare il collegamento a "Prepara IBM MQ " nella cartella **Avvia** > **Tutti i programmi** > **IBM MQ** . Selezionare il collegamento che corrisponde all'installazione di IBM MQ in una configurazione a più installazioni.

b) Fare clic su **Avanti** e lasciare **No** selezionato in risposta alla domanda "Identifica se è presente un controller di dominio Windows 2000 o successivo nella rete"[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 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 MQ su ciascun controllore, 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 immettere `mqm` ; fare clic su **Verifica nomi** > **OK** > **OK**

Risultati

1. Verificare che "Prepara IBM MQ " abbia creato l'utente del dominio, `MUSR_MQADMIN`:

a. Aprire **Server Manager** > **Ruoli** > **Active Directory Domain Services** > ***wmq.example.com*** > **Utenti**.

[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 MQ come se non fosse nel dominio.

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 509, per verificare che l'installazione e la configurazione stiano funzionando correttamente.
2. Tornare all'attività, “Creazione di un gestore code a più istanze su controller di dominio Windows” a pagina 494, per completare l'attività di configurazione di un gestore code a più istanze sui controller di dominio.

Attività correlate

Windows Aggiunta di un secondo controller di dominio Windows a un dominio di esempio

Riferimenti correlati

Diritti utente richiesti per un servizio IBM MQ Windows

Windows *Verifica del 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 una configurazione del 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.

Questo esempio utilizza la configurazione a più istanze descritta in “Creazione di un gestore code a più istanze su controller di dominio Windows” a pagina 494. 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 7 Service Pack 1. 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 utilizzando IBM MQ Explorer

Prima di utilizzare le applicazioni di esempio per verificare il failover, eseguire IBM 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.

Attenzione: 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 il IBM 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 IBM MQ Explorer, arrestare l'istanza del gestore code attivo, consentendo il passaggio all'istanza in standby e istruendo i client riconnettibili 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 per ristabilire tutte e tre le connessioni. 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
```

Windows *Protezione dei dati del gestore code condiviso e delle directory di log e dei 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 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 di IBM 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 76 a pagina 505. Proteggere una cartella remota con un gruppo globale. Passare il nome del gruppo globale al gestore code quando lo si crea su *mars*. Passare 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 sezione **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.

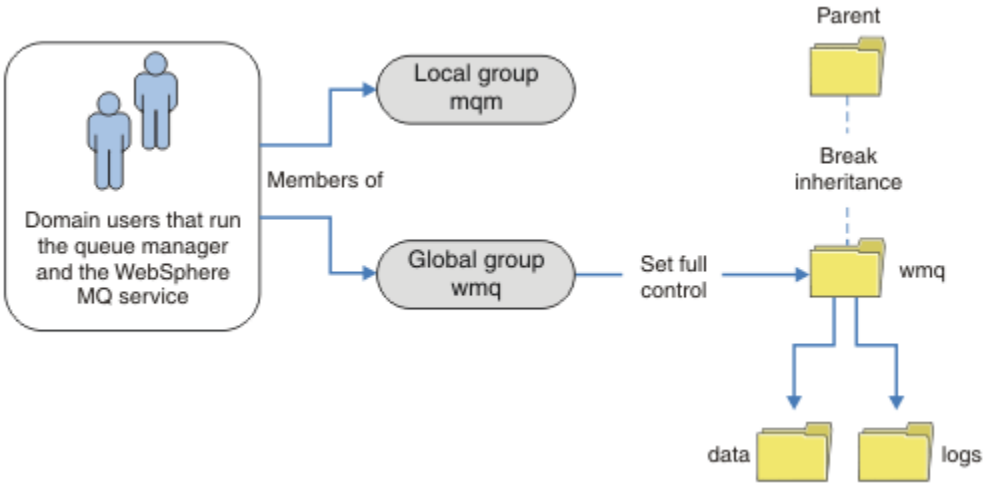


Figura 76. Protezione dei dati e dei log del gestore code mediante un gruppo di sicurezza globale alternativo (1)

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 76 a pagina 505, gli utenti che eseguono i processi del gestore code vengono visualizzati come utenti del dominio.

Se si stanno distribuendo molti server IBM MQ , il raggruppamento di utenti in Figura 76 a pagina 505 non è conveniente. È necessario ripetere il processo di aggiunta di utenti ai gruppi locali per ogni server IBM MQ . Invece, creare un gruppo globale `Domain mqm` sul controller di dominio e rendere gli utenti che eseguono IBM MQ membri del gruppo `Domain mqm` ; consultare Figura 77 a pagina 506. Quando si installa IBM MQ come un'installazione di dominio, la procedura guidata "Prepara IBM 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 MQ su server differenti, ma su un singolo server è necessario disporre di utenti differenti per eseguire IBM 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.

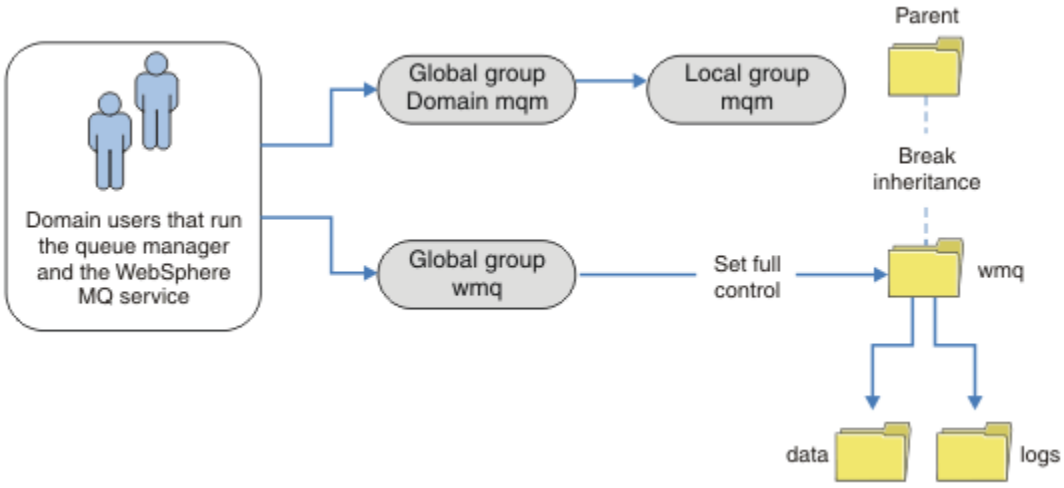


Figura 77. Protezione dei dati e dei log del gestore code utilizzando un gruppo di sicurezza globale alternativo (2)

L'organizzazione in Figura 77 a pagina 506 è inutilmente complicata così com' è. L'accordo ha due gruppi globali con membri identici. È possibile semplificare l'organizzazione e definire un solo gruppo globale; consultare Figura 78 a pagina 506.

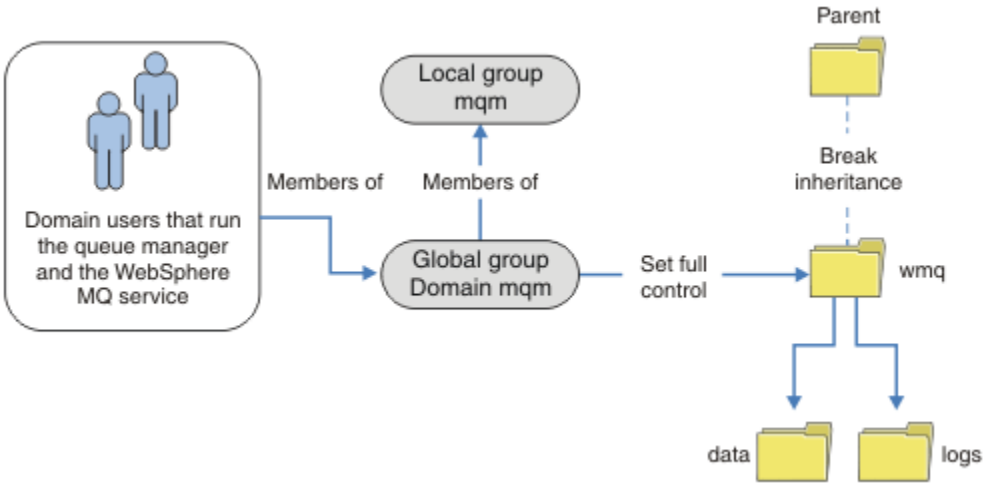


Figura 78. Protezione dei log e dei dati del gestore code utilizzando un gruppo di sicurezza globale alternativo (3)

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 79 a pagina 507. In Figura 79 a pagina 507, sono definiti due gruppi di utenti del dominio, in gruppi globali separati per proteggere file di dati e di log del gestore code differenti. Vengono visualizzati due diversi gruppi `mqm` locali, che devono

trovarsi su server IBM 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 MQ propaga `Domain mqm` al gruppo `mqm` locale come in Figura 78 a pagina 506, poiché esistono due gruppi di utenti.

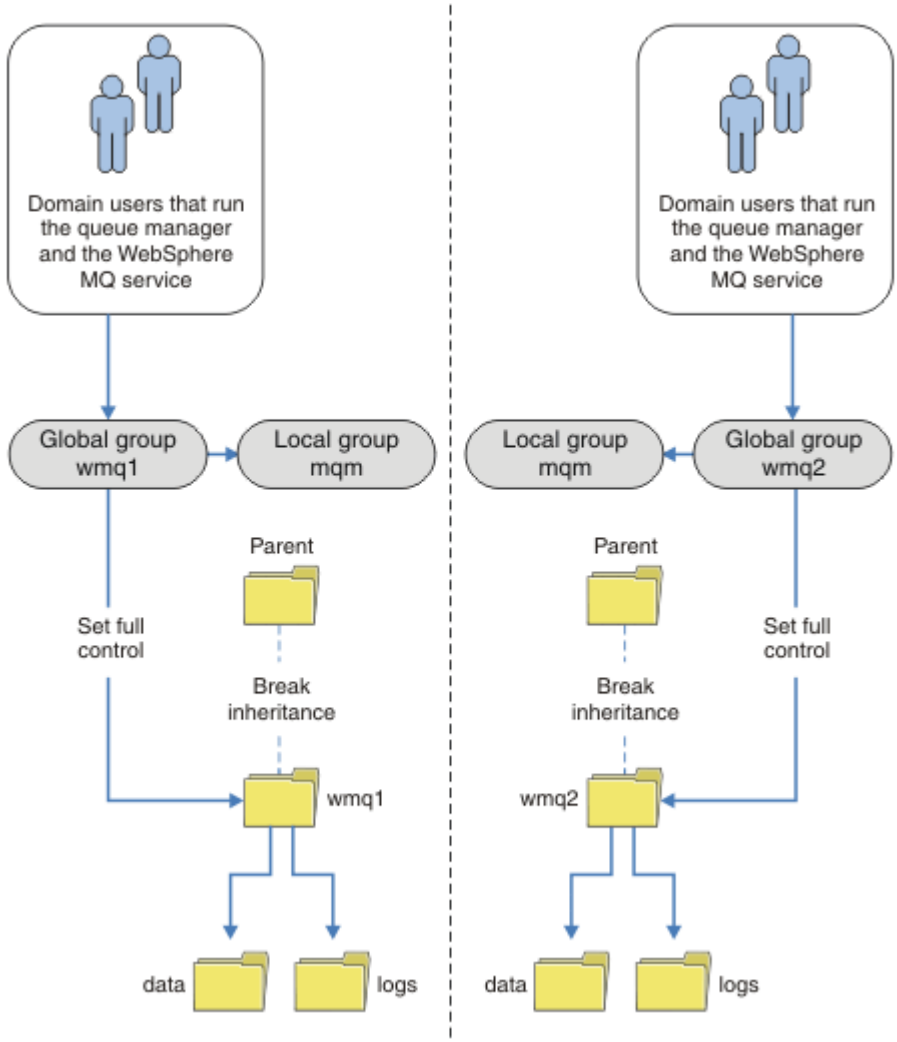


Figura 79. Protezione dei dati e dei log del gestore code utilizzando un principal di sicurezza globale alternativo (4)

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 78 a pagina 506.

Windows *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 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 di IBM MQ per accedere alle directory.

Due esempi dimostrano come configurare il controllo accessi per IBM 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 509, 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 513, 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 diversi, ad esempio con un gestore code a più istanze, la protezione dei dati e dei file di log con il gruppo di protezione alternativo è l'unica scelta; consultare “Protezione dei dati del gestore code condiviso e delle directory di log e dei file su Windows” a pagina 504.

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 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 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 509, 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 80 a pagina 509. Il gruppo locale, `wmq`, è un esempio di un gruppo di protezione alternativo.

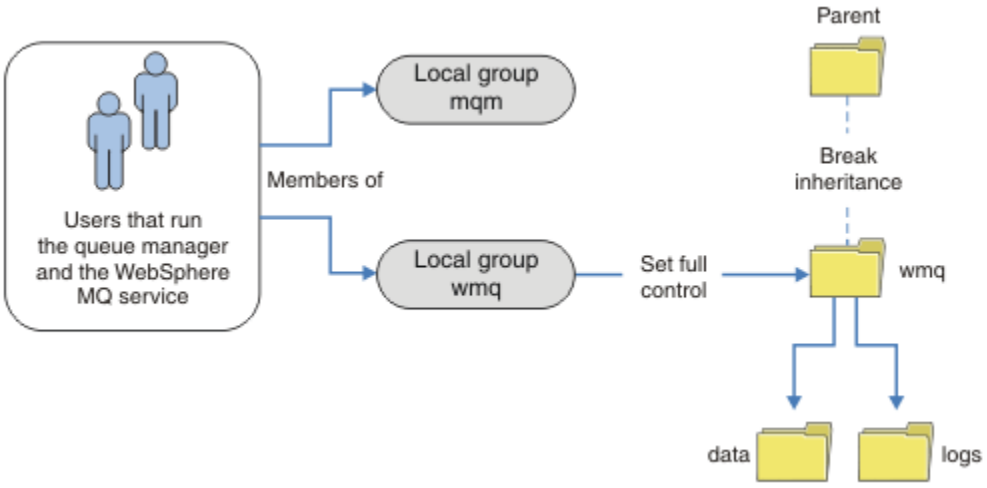


Figura 80. Protezione dei dati e dei log del gestore code utilizzando un gruppo di protezione locale alternativo, wmq

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 “Protezione dei dati del gestore code condiviso e delle directory di log e dei file su Windows” a pagina 504.
5. Creare il gestore code specificando il principal o il gruppo di sicurezza alternativo nel comando **`crtmqm`** , con il parametro `-a` .

Windows *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 MQ for Windows come installazione primaria.
2. Eseguire la procedura guidata "Prepara IBM 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 478, 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 478.

In Windows, è possibile creare i percorsi di dati e log predefiniti per un IBM 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 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 MQ è configurata come parte di un dominio, rendere l'ID utente un membro del gruppo `Domain mqm` . La procedura guidata "Prepara IBM 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:

   ```
   IBM MQ queue manager created.
   Directory 'c:\wmq\data\QMGR' created.
   The queue manager is associated with installation '1'
   ```

```
Creating or replacing default objects for queue manager 'QMGR'
Default objects statistics : 74 created. 0 replaced.
Completing setup.
Setup completed.
```

6. 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:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation '1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

2. 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: IBM 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:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended.
```

6. Eliminare il gestore code.

```
dltmqm QMGR
```

   La risposta del sistema:

```
IBM 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 478
Un gestore code a più istanze su Windows richiede che i relativi dati e log siano condivisi. 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

Windows Lettura e scrittura dei dati e dei file di log autorizzati da un gruppo di sicurezza locale alternativo
Questa sezione illustra 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 491
“Creazione di un gestore code a più istanze su workstation o server di dominio su Windows” a pagina 479

Windows *Lettura e scrittura dei dati e dei file di log autorizzati da un gruppo di sicurezza locale alternativo*

Questa sezione illustra 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 MQ for Windows come installazione primaria.
2. Eseguire la procedura guidata "Prepara IBM 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 478, 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 478.

In Windows, è possibile creare i percorsi di dati e log predefiniti per un IBM 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, si configura un gruppo locale per familiarizzare con l'utilizzo di un gruppo di protezione alternativo senza installare IBM 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 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 protezione locale alternativo, è possibile eseguire l'attività con un'installazione IBM 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) Identifica l'ID utente che esegue il servizio IBM MQ .

      i) Fare clic su **Avvia** > **Esegui ...**, immettere `services.msc` e fare clic su **OK**.

      ii) Fare clic sul servizio IBM 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 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 MQ è stato installato come parte di un dominio e verranno eseguite le attività in "Creazione di un gestore code a più istanze su workstation o server di dominio su Windows" a pagina 479, gli ID utente del dominio creati in "Creazione di un dominio Active Directory e DNS su Windows" a pagina 482 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 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 Windows Sicurezza, quindi fare clic su **OK** > **OK** > **Applica** > **OK**.

2. Aprire un prompt dei comandi.
3. Riavviare il servizio IBM 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 MQ è configurata come parte di un dominio, rendere l'ID utente un membro del gruppo `Domain mqm` . La procedura guidata "Prepara IBM 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:

   ```
   IBM MQ queue manager created.
   Directory 'c:\wmq1\data\QMGR' created.
   The queue manager is associated with installation '1'
   Creating or replacing default objects for queue manager 'QMGR'
   Default objects statistics : 74 created. 0 replaced.
   Completing setup.
   Setup completed.
   ```

8. 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:

   ```
   IBM MQ queue manager 'QMGR' starting.
   The queue manager is associated with installation '1'.
   5 log records accessed on queue manager 'QMGR' during the log
   replay phase.
   Log replay for queue manager 'QMGR' complete.
   Transaction manager state recovered for queue manager 'QMGR'.
   IBM MQ queue manager 'QMGR' started using V7.1.0.0.
   ```

2. 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: IBM 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:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended.
```

6. Eliminare il gestore code.

```
dltmqm QMGR
```

La risposta del sistema:

```
IBM 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
```

Attività correlate

Windows 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.

Linux *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 .

Informazioni su questa attività

L'esempio è configurato su un computer notebook da 2 GHz con 3 GB di RAM su cui è in esecuzione Windows 7 Service Pack 1. 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 MQI WebSphere MQ viene installato su un'immagine VMware aggiuntiva di 400 MB che esegue Windows 7 Service Pack 1 ed esegue le applicazioni ad alta disponibilità di esempio. 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.

Procedura

1. Collegarsi come root.
2. Leggere la sezione Installazione IBM MQ - panoramica e seguire il collegamento appropriato per installare IBM MQ, creare l'utente e il gruppo mqm e definire `/var/mqm`.
3. Completare l'attività Verifica del funzionamento del file system condiviso per verificare che il file system supporti gestori code a più istanze.
4. Per Server1, completare la seguente procedura:
   a. Creare le directory di log e di dati in una cartella comune, `/MQHA`, da condividere. Ad esempio:
      i) **mkdir** */MQHA*
      ii) **mkdir** */MQHA/logs*
      iii) **mkdir** */MQHA/qmgrs*
5. Per Server2, completare il seguente passo:

a. Creare la cartella, /MQHA, per montare il file system condiviso. Mantenere lo stesso percorso di Server1. Ad esempio:

i) **mkdir** */MQHA*

6. 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 .
   a. **chown -R** mqm:mqm */MQHA*
   b. **chmod -R** ug+rwx */MQHA*
7. Creare il gestore code immettendo il seguente comando: **crtmqm -ld** */MQHA/logs* **-md** */MQHA/qmgrs QM1*
8. Aggiungi[2]Da /MQHA *(rw,sync,no_wdelay,fsid=0) a /etc/exports
9. Per Server1, completare la seguente procedura:
   a. Avviare il daemon NFS : */etc/init.d/* **nfs** start
   b. 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
```

10. Per Server2, completare la seguente procedura:
    a. Montare il file system esportato /MQHA immettendo il seguente comando: **mount -t** nfs4 **-o** hard,intr *Server1:/ /MQHA*
    b. 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
```

11. 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 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.

Linux *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

[2] '*' consente a tutte le macchine che possono raggiungere questo montaggio /MQHA per la lettura/scrittura. Limitare l'accesso su una macchina di produzione.

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 517. 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.

Nell'esempio, il client è in esecuzione su Windows 7 Service Pack 1. Il sistema ospita due server VMware Linux che eseguono il gestore code a più istanze.

Verifica del failover utilizzando IBM MQ Explorer

Prima di utilizzare le applicazioni di esempio per verificare il failover, eseguire IBM 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 il IBM 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 IBM MQ Explorer, arrestare l'istanza del gestore code attivo, consentendo la commutazione all'istanza in standby e istruendo i client riconnettibili 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 per ristabilire tutte e tre le connessioni. 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
```

Multi *Eliminazione di un gestore code a più istanze*

Su Multiplatforms, per eliminare completamente un gestore code a più istanze, utilizzare il comando **dltmqm** per eliminare il gestore code e 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*.

Linux UNIX 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 QM1 o

dltmqm QM1

Multi *Avvio e arresto di un gestore code a più istanze*

Avvio e arresto di un gestore code configurato su Multiplatforms 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, IBM MQ non ha alcun controllo su quale istanza diventa 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.

Multi *File system condiviso*

Su piattaforme multiple, un gestore code a più istanze utilizza un filesystem 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 IBM MQ su un supporto alternativo e, se il supporto di log primario ha esito negativo, eseguire il ripristino utilizzando i log sul supporto alternativo. È possibile utilizzare un gestore code di backup per gestire questo processo.

Multi *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.

Multi *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 da IBM MQ classes for 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 se le applicazioni connesse localmente all'istanza non riuscita si sono disconnesse dall'istanza non riuscita.

Le applicazioni connesse localmente devono terminare o disconnettersi da un'istanza del gestore code non riuscita per poter riavviare l'istanza non riuscita. 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.

Multi *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 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 da IBM MQ classes for 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. La riconnessione IBM MQ non modifica o reinstrada 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. I client devono essere compilati per essere eseguiti con librerie client IBM WebSphere MQ 7.0.1 o superiori. Devono essere connessi ad almeno un gestore code IBM WebSphere MQ 7.0.1 .

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.

Multi *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 recupero dell'applicazione è la perdita del contesto condiviso tra IBM MQ MQI client e il gestore code e memorizzato nel gestore code. IBM MQ MQI client ripristina la maggior parte del contesto, ma ci sono alcune parti del contesto che 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

Dalla prospettiva della consegna dei messaggi, il failover non modifica le proprietà persistenti della messaggistica IBM 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 non è riuscita. 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 da IBM MQ classes for Java.

Con un'applicazione IBM MQ MQI client , 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. I programmi server IBM MQ in genere non vengono riavviati sull'istanza del gestore code in standby quando un'istanza del gestore code a più istanze ha esito negativo.

È possibile automatizzare il riavvio di un programma server IBM MQ sul 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 IBM MQ MQI client elabora l'input dei messaggi persistenti da una coda e inserisce le risposte dei 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 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 526.

Sono disponibili tre modelli di progettazione alternativi per le applicazioni IBM MQ MQI client in seguito a 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_BROKENo MQRC_Q_MGR_NOT_AVAILABLE dalla successiva chiamata MQI dopo la perdita della connessione. L'applicazione deve eliminare tutte le informazioni sullo stato IBM MQ , come gli handle di coda, ed emettere una nuova chiamata MQCONN o MQCONNX per stabilire una nuova connessione, quindi riaprire gli oggetti IBM 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, è stato fornito un esempio, “2” a pagina 526, di un IBM MQ MQI client 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 conoscere il modo in cui la riconnessione modifica lo stato di un IBM MQ MQI client per progettare l'applicazione client in modo che sopravviva 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 IBM 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 IBM MQ MQI client è consapevole del failover stesso e ripristina il maggior numero possibile di contesti, dopo la riconnessione, memorizzando alcune informazioni di stato nel client ed emettendo ulteriori chiamate MQI per conto dell'applicazione client per ripristinare il suo stato IBM 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 programma di gestione degli errori potrebbe disconnettersi da IBM MQ e riconnettersi di nuovo oppure arrestare del tutto il programma. Per migliorare la continuità, potrebbe essere necessario gestire 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 MQPUT chiamata all'esterno del punto di sincronizzazione restituisce MQRC_CALL_INTERRUPTED se IBM MQ MQI client non sa se il messaggio è stato consegnato correttamente al gestore code. La riconnessione durante MQCMIT funziona in modo simile.
- MQRC_CALL_INTERRUPTED viene restituito - dopo una riconnessione riuscita - se IBM MQ MQI client 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 in base al nome (perché un'altra applicazione l'ha già creata), quando si verifica la riconnessione, IBM MQ MQI client 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.

Multi *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 IBM MQ vengono associate ai supporti di archiviazione, per utilizzare al meglio i supporti. Per i gestori code *a più istanze* , esiste una distinzione importante tra due tipi di file e directory IBM 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.

- File eseguibili IBM MQ e la directory tools. 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 IBM MQ, ad esempio il file `mqs.ini` su sistemi Windows, UNIX and Linux o parte della propria gestione della configurazione, come 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`. Su Windows la directory dei dati predefinita è la directory di installazione IBM 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 MQ Availability

Le applicazioni stanno utilizzando altre funzionalità IBM MQ per migliorare la disponibilità. I gestori code a più istanze completano altre capacità di alta disponibilità.

IBM 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

z/OS 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.

IBM MQ I client aumentano la disponibilità delle applicazioni

I programmi IBM MQ MQI client possono connettersi a gestori code differenti 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 da IBM MQ classes for 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.

MQ Adv. Linux V 9.1.0 Alta disponibilità RDQM

RDQM (gestore code di dati replicati) è una soluzione alta disponibilità disponibile su piattaforme Linux .

Una configurazione RDQM è composta da tre server configurati in un gruppo HA (High Availability), ciascuno con una istanza del gestore code. Un'istanza è il gestore code in esecuzione, che replica in modo sincrono i dati nelle altre due istanze. Se il server su cui è in esecuzione questo gestore code ha esito negativo, viene avviata un'altra istanza del gestore code con cui devono operare i dati correnti. Le tre istanze del gestore code condividono un indirizzo IP mobile, pertanto i clienti devono essere configurati solo con un singolo indirizzo IP. Solo un'istanza del gestore code può essere eseguita contemporaneamente, anche se il gruppo HA viene partizionato a causa di problemi di rete. Il server che esegue il gestore code è noto come 'primario ', ciascuno degli altri due server è noto come 'secondario'.

Tre nodi sono utilizzati per ridurre notevolmente la possibilità che si verifichi una situazione di divisione del cervello. In un sistema ad alta disponibilità a due nodi, la divisione del cervello può verificarsi quando la connettività tra i due nodi è interrotta. Senza connettività, entrambi i nodi potrebbero eseguire il gestore code contemporaneamente, accumulando dati differenti. Quando la connessione viene ripristinata, ci sono due versioni differenti dei dati (un 'split-brain ') e l'intervento manuale è richiesto per decidere quale serie di dati conservare e quale scartare.

RDQM utilizza un sistema a tre nodi con quorum per evitare la situazione di divisione del cervello. I nodi che possono comunicare con almeno uno degli altri nodi formano un quorum. I gestori code possono essere eseguiti solo su un nodo con quorum. Il gestore code non può essere eseguito su un nodo che non è connesso ad almeno un altro nodo, quindi non può essere eseguito su due nodi contemporaneamente:

- Se si verifica un malfunzionamento di un singolo nodo, il gestore code può essere eseguito su uno degli altri due nodi. Se due nodi hanno esito negativo, il gestore code non può essere eseguito sul nodo rimanente perché il nodo non ha il quorum (il nodo rimanente non è in grado di determinare se gli altri due nodi hanno avuto esito negativo o se sono ancora in esecuzione e hanno perso la connettività).
- Se un singolo nodo perde la connettività, il gestore code non può essere eseguito su questo nodo perché il nodo non ha il quorum. Il gestore code può essere eseguito su uno dei due nodi rimanenti, che hanno il quorum. Se tutti i nodi perdono la connettività, il gestore code non può essere eseguito su nessuno dei nodi, poiché nessuno dei nodi ha il quorum.

Nota: IBM MQ Console non supporta i gestori code di dati replicati. È possibile utilizzare IBM MQ Explorer con gestori code di dati replicati, ma questo non visualizza le informazioni specifiche delle funzioni RDQM.

La configurazione del gruppo dei tre nodi è gestita da Pacemaker. La replica tra i tre nodi è gestita da DRBD. (Consultare https://clusterlabs.org/pacemaker/ per informazioni su Pacemaker e https://docs.linbit.com/docs/users-guide-9.0/ per informazioni su DRBD.)

È possibile eseguire il backup dei gestori code di dati replicati utilizzando il processo descritto in “Backup dei dati del gestore code” a pagina 622. L'arresto del gestore code e il backup non ha alcun effetto sul monitoraggio del nodo eseguito dalla configurazione RDQM.

La seguente figura mostra una distribuzione tipica con un RDQM in esecuzione su ognuno dei tre nodi nel gruppo HA.

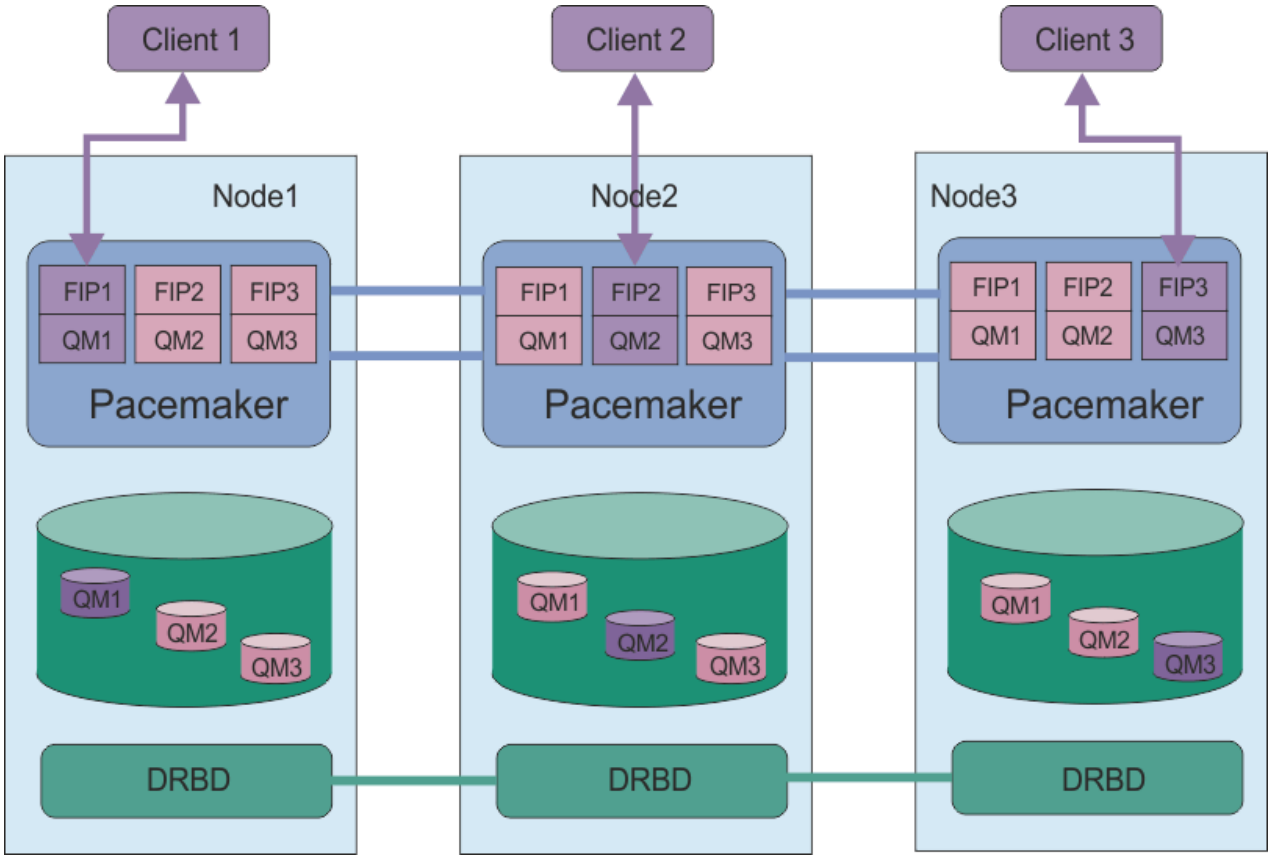


Figura 81. Esempio di gruppo HA con tre RDQM

Nella figura successiva, Node3 ha avuto esito negativo, i collegamenti Pacemaker sono stati persi e il gestore code QM3 viene eseguito su Node2 .

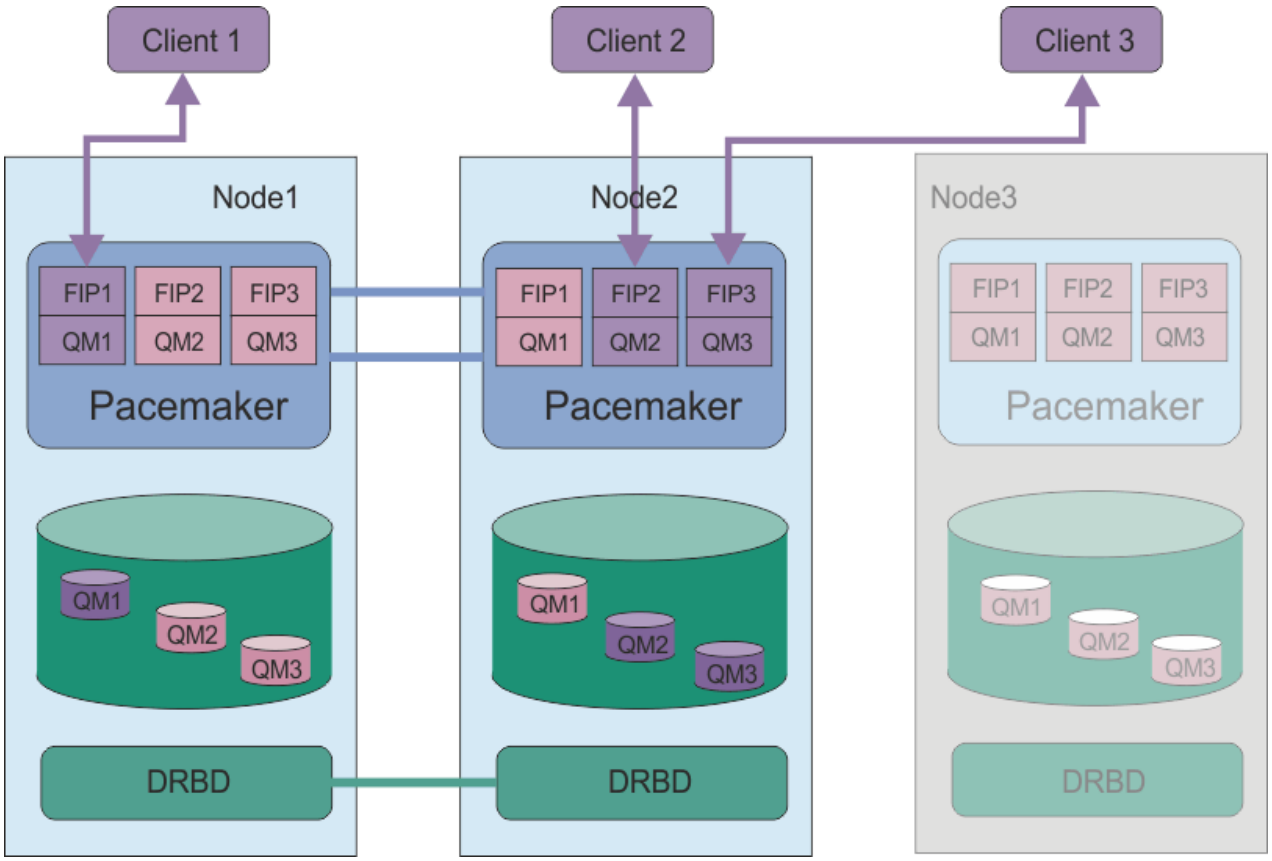


Figura 82. Esempio dopo l'esito negativo di node3

Nota: Quando i gestori code eseguono il failover su un altro nodo, conservano lo stato che avevano al failover. I gestori code in esecuzione vengono avviati, i gestori code arrestati rimangono arrestati.

Attività correlate

Installazione di RDQM (gestori code di dati replicati)

Aggiornamento di RDQM (gestori code di dati replicati)

Migrazione dei gestori code di dati replicati

Linux V 9.1.0 *Requisiti per la soluzione RDQM HA*

È necessario soddisfare diversi requisiti prima di configurare il gruppo HA (High Availability) RDQM.

Requisiti di sistema

Prima di configurare il gruppo HA RDQM, è necessario completare alcune operazioni di configurazione su ognuno dei tre server che fanno parte del gruppo HA.

- Ogni nodo richiede un gruppo di volumi denominato `drbdpool`. La memoria per ogni gestore code di dati replicati viene assegnata come un volume logico separato per gestore code da questo gruppo di volumi. Per prestazioni ottimali, questo gruppo di volumi deve essere costituito da uno o più volumi fisici che corrispondono alle unità disco interne (preferibilmente SSD). È possibile creare `drbdpool` prima o dopo aver installato la soluzione RDQM HA, ma è necessario creare `drbdpool` prima di creare effettivamente qualsiasi RDQM. Verificare la configurazione del gruppo di volumi utilizzando il comando **vgs** . L'output dovrebbe essere simile al seguente:

```
  VG       #PV #LV #SN Attr   VSize   VFree
  drbdpool   1   9   0 wz--n- <16.00g <7.00g
  rhel       1   2   0 wz--n- <15.00g     0
```

In particolare, verificare che non vi sia alcun carattere c nella sesta colonna degli attributi (ovvero, `wz--nc`). c indica che il clustering è abilitato e, se lo è, è necessario eliminare il gruppo volumi e ricrearlo senza clustering.

- Dopo aver creato il gruppo di volumi `drbdpool` , non eseguire altre operazioni. IBM MQ gestisce i volumi logici creati in `drbdpool`e come e dove sono montati.
- Ogni nodo richiede un massimo di tre interfacce utilizzate per configurare il supporto RDQM:
  - Un'interfaccia primaria per Pacemaker per monitorare il gruppo HA.
  - Un'interfaccia alternativa per Pacemaker per monitorare il gruppo HA.
  - Un'interfaccia per la replica di dati sincrona, nota come interfaccia di replica. Deve avere una larghezza di banda sufficiente per supportare i requisiti di replica dato il carico di lavoro previsto di tutti i gestori code di dati replicati in esecuzione nel gruppo HA.

  È possibile configurare il gruppo HA in modo che lo stesso indirizzo IP venga utilizzato per tutte e tre le interfacce, un indirizzo IP separato viene utilizzato per ciascuna interfaccia o lo stesso indirizzo IP viene utilizzato per l'indirizzo principale e alternativo e un indirizzo IP separato per l'interfaccia di replica.

  Per la massima tolleranza di errore, queste interfacce devono essere NIC (Network Interface Card) indipendenti.
- DRBD richiede che ogni nodo nel gruppo HA abbia un nome host internet valido (il valore restituito da `uname -n`), come definito da RFC 952 modificato da RFC 1123.
- Se è presente un firewall tra i nodi nel gruppo HA, il firewall deve consentire il traffico tra i nodi su un intervallo di porte. Viene fornito uno script di esempio, `/opt/mqm/samp/rdqm/firewalld/configure.sh`, che apre le porte necessarie se si sta eseguendo il firewall standard in RHEL. È necessario eseguire lo script come `root`. Se si utilizza un altro firewall, esaminare le definizioni di servizio `/usr/lib/firewalld/services/rdqm*` per vedere quali porte devono essere aperte.
- Se il sistema utilizza SELinux in modalità di forzatura, è necessario eseguire il seguente comando:

```
semanage permissive -a drbd_t
```

Requisiti di rete

Si consiglia di individuare i tre nodi nel gruppo HA RDQM nello stesso centro dati.

Se si sceglie di individuare i nodi in data center differenti, tenere presente le seguenti limitazioni:

- Le prestazioni peggiorano rapidamente con l'aumento della latenza tra i data center. Anche se IBM supporterà una latenza fino a 5 ms, potresti scoprire che le prestazioni della tua applicazione non possono tollerare più di 1 o 2 ms di latenza.
- I dati inviati attraverso il link di replicazione non sono soggetti ad alcuna ulteriore crittografia oltre a quella che potrebbe essere in atto utilizzando IBM MQ AMS.

È possibile configurare un indirizzo IP mobile per consentire a un client di utilizzare lo stesso indirizzo IP per un gestore code di dati replicati (RDQM) indipendentemente dal nodo nel gruppo HA su cui è in esecuzione. L'indirizzo mobile si collega a un'interfaccia fisica denominata sul nodo primario per RDQM. Se l'RDQM esegue il failover e un nodo differente diventa il nodo primario, l'IP mobile viene collegato a un'interfaccia con lo stesso nome sul nuovo primario. Le interfacce fisiche sui tre nodi devono tutti avere lo stesso nome e appartenere alla stessa sottorete dell'indirizzo IP mobile.

Requisiti utente per configurare il cluster

È possibile configurare il gruppo HA RDQM come utente `root`. Se non si desidera eseguire la configurazione come `root`, eseguire la configurazione come utente nel gruppo `mqm` . Affinché un utente `mqm` configuri il cluster RDQM, è necessario soddisfare i seguenti requisiti:

- L'utente `mqm` deve essere in grado di utilizzare sudo per eseguire comandi su ciascuno dei tre server che costituiscono il gruppo HA RDQM.

- Se l'utente mqm può utilizzare SSH senza una password per eseguire i comandi su ciascuno dei tre server che costituiscono il gruppo HA RDQM, l'utente deve eseguire i comandi solo su uno dei server.
- Se si configura SSH senza password per l'utente mqm , tale utente deve avere lo stesso UID su tutti e tre i server.

È necessario configurare sudo in modo che l'utente mqm possa eseguire i seguenti comandi con autorizzazione root:

```
/opt/mqm/bin/crtmqm
/opt/mqm/bin/dltmqm
/opt/mqm/bin/rdqmadm
/opt/mqm/bin/rdqmstatus
```

Requisiti utente per l'utilizzo dei gestori code

Per creare, eliminare o configurare i gestori code di dati replicati (RDQM), è necessario utilizzare un ID utente che appartiene ai gruppi mqm e haclient (il gruppo haclient viene creato durante l'installazione di Pacemaker).

Configurazione di SSH senza password

È possibile impostare SSH senza password in modo che sia necessario immettere solo comandi di configurazione su un nodo nel gruppo HA.

Informazioni su questa attività

Per impostare SSH senza password, devi configurare l'id mqm su ogni nodo, quindi generare una chiave su ogni nodo per quell' utente. Si distribuiscono quindi le chiavi agli altri nodi e si verifica la connessione per aggiungere ciascun nodo all'elenco di host noti. Infine, si blocca l'id mqm .

Nota: Le istruzioni presuppongono che si stia definendo un gruppo HA con interfacce primarie, alternative e di replica separate e che si definisca quindi l'accesso SSH senza password sulle interfacce primaria e alternativa. Se intendi configurare un sistema con un singolo indirizzo IP, definisci l'accesso SSH senza password su quella singola interfaccia.

Procedura

1. Su ciascuno dei tre nodi, completa la seguente procedura per configurare l'utente mqm e generare una chiave SSH:
   a) Modificare la directory home di mqm in /home/mqm:

   ```
   usermod -d /home/mqm mqm
   ```

   b) Creare la directory /home/mqm :

   ```
   mkhomedir_helper mqm
   ```

   c) Aggiungere la password mqm :

   ```
   passwd mqm
   ```

   d) Eseguire la shell interattiva come mqm:

   ```
   su mqm
   ```

   e) Generare la chiave di autenticazione mqm :

   ```
   ssh-keygen -t rsa -f /home/mqm/.ssh/id_rsa -N ''
   ```

2. Su ciascuno dei tre nodi, completare la seguente procedura per aggiungere la chiave del nodo agli altri due nodi e verificare le connessioni per ogni nodo primario e (se utilizzato) gli indirizzi alternativi:
   a) Aggiungere la chiave ai nodi remoti

```
ssh-copy-id -i /home/mqm/.ssh/id_rsa.pub remote_node1_primary_address
ssh-copy-id -i /home/mqm/.ssh/id_rsa.pub remote_node1_alternate_address
ssh-copy-id -i /home/mqm/.ssh/id_rsa.pub remote_node2_primary_address
ssh-copy-id -i /home/mqm/.ssh/id_rsa.pub remote_node2_alternate_address
```

b) Controllare ssh senza password e aggiornare known_hosts per i nodi remoti:

```
ssh remote_node1_primary_address uname -n
ssh remote_node1_alternate_address uname -n
ssh remote_node2_primary_address uname -n
ssh remote_node2_alternate_address uname -n
```

Per ogni connessione, viene richiesto di confermare che si desidera procedere. Confermare per ognuno di aggiornare known_hosts. È necessario completare questa operazione prima di tentare di configurare il gruppo HA utilizzando SSH senza password.

c) Uscire dalla shell interattiva come `mqm`:

```
exit
```

3. Su ciascun nodo, come root, completare la seguente procedura per eliminare la password `mqm` e bloccare l'ID:
   a) Rimuovere la password `mqm` :

```
passwd -d mqm
```

   b) Blocca `mqm`:

```
passwd -l mqm
```

4. Su ogni nodo, come root, completa la seguente procedura per configurare l'accesso sudo per l'utente `mqm` :
   a) Modificare il file `sudoers` utilizzando il comando **`visudo`** :

```
visudo
```

   b) Cercare la linea "`## Allows people in group wheel to run all commands`" e aggiungere il seguente testo sotto la linea:

```
#%mqm    ALL=(ALL)       ALL
```

   c) Cercare la linea "`## Same thing without a password`" e aggiungere il seguente testo sotto la linea:

```
%mqm            ALL=(ALL)       NOPASSWD: ALL
```

Linux V 9.1.0 *Definizione del cluster Pacemaker (gruppo HA)*

Il gruppo HA è un cluster Pacemaker . Definire il cluster Pacemaker modificando il file `/var/mqm/rdqm.ini` ed eseguendo il comando **`rdqmadm`** .

Informazioni su questa attività

Consultare https://clusterlabs.org/pacemaker/ per informazioni su Pacemaker. È possibile creare il cluster Pacemaker come utente nel gruppo `mqm` se l'utente `mqm` può utilizzare `sudo`. Se l'utente può anche eseguire l'SSH su ciascun server senza una password, è necessario modificare solo il file `rdqm.ini` ed eseguire **`rdqmadm`** su uno dei server per creare il cluster Pacemaker . Altrimenti, è necessario creare il file ed eseguire il comando come `root` su ciascuno dei server che devono essere nodi.

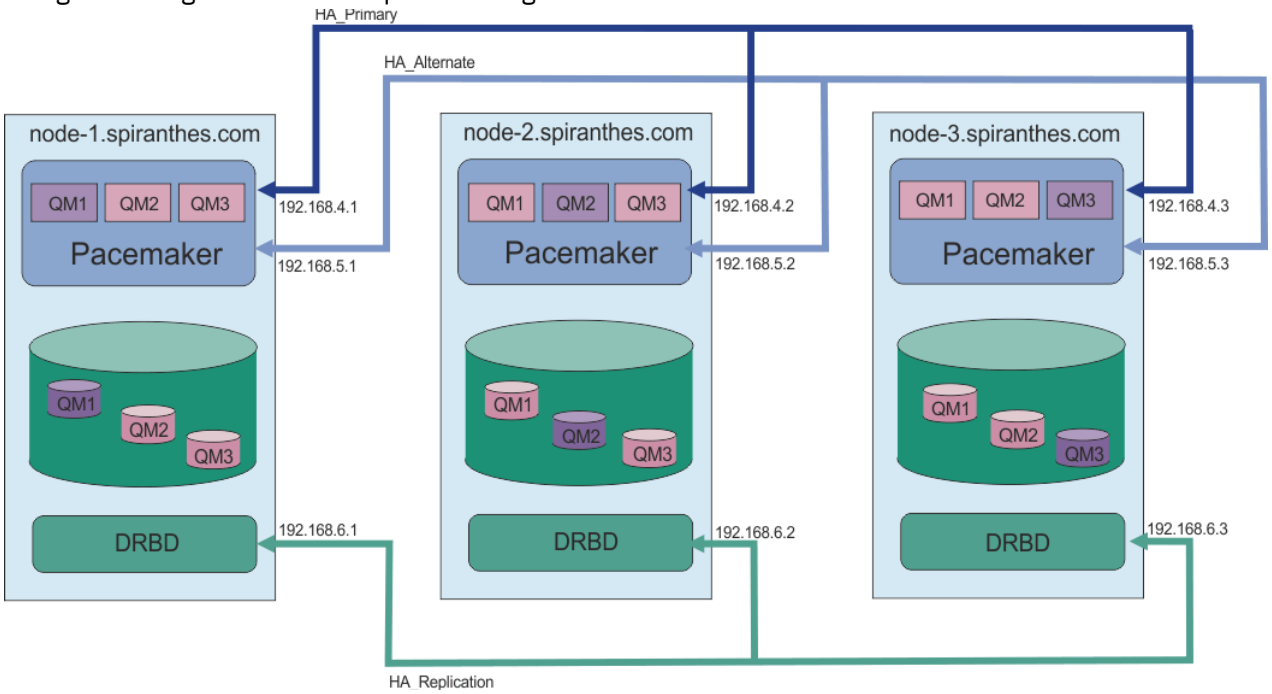
Il file `rdqm.ini` fornisce gli indirizzi IP per tutti i nodi nel cluster Pacemaker . È possibile definire le interfacce `HA_Primary` e `HA_Secondary` utilizzate per Pacemaker per monitorare il sistema, ma Pacemaker può invece utilizzare l'interfaccia di replica, denominata `HA_Replication`, per questo scopo, se necessario. L'interfaccia `HA_Replication` deve avere una larghezza di banda sufficiente per

supportare i requisiti di replica dato il carico di lavoro previsto di tutti gli RDQM in esecuzione nel gruppo HA.

Il seguente file di esempio mostra la configurazione per un cluster Pacemaker di esempio che utilizza un indirizzo IP separato per ogni interfaccia:

```
Node:
  HA_Primary=192.168.4.1
  HA_Alternate=192.168.5.1
  HA_Replication=192.168.6.1
Node:
  HA_Primary=192.168.4.2
  HA_Alternate=192.168.5.2
  HA_Replication=192.168.6.2
Node:
  HA_Primary=192.168.4.3
  HA_Alternate=192.168.5.3
  HA_Replication=192.168.6.3
```

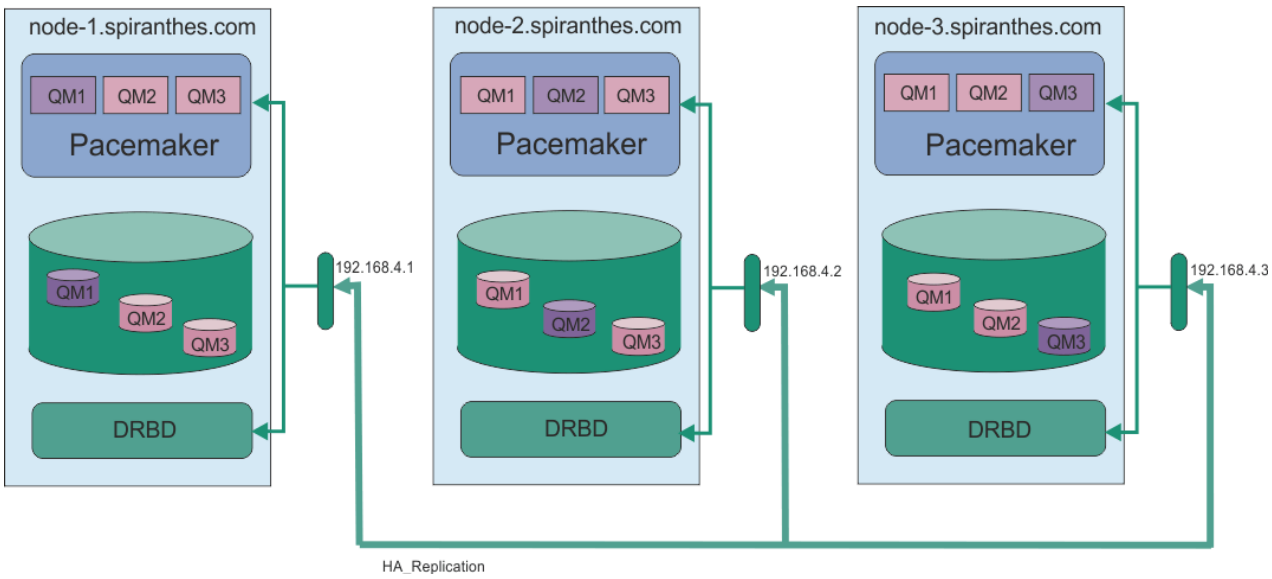
Il seguente diagramma illustra questa configurazione:



Il seguente file di esempio mostra la configurazione di un esempio di cluster Pacemaker che utilizza l'interfaccia `HA_Replication` per il monitoraggio. In questo caso, specificare solo l'interfaccia `HA_Replication` :

```
Node:
  HA_Replication=192.168.4.1
Node:
  HA_Replication=192.168.4.2
Node:
  HA_Replication=192.168.4.3
```

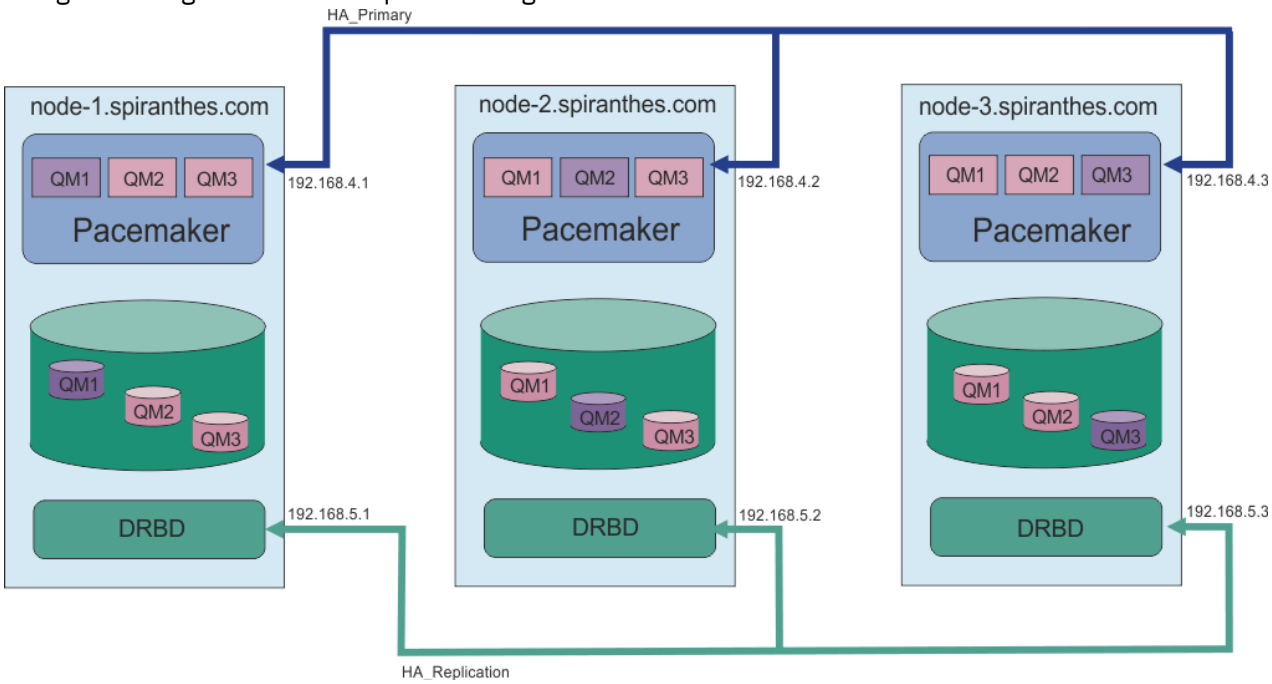
Il seguente diagramma illustra questa configurazione:



Se si desidera utilizzare due indirizzi IP, il file `rdqm.ini` ha un campo `HA_Primary` e un campo `HA_Replication` per ciascun nodo, ma non un campo `HA_Alternate` :

```
Node:
  HA_Primary=192.168.4.1
  HA_Replication=192.168.5.1
Node:
  HA_Primary=192.168.4.2
  HA_Replication=192.168.5.2
Node:
  HA_Primary=192.168.4.3
  HA_Replication=192.168.5.3
```

Il seguente diagramma illustra questa configurazione:



L'ordine in cui si specificano i nodi deve essere lo stesso in tutti i file `rdqm.ini` nella configurazione. I tre nodi devono avere una vista comune per cui uno è Node1, un Node2 e così via.

Procedura

- Per definire il cluster Pacemaker come utente `root`:
  a) Modificare il file `/var/mqm/rdqm.ini` su uno dei tre server in modo che il file definisca il cluster.
  b) Copiare il file negli altri due server che saranno nodi nel cluster Pacemaker .
  c) Eseguire il seguente comando come `root` su ognuno dei tre server:

```
rdqmadm -c
```

- Per definire il cluster Pacemaker come utente nel gruppo `mqm` su ciascun nodo:
  a) Assicurarsi che l'utente `mqm` possa utilizzare **sudo** per eseguire comandi.
  b) Modificare il file `/var/mqm/rdqm.ini` su uno dei tre server in modo che il file definisca il cluster Pacemaker .
  c) Copiare `/var/mqm/rdqm.ini` negli altri due server che saranno nodi nel cluster Pacemaker .
  d) Immettere il seguente comando su ciascun server:

```
rdqmadm -c
```

- Per definire il cluster Pacemaker come utente nel gruppo `mqm` da un nodo:
  a) Assicurarsi che l'utente `mqm` possa utilizzare **sudo** per eseguire i comandi e, facoltativamente, connettersi a ciascun server utilizzando SSH senza una password.
  b) Modificare il file `/var/mqm/rdqm.ini` su uno dei tre server in modo che il file definisca il cluster Pacemaker .
  c) Esegui il seguente comando:

```
rdqmadm -c
```

Riferimenti correlati

rdqmadm (gestione cluster gestore code dati replicati)

Linux V 9.1.0 *Eliminazione del cluster Pacemaker (gruppo HA)*

Il gruppo HA è un cluster Pacemaker . È possibile eliminare una configurazione cluster Pacemaker eseguendo il comando **rdqmadm** con l'opzione `-u` .

Informazioni su questa attività

Non è possibile eliminare la configurazione del cluster Pacemaker se i gestori code di dati replicati esistono ancora su uno dei nodi.

Procedura

- Per eliminare la configurazione del cluster Pacemaker , immettere il seguente comando da uno dei nodi:

```
rdqmadm -u
```

Riferimenti correlati

rdqmadm (gestione cluster gestore code dati replicati)

Linux V 9.1.0 ***Creazione di un RDQM HA***

Utilizzare il comando **crtmqm** per creare un gestore code di dati replicati ad alta disponibilità (RDQM).

Informazioni su questa attività

È possibile creare un gestore code dati replicati ad alta disponibilità (RDQM) come utente nel gruppo `mqm` se l'utente mqm può utilizzare sudo. Se l'utente può anche eseguire SSH su ogni nodo senza una

password, è necessario eseguire il comando di creazione RDQM solo su un nodo per creare RDQM su tutti e tre i nodi. Altrimenti, è necessario essere `root` per creare un RDQM ed eseguire i comandi su tutti e tre i nodi.

Procedura

- Per creare un RDQM come utente nel gruppo `mqm` :
  a) Assicurarsi che l'utente `mqm` possa utilizzare **sudo** per eseguire i comandi e che possa connettersi a ciascun server utilizzando SSH senza una password.
  b) Immettere il seguente comando:

  ```
  crtmqm -sx [-fs FilesystemSize] qmname
  ```

  dove *qmname* è il nome del gestore code di dati replicati. Facoltativamente, è possibile specificare la dimensione del file system per il gestore code (ossia, la dimensione del volume logico creato nel gruppo di volumi drbdpool).

  Il comando tenta di utilizzare SSH per connettersi agli altri nodi nel cluster come utente `mqm` . Se la connessione ha esito positivo, le istanze secondarie del gestore code vengono create sui nodi. In caso contrario, è necessario creare le istanze secondarie ed eseguire il comando **`crtmqm -sx`** (come descritto per l'utente `root`).
- Per creare un RDQM come utente `root`:
  a) Immettere il comando riportato di seguito su ciascuno dei nodi che devono ospitare le istanze secondarie di RDQM:

  ```
  crtmqm -sxs [-fs FilesystemSize] qmname
  ```

  dove *qmname* è il nome del gestore code di dati replicati. Facoltativamente, è possibile specificare la dimensione del file system per il gestore code (ossia, la dimensione del volume logico creato nel gruppo di volumi drbdpool). È necessario specificare la stessa dimensione del file system per RDQM su tutti e tre i nodi nel gruppo HA.

  Il comando crea un'istanza secondaria di RDQM.
  b) Sul nodo rimanente, immettere il seguente comando:

  ```
  crtmqm -sx [-fs FilesystemSize] qmname
  ```

  dove *qmname* è il nome del gestore code di dati replicati. Facoltativamente, è possibile specificare la dimensione del filesystem per il gestore code.

  Il comando determina se l'istanza secondaria del gestore code esiste sugli altri due nodi. Se esistono comandi secondari, il comando crea e avvia il gestore code primario. Se i secondari non esistono, viene richiesto di eseguire il comando **`crtmqm -sxs`** su ciascuno dei nodi.

  Oltre agli argomenti DataPath (**`-md`**) e LogPath (**`-ld`**), tutti gli argomenti validi per la creazione di un gestore code standard Linux sono validi anche per un gestore code di dati replicati primario.

  Nota: Quando si crea un RDQM, per il link di replica viene assegnato il successivo numero di porta libero superiore a 7000. Se viene rilevato che la porta scelta è utilizzata da un'altra applicazione, il comando **`crtmqm`** ha esito negativo con l'errore AMQ6543 e tale porta viene aggiunta a un elenco di esclusione. È possibile eliminare le istanze secondarie del gestore code, quindi eseguire nuovamente il comando **`crtmqm`** .

Riferimenti correlati
crtmqm

Linux V 9.1.0 *Eliminazione di un RDQM HA*
Utilizzare il comando **`dltmqm`** per eliminare un RDQM (high availability replicated data queue manager).

Informazioni su questa attività

È necessario eseguire il comando per eliminare RDQM sul nodo primario di RDQM. RDQM deve essere terminato per primo. È possibile eseguire il comando come un utente mqm se tale utente dispone dei privilegi sudo necessari. Altrimenti, è necessario eseguire il comando come root. Una volta eliminate le risorse associate al gestore code primario, il comando tenta di eliminare i gestori code secondari utilizzando ssh per connettersi agli altri nodi. Se questa eliminazione non riesce, è necessario eseguire `dltmqm` manualmente sugli altri nodi per completare il processo. Su un nodo secondario, il comando ha esito negativo se il gestore code primario non è stato già eliminato.

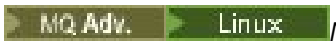
Procedura

- Per eliminare un RDQM, immettere il seguente comando:

```
dltmqm RDQM_name
```

Riferimenti correlati

dltmqm



Migrazione di un gestore code per diventare un gestore code HA RDQM

È possibile migrare un gestore code esistente per diventare un gestore code di dati replicati (RDQM) HA (high availability) eseguendo il backup dei relativi dati persistenti, quindi ripristinando i dati in un gestore code RDQM appena creato con lo stesso nome.

Informazioni su questa attività

I gestori code di dati replicati HA richiedono un volume logico dedicato (file system) e la configurazione della replica del disco e del controllo HA. Questi componenti vengono configurati solo quando viene creato un nuovo gestore code. Un gestore code esistente può essere migrato per utilizzare RDQM eseguendo il backup dei dati persistenti, quindi ripristinando i dati su un gestore code RDQM appena creato con lo stesso nome. Questa procedura conserva la configurazione del gestore code, lo stato e i messaggi persistenti al momento della creazione del backup.

Nota: È possibile migrare un gestore code solo da una versione di IBM MQ uguale o inferiore alla versione in cui è installato RDQM. Anche il sistema operativo e l'architettura devono essere uguali. Altrimenti, è necessario creare un nuovo gestore code sulla piattaforma di destinazione; fare riferimento a Spostamento di un gestore code su un sistema operativo differente.

È necessario soddisfare le seguenti condizioni prima di migrare un gestore code:

- Valutare i requisiti di alta disponibilità e consultare “Alta disponibilità RDQM” a pagina 531.
- Esaminare le applicazioni e i gestori code che si connettono al gestore code. Considerare le modifiche richieste per instradare le connessioni al nodo RDQM su cui è in esecuzione il gestore code. Ad esempio, se si configura l'alta disponibilità RDQM, è possibile considerare l'utilizzo di un indirizzo IP mobile, consultare “Creazione ed eliminazione di un indirizzo IP mobile” a pagina 548.
- Eseguire il provisioning o identificare i nodi RDQM esistenti per la configurazione scelta. Per informazioni relative ai requisiti di sistema per RDQM, consultare “Requisiti per la soluzione RDQM HA” a pagina 533.
- Installare IBM MQ Advanced, che include la funzione RDQM, su ciascun nodo.
- Configurare la configurazione del gruppo HA RDQM, consultare “Definizione del cluster Pacemaker (gruppo HA)” a pagina 536.
- Facoltativamente, verificare la configurazione RDQM utilizzando un gestore code di prova, che può quindi essere eliminato. La verifica della configurazione è consigliata per identificare e risolvere eventuali problemi prima di migrare il gestore code.
- Esaminare la configurazione della sicurezza per il gestore code, quindi replicare gli utenti e i gruppi locali richiesti su ciascun nodo RDQM.
- Esaminare il gestore code e la configurazione del canale per determinare se vengono utilizzate le uscite API, le uscite canale o le uscite di conversione dati. Installare le uscite richieste su ciascun nodo RDQM.

- Esaminare i servizi del gestore code che sono stati definiti, quindi installare e configurare i processi richiesti su ciascun nodo RDQM.

Procedura

1. Eseguire il backup del gestore code esistente:
   a) Arrestare il gestore code esistente emettendo un comando di attesa arresto `endmqm -w` o un comando di arresto immediato `endmqm -i`. Questa operazione è importante per garantire la congruenza dei dati nel backup.
   b) Determinare l'ubicazione della directory dei dati del gestore code visualizzando il file di configurazione IBM MQ , `mqs.ini`. Su Linux, questo file si trova nella directory `/var/mqm` . Per ulteriori informazioni su `mqs.ini`, consultare “File di configurazione IBM MQ , mqs.ini” a pagina 84.

      Individuare la sezione `QueueManager` per il gestore code nel file. Se la stanza contiene una chiave denominata `DataPath` , il suo valore è la directory dei dati del gestore code. Se la chiave non esiste, la directory dei dati del gestore code può essere determinata utilizzando i valori delle chiavi `Prefix` e `Directory` . La directory dei dati del gestore code è una concatenazione di questi valori, nel formato *prefisso*/qmgrs/*directory*. Per ulteriori informazioni sulla stanza QueueManager , consultare “Stanza QueueManager del file mqs.ini” a pagina 95.
   c) Creare un backup della directory dei dati del gestore code. Su Linux, è possibile eseguire questa operazione utilizzando il comando **`tar`** . Ad esempio, per eseguire il back up della directory di dati per un gestore code è possibile utilizzare il seguente comando. Notare l'ultimo parametro del comando, che è un singolo punto (punto):

      ```
      tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
      ```

   d) Determinare l'ubicazione della directory di log del gestore code visualizzando IBM MQ file di configurazione del gestore code `qm.ini`. Questo file si trova nella directory dei dati del gestore code. Per ulteriori informazioni sul file, consultare “File di configurazione del gestore code, qm.ini” a pagina 97.

      La directory di log del gestore code è definita come il valore della chiave `LogPath` nella stanza `Log` . Per informazioni sulla sezione, consultare “Stanza di log del file qm.ini” a pagina 125.
   e) Creare un backup della directory di log del gestore code. Su Linux, è possibile eseguire questa operazione utilizzando il comando tar. Ad esempio, per eseguire il back up della directory di log per un gestore code, è possibile utilizzare il seguente comando. Notare l'ultimo parametro del comando, che è un singolo punto (punto):

      ```
      tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
      ```

   f) Creare un backup dei repository dei certificati utilizzati dal gestore code se non si trovano nella directory dei dati del gestore code. Verificare che sia il file del database delle chiavi che il file stash delle password siano sottoposti a backup. Per informazioni sul repository delle chiavi del gestore code, consultare Il repository delle chiavi SSL/TLS e Individuazione del repository delle chiavi per un gestore code. Per informazioni sull'individuazione dell'archivio chiavi AMS se il gestore code è configurato per utilizzare l'intercettazione MCA (Message Channel Agent) AMS, consultare Intercettazione MCA (Message Channel Agent).
   g) Il gestore code esistente non è più richiesto, quindi può essere eliminato. Tuttavia, laddove possibile, è necessario eliminare il gestore code esistente solo dopo che è stato ripristinato correttamente nel sistema di destinazione. Il differimento dell'eliminazione garantisce che il gestore code possa essere riavviato se il processo di migrazione non viene completato correttamente.

      Nota: Se si rinvia l'eliminazione del gestore code esistente, non riavviarla. È importante che il gestore code rimanga chiuso perché ulteriori modifiche alla relativa configurazione o stato vengono perse durante la migrazione.
2. Preparare il nodo RDQM primario:

a) Creare un nuovo gestore code RDQM con lo stesso nome del gestore code di cui è stato eseguito il backup. Assicurarsi che il file system assegnato per il gestore code RDQM da **crtmqm** sia abbastanza grande da contenere i dati, i log primari e i log secondari per il gestore code esistente, oltre a spazio aggiuntivo per l'espansione futura. Per informazioni su come creare un gestore code RDQM, consultare “Creazione di un RDQM HA” a pagina 539.

b) Determinare il nodo RDQM primario per il gestore code. Per informazioni su come determinare il nodo primario, vedere rdqmstatus (visualizzazione dello stato RDQM).

c) Sul nodo RDQM primario, se il gestore code RDQM è avviato, arrestarlo utilizzando il comando `endmqm -w` o `endmqm -i` .

d) Sul nodo RDQM primario, stabilire l'ubicazione delle directory di dati e di log per il gestore code RDQM (utilizzare i metodi descritti nei passi 1b e 1d).

e) Sul nodo RDQM primario, eliminare il contenuto dei dati del gestore code RDQM e le directory di log, ma non le directory stesse.

3. Ripristinare il gestore code sul nodo RDQM primario:

a) Copiare i backup dei dati del gestore code e le directory di log nel nodo RDQM primario, oltre a eventuali backup separati dei repository dei certificati utilizzati dal gestore code.

b) Ripristinare il backup della directory di dati del gestore code nella directory di dati vuota per il nuovo gestore code RDQM, assicurando che la proprietà e le autorizzazioni del file siano conservate. Se il backup è stato creato utilizzando il comando tar di esempio nel passaggio 1c , l'utente root può utilizzare il seguente comando per ripristinarlo:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

c) Ripristinare il backup della directory di log del gestore code nella directory di log vuota per il nuovo gestore code RDQM, verificando che le autorizzazioni e la proprietà del file siano conservate. Se il backup è stato creato utilizzando il comando tar di esempio nel passo 1e , l'utente root può utilizzare il seguente comando per ripristinarlo:

```
tar -xvzpf qm-log.tar.gz -C queue_manager_log_dir
```

d) Modificare il file di configurazione del gestori code ripristinato, `qm.ini`, nella directory dei dati per il gestore code RDQM. Aggiornare il valore della chiave `LogPath` nella stanza `Log` per specificare la directory di log per il gestore code RDQM.

Esaminare gli altri percorsi file definiti nel file di configurazione e aggiornarli, se necessario. Ad esempio, potrebbe essere necessario aggiornare i seguenti percorsi:

- Il percorso per i file di log degli errori generati dai servizi di messaggi diagnostici.
- Il percorso per le uscite richieste dal gestore code.
- Il percorso per i file di caricamento switch se il gestore code è un coordinatore della transazione XA.

e) Se il gestore code è configurato per utilizzare l'intercettazione AMS Message Channel Agent (MCA), copiare il keystore AMS nella nuova installazione RDQM, quindi esaminare e aggiornare la configurazione. Il keystore deve essere disponibile su ciascun nodo RDQM, quindi se non è ubicato nel filesystem replicato per il gestore code, deve essere copiato su ciascun nodo. Per ulteriori informazioni, consultare Intercettazione MCA (Message Channel Agent).

f) Verificare che il Gestore code sia visualizzato dal comando **dspmq** e che il suo stato sia riportato come terminato. Il seguente esempio mostra l'output di esempio per un gestore code HA RDQM:

```
$ dspmq -o status -o ha
QMNAME(QM1) STATUS(Ended normally) HA(Replicated)
```

g) Verificare che i dati del gestore code ripristinati siano stati replicati sui nodi RDQM secondari utilizzando il comando **rdqmstatus** per visualizzare lo stato per il gestore code. Lo stato HA deve essere riportato come `Normal` su ciascun nodo. Il seguente esempio mostra l'output di esempio per un gestore code HA RDQM:

```
$ rdqmstatus -m QM1
Node:                           mqhavm10-adm
Queue manager status:           Ended normally
Queue manager file system:      50MB used, 0.2GB allocated [42%]
HA role:                        Primary
HA status:                      Normal
HA control:                     Disabled
HA current location:            This node
HA preferred location:          This node
HA floating IP interface:       None
HA floating IP address:         None

Node:                           mqhavm11-adm
HA status:                      Normal

Node:                           mqhavm12-adm
HA status:                      Normal
```

h) Avviare il gestore code sul nodo RDQM primario.

i) Connettersi al gestore code e aggiornare il valore dell'attributo del gestore code SSLKEYR per specificare la nuova ubicazione del repository dei certificati del gestore code. Per impostazione predefinita, il valore di questo attributo è impostato su *queue_manager_data_directory*/ssl/key. Il repository certificati deve essere ubicato nella stessa ubicazione su ciascun nodo RDQM. Se il repository non si trova nel file system replicato per il gestore code, deve essere copiato su ciascun nodo.

j) Esaminare le definizioni degli oggetti IBM MQ per il gestore code e aggiornare il valore degli attributi degli oggetti che fanno riferimento alle impostazioni di rete modificate, la directory di installazione di IBM MQ o la directory dei dati del gestore code, inclusi i seguenti oggetti:

- Indirizzi IP locali utilizzati dai listener (attributoIPADDR).
- Indirizzi IP locali utilizzati dai canali (attributoLOCLADDR).
- Indirizzi IP locali definiti per i canali riceventi del cluster (attributoCONNAME).
- Gli indirizzi IP locali definiti per gli oggetti delle informazioni di comunicazione (attributoGRPADDR).
- Percorsi di sistema definiti per le definizioni di processo e oggetto servizio.

k) Arrestare e riavviare il gestore code per rendere effettive le modifiche.

l) Ripetere il passo 3j per gestori code remoti, più le impostazioni equivalenti per le applicazioni, che si connettono al gestore code migrato, incluso:

- Nomi connessione canale (attributoCONNAME).
- Le regole di autenticazione del canale che limitano le connessioni in entrata dal gestore code in base al relativo nome host o indirizzo IP.
- Tabelle CCDT (Client Channel Definition Table), DNS (Domain Name Settings), instradamento di rete o informazioni di connessione equivalenti.

m) Eseguire un failover gestito del gestore code su ciascun nodo RDQM per assicurarsi che la configurazione richiesta sia stata stabilita correttamente, fare riferimento a "Impostazione della posizione preferita per un RDQM" a pagina 547.

Ridimensionamento del file system per un gestore code HA RDQM
Per ridimensionare il filesystem per un gestore code di dati replicati (RDQM) HA (High Availability) esistente, eseguire il backup dei propri dati persistenti, quindi ripristinare i dati su un gestore code RDQM appena creato che ha lo stesso nome ma un filesystem di dimensione diversa.

Informazioni su questa attività

I gestori code di dati replicati HA richiedono un volume logico dedicato (filesystem) e la configurazione della replica del disco e il controllo HA. Questi componenti vengono configurati solo quando viene creato un nuovo gestore code. Il file system non può essere ridimensionato dopo che è stato creato perché deve avere la stessa dimensione su ogni nodo. Per ridimensionare il filesystem per un gestore code di dati replicati esistente (RDQM), è possibile eseguire il backup dei dati persistenti, quindi ripristinare i

dati su un gestore code RDQM appena creato che ha lo stesso nome ma un filesystem di dimensione diversa. Questa procedura conserva la configurazione del gestore code, lo stato e i messaggi persistenti al momento della creazione del backup.

Procedura

1. Eseguire il backup del gestore code RDQM esistente sul nodo RDQM primario:
   a) Determinare il nodo RDQM primario per il gestore code. Per informazioni su come determinare il nodo primario, vedere rdqmstatus (visualizzazione dello stato RDQM) .
   b) Sul nodo RDQM primario, se il gestore code RDQM è avviato, arrestarlo utilizzando il comando **endmqm -w** o **endmqm -i** .
   c) Determinare l'ubicazione della directory dei dati del gestore code visualizzando il file di configurazione IBM MQ , `mqs.ini`. Su Linux, questo file si trova nella directory `/var/mqm` . Per ulteriori informazioni su `mqs.ini`, consultare “File di configurazione IBM MQ , mqs.ini” a pagina 84.

      Individuare la sezione `QueueManager` per il gestore code nel file. La directory dei dati del gestore code è il valore della chiave denominata `DataPath`. Per ulteriori informazioni sulla stanza `QueueManager` , consultare “Stanza QueueManager del file mqs.ini” a pagina 95.
   d) Creare un backup della directory dei dati del gestore code. Su Linux, è possibile eseguire questa operazione utilizzando il comando **tar** . Ad esempio, per eseguire il back up della directory di dati per un gestore code è possibile utilizzare il seguente comando. Notare l'ultimo parametro del comando, che è un singolo carattere punto (.):

      ```
      tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
      ```
   e) Determinare l'ubicazione della directory di log del gestore code visualizzando IBM MQ file di configurazione del gestore code `qm.ini`. Questo file si trova nella directory dei dati del gestore code. Per ulteriori informazioni sul file, consultare “File di configurazione del gestore code, qm.ini” a pagina 97.

      La directory di log del gestore code è definita come il valore della chiave `LogPath` nella stanza Log. Per informazioni sulla sezione, consultare “Stanza di log del file qm.ini” a pagina 125.
   f) Creare un backup della directory di log del gestore code. Su Linux, è possibile eseguire questa operazione utilizzando il comando **tar** . Ad esempio, per eseguire il back up della directory di log per un gestore code, è possibile utilizzare il seguente comando. Notare l'ultimo parametro del comando, che è un singolo carattere punto (.):

      ```
      tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
      ```
   g) Eliminare il gestore code RDQM esistente.
2. Ripristinare il gestore code con un filesystem della dimensione richiesta:
   a) Creare un nuovo gestore code RDQM con lo stesso nome del gestore code di cui è stato eseguito il backup. Assicurarsi che il file system assegnato per il gestore code RDQM da **crtmqm** sia la dimensione richiesta e che sia sufficientemente grande per contenere i dati, i log primari e i log secondari per il gestore code esistente, più dello spazio aggiuntivo per l'espansione futura. Per informazioni su come creare un gestore code RDQM, consultare “Creazione di un RDQM HA” a pagina 539.
   b) Determinare il nodo RDQM primario per il gestore code. Per informazioni su come determinare il nodo primario, vedere rdqmstatus (visualizzazione dello stato RDQM).
   c) Sul nodo RDQM primario, se il gestore code RDQM è avviato, arrestarlo utilizzando il comando **endmqm -w** o **endmqm -i** .
   d) Sul nodo RDQM primario, stabilire la nuova ubicazione delle directory di dati e di log per il gestore code RDQM (utilizzare i metodi descritti ai passi 1c e 1e).

e) Sul nodo RDQM primario, eliminare il contenuto dei dati del gestore code RDQM e le directory di log, ma non le directory stesse.

f) Sul nodo RDQM primario, ripristinare il backup della directory di dati del gestore code nella directory di dati vuota per il nuovo gestore code RDQM, verificando che la proprietà e le autorizzazioni del file siano conservate. Se il backup è stato creato utilizzando il comando **tar** di esempio nel passo 1d , il seguente comando può essere utilizzato dall'utente root per ripristinarlo:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

g) Sul nodo RDQM principale, ripristinare il backup della directory di log del gestore code nella directory di log vuota per il nuovo gestore code RDQM, verificando che la proprietà del file e le autorizzazioni siano conservate. Se il backup è stato creato utilizzando il comando **tar** di esempio nel passo 1f , il seguente comando può essere utilizzato dall'utente root per ripristinarlo:

```
tar -xvzpf qm-log.tar.gz -C queue_manager_log_dir
```

h) Sul nodo RDQM primario, modificare il file di configurazione del gestore code ripristinato, `qm.ini`, nella directory dei dati per il nuovo gestore code RDQM. Aggiornare il valore della chiave `LogPath` nella stanza `Log` per specificare la directory di log per il nuovo gestore code RDQM determinato al passo 2d. Esaminare gli altri percorsi file definiti nel file di configurazione e aggiornarli, se necessario. Ad esempio, potrebbe essere necessario aggiornare i seguenti percorsi:

- Il percorso per i file di log degli errori generati dai servizi di messaggi diagnostici.
- Il percorso per le uscite richieste dal gestore code.
- Il percorso per i file di caricamento switch se il gestore code è un coordinatore della transazione XA.

i) Verificare che il Gestore code sia visualizzato dal comando **dspmq** e che il suo stato sia riportato come terminato. Il seguente esempio mostra l'output di esempio per un gestore code HA RDQM:

```
$ dspmq -o status -o ha
QMNAME(QM1) STATUS(Ended normally) HA(Replicated)
```

j) Verificare che i dati del gestore code ripristinati siano stati replicati sui nodi RDQM secondari utilizzando il comando **rdqmstatus** per visualizzare lo stato per il gestore code. Lo stato HA deve essere riportato come `Normal` su ciascun nodo. Il seguente esempio mostra l'output di esempio per un gestore code HA RDQM:

```
$ rdqmstatus -m QM1
Node: mqhavm10-adm
Queue manager status:         Ended normally
Queue manager file system:    50MB used, 0.2GB
allocated [42%]
HA role:                      Primary
HA status:                    Normal
HA control:                   Disabled
HA current location:          This node
HA preferred location:        This node
HA floating IP interface:     None
HA floating IP address:       None
Node:                         mqhavm11-adm
HA status:                    Normal
Node:                         mqhavm12-adm
HA status:                    Normal
```

k) Avviare il gestore code sul nodo RDQM primario.

l) Eseguire un failover gestito del gestore code su ciascun nodo RDQM per assicurarsi che la configurazione richiesta sia stata stabilita correttamente, fare riferimento a “Impostazione della posizione preferita per un RDQM” a pagina 547.

V 9.1.5 *Archiviazione dello stato dell'applicazione persistente*

È possibile memorizzare le informazioni sullo stato persistente relative alle applicazioni insieme ad altri dati del gestore code.

Ogni gestore code IBM MQ dispone di un filesystem dedicato per il relativo stato persistente, che include sia i dati della coda che il log di recupero. In una configurazione RDQM, il filesystem è supportato da un volume logico replicato tra i sistemi Linux (nodi). Il file system include una directory `userdata` che è possibile utilizzare per memorizzare le informazioni sullo stato persistente per le applicazioni. Quindi, quando un gestore code di dati replicati si sposta per essere eseguito su un altro nodo nella configurazione RDQM, è disponibile il contesto dell'applicazione e il contesto del gestore code. Vedere Contenuto della directory su Unix e Linux Systems.

Se si sceglie di memorizzare lo stato dell'applicazione nella directory `userdata` , è necessario tenere presente che i dati scritti in questa ubicazione potrebbero consumare lo spazio su disco disponibile assegnato al gestore code. È necessario assicurarsi che sia disponibile spazio su disco sufficiente per il gestore code per scrivere i dati della coda, i log e altre informazioni sullo stato persistente.

La directory `userdata` ha la proprietà utente e gruppo mqm ed è leggibile in modo che gli utenti possano accedervi senza dover far parte del gruppo di amministratori IBM MQ (mqm). Non è possibile modificare le autorizzazioni della directory `userdata` , ma è possibile creare il contenuto in essa con qualsiasi proprietà e autorizzazione richiesti.

Durante un failover del gestore code RDQM, il gestore code viene terminato e il relativo file system viene smontato sul nodo RDQM corrente. Il filesystem viene quindi montato e il gestore code viene riavviato su un altro nodo nella configurazione RDQM. Un file system non può essere smontato se un processo ha un handle aperto per uno dei suoi file. Per garantire che un failover del gestore code possa essere completato, se il filesystem del gestore code non può essere smontato, ai processi che hanno un handle di file aperto viene inviato un segnale SIGTERM, seguito da un SIGKILL se gli handle aperti non vengono rilasciati. Le applicazioni devono essere progettate per rispondere correttamente a SIGTERM. Se le applicazioni o i processi sono configurati come un servizio del gestore code, durante un failover gestito possono essere terminati durante l'arresto del gestore code prima che il filesystem venga smontato. Se un'applicazione o un processo non è configurato come servizio del gestore code o si verifica un failover non gestito, ad esempio una perdita del quorum, è probabile che i segnali vengano inviati per rilasciare il file system.

Linux V 9.1.0 *Impostazione della posizione preferita per un RDQM*

L'ubicazione preferita per un gestore code di dati replicati (RDQM) identifica il nodo in cui deve essere eseguito RDQM se tale nodo è disponibile.

Informazioni su questa attività

L'ubicazione preferita è il nome del nodo su cui Pacemaker deve eseguire il gestore code quando il gruppo HA è in uno stato normale (tutti i nodi e le connessioni disponibili). L'ubicazione preferita viene inizializzata con il nome del nodo principale quando viene creato il gestore code. È possibile eseguire i comandi per impostare l'ubicazione preferita su uno qualsiasi dei tre nodi. È necessario essere un utente che appartiene ai gruppi `mqm` e `haclient` .

Procedura

- Per assegnare il nodo locale o specificato come Ubicazione preferita per il gestore code denominato, immettere il seguente comando:

  ```
  rdqmadm -p -m qmname [ -n nodename[,nodename  ]
  ```

  dove *qmname* è il nome dell'RDQM per cui si sta specificando l'ubicazione preferita e *nodename* è facoltativamente il nome del nodo preferito.

  Se il gruppo HA si trova in uno stato normale e l'ubicazione preferita non è il nodo primario corrente, il gestore code viene arrestato e riavviato nella nuova ubicazione preferita. È possibile specificare un elenco separato da virgole di due nomi nodo per assegnare una seconda preferenza di Ubicazione preferita.
- Per cancellare la posizione preferita in modo che il gestore code non ritorni automaticamente a un nodo quando viene ripristinato, immettere il seguente comando:

```
rdqmadm -p -m qmname -d
```

Riferimenti correlati

rdqmadm (gestione cluster gestore code dati replicati)

Linux V 9.1.0 *Creazione ed eliminazione di un indirizzo IP mobile*

Un indirizzo IP mobile consente al client di utilizzare lo stesso indirizzo IP per un gestore code di dati replicati (RDQM) indipendentemente dal nodo nel gruppo HA su cui è in esecuzione.

Informazioni su questa attività

È possibile creare o eliminare un indirizzo IP mobile utilizzando il comando **rdqmint** . L'indirizzo mobile si collega a un'interfaccia fisica denominata sul nodo primario per RDQM. Se l'RDQM esegue il failover e un nodo differente diventa il nodo primario, l'IP mobile viene collegato a un'interfaccia con lo stesso nome sul nuovo primario. Le interfacce fisiche sui tre nodi devono appartenere alla stessa sottorete dell'indirizzo IP mobile. Il seguente diagramma illustra l'utilizzo di un indirizzo IP mobile.

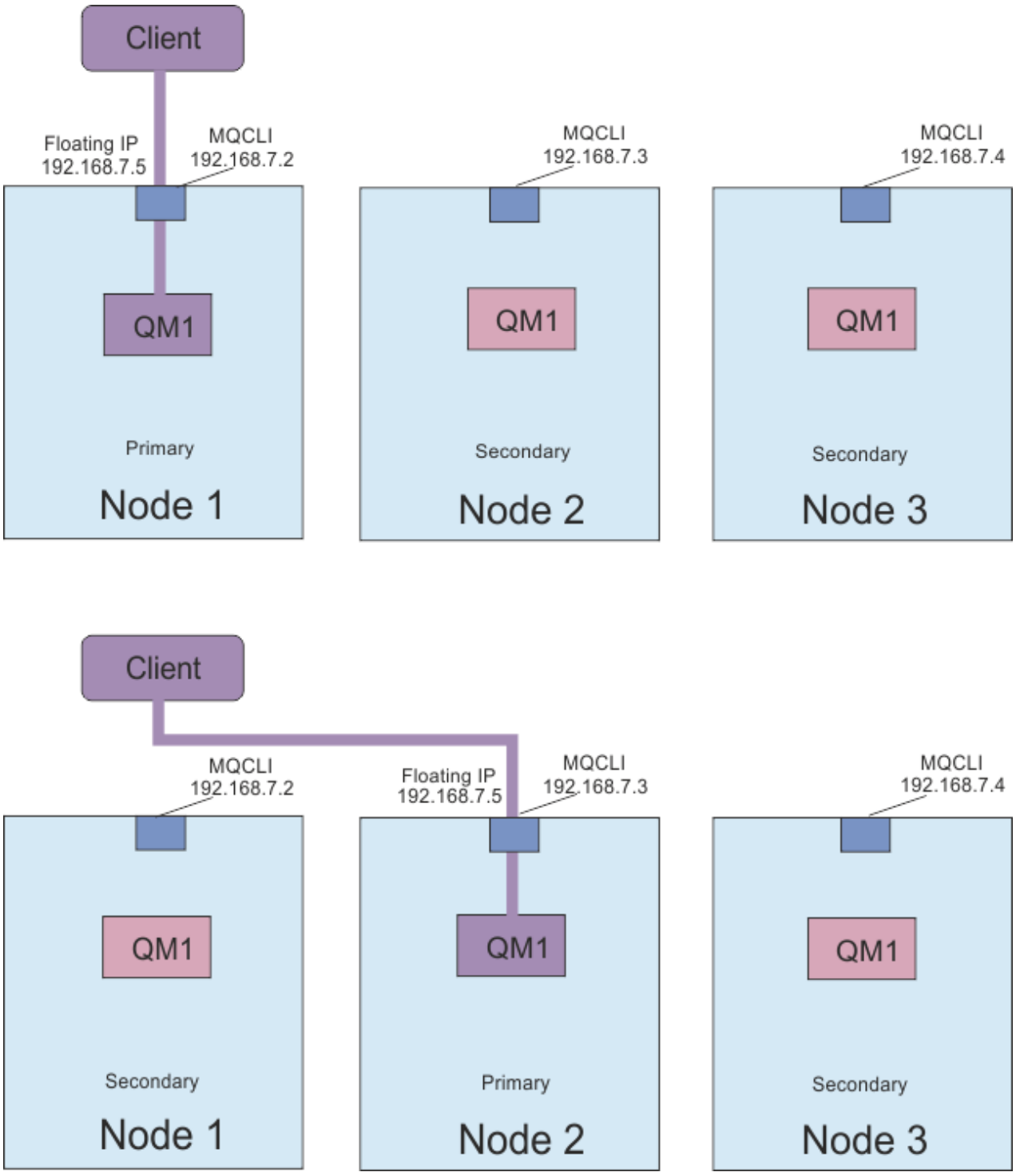


Figura 83. Indirizzo IP mobile

Per eseguire il comando **rdqmint** , è necessario essere un utente nei gruppi `mqm` e `haclient` . È possibile creare o eliminare l'indirizzo IP mobile sul nodo primario per RDQM o su uno dei nodi secondari.

Nota: Non è possibile utilizzare lo stesso indirizzo IP mobile per più RDQM, l'indirizzo IP mobile per ogni RDQM deve essere univoco.

Procedura

- Per creare un indirizzo IP mobile per un RDQM, immettere il seguente comando:

```
rdqmint -m qmname -a  -f ipv4address -l interfacename
```

dove:

QMNAME
È il nome dell'RDQM per cui si sta creando l'indirizzo IP mobile.

ipv4address
L'indirizzo IP mobile in formato ipv4 .

L'indirizzo IP mobile deve essere un indirizzo IPv4 valido che non sia già definito su nessuna applicazione e deve appartenere alla stessa sottorete degli indirizzi IP statici definiti per l'interfaccia locale.

interfaceName
Il nome dell'interfaccia fisica sul nodo primario a cui collegarsi.

Ad esempio:

```
rdqmint -m QM1 -a -f 192.168.7.5 -l MQCLI
```

- Per eliminare un indirizzo IP mobile esistente, immettere il comando seguente:

```
rdqmint -m qmname -d
```

Riferimenti correlati
rdqmint (aggiungere o eliminare l'indirizzo IP mobile per RDQM)

Linux V 9.1.0 *Avvio, arresto e visualizzazione dello stato di un RDQM HA*

Utilizzare varianti di comandi di controllo IBM MQ standard per avviare, arrestare e visualizzare lo stato corrente di un gestore code di dati replicati (RDQM).

Informazioni su questa attività

È necessario eseguire i comandi che avviano, arrestano e visualizzano lo stato corrente di un gestore code di dati replicati (RDQM) come utente appartenente ai gruppi `mqm` e `haclient` .

È necessario eseguire i comandi per avviare e arrestare un gestore code sul nodo primario per tale gestore code.

Procedura

- Per avviare un RDQM, immettere il seguente comando sul nodo primario di RDQM:

```
strmqm qmname
```

dove *qmname* è il nome dell'RDQM che si desidera avviare.

RDQM viene avviato e Pacemaker avvia la gestione di RDQM. È necessario specificare l'opzione `-ns` con `strmqm` se si desidera specificare altre opzioni `strmqm` .

- Per arrestare un RDQM, immettere il seguente comando sul nodo primario del RDQM:

```
endmqm qmname
```

dove *qmname* è il nome dell'RDQM che si desidera arrestare.

Pacemaker cessa di gestire RDQM, quindi l'RDQM viene terminato. Tutti gli altri parametri **endmqm** possono essere utilizzati quando si arresta un RDQM.

- Per visualizzare lo stato di un RDQM, immettere il seguente comando:

```
dspmq
```

Le informazioni sullo stato che vengono emesse dipendono dal fatto che si esegua il comando sul nodo primario o secondario di RDQM. Se eseguito sul nodo primario, viene visualizzato uno dei normali messaggi di stato restituiti da **dspmq** . Se si esegue il comando su un nodo secondario, viene visualizzato lo stato `running elsewhere` . Ad esempio, se **dspmq** viene eseguito sul nodo RDQM7, potrebbero essere restituite le seguenti informazioni:

```
QMNAME(RDQM8)                           STATUS(Running elsewhere)
QMNAME(RDQM9)                           STATUS(Running elsewhere)
QMNAME(RDQM7)                           STATUS(Running)
```

Se il nodo primario non è disponibile o se **dspmq** viene eseguito da un utente non `root` o da un membro del gruppo `haclient` , viene riportato lo stato `Unavailable` . Ad esempio:

```
QMNAME(RDQM8)              STATUS(Unavailable)
QMNAME(RDQM9)              STATUS(Unavailable)
QMNAME(RDQM7)              STATUS(Unavailable)
```

È possibile immettere il comando **dspmq -o ha** (o **dspmq -o HA**) per visualizzare un elenco di gestori code noti a un nodo e se sono RDQM o meno, ad esempio:

```
dspmq -o ha

QMNAME(RDQM8)                                         HA(Replicated)
QMNAME(RDQM9)                                         HA(Replicated)
QMNAME(RDQM7)                                         HA(Replicated)
QMNAME(QM7)                                           HA()
```

Riferimenti correlati

dspmq (visualizza gestori code)

endmqm (fine gestore code)

strmqm (avvio gestore code)

Linux V 9.1.0 ***Visualizzazione dello stato del gruppo RDQM e HA***

È possibile visualizzare lo stato del gruppo HA e dei singoli gestori code di dati replicati (RDQM).

Informazioni su questa attività

Utilizzare il comando **rdqmstatus** per visualizzare lo stato di singoli RDQM e del gruppo HA nel suo complesso.

È necessario essere un utente nei gruppi `mqm` e `haclient` per eseguire il comando **rdqmstatus** . È possibile eseguire il comando su uno qualsiasi dei tre nodi.

Procedura

- Per visualizzare lo stato di un nodo e gli RDQM che fanno parte della configurazione HA:

  ```
  rdqmstatus
  ```

  Viene visualizzata l'identificazione del nodo su cui è stato eseguito il comando e lo stato degli RDQM nella configurazione HA, ad esempio:

  ```
  Node:                                 mqhavm07.exampleco.com

  Queue manager name:                   RDQM8
  Queue manager status:                 Running elsewhere
  HA current location:                  mqhavm08.exampleco.com

  Queue manager name:                   RDQM9
  Queue manager status:                 Running elsewhere
  HA current location:                  mqhavm09.exampleco.com

  Queue manager name:                   RDQM7
  Queue manager status:                 Running
  HA current location:                  This node
  ```

- Per visualizzare lo stato dei tre nodi nel gruppo HA, immettere il seguente comando:

  ```
  rdqmstatus -n
  ```

  Viene riportato lo stato in linea o fuori linea di ciascun nodo. Ad esempio:

  ```
  Node mqha04(mqhavm04.example.com) is online
  Node mqha05(mqhavm05.example.com) is offline
  Node mqha06(mqhavm06.example.com) is online
  ```

- Per visualizzare lo stato di un particolare gestore code su tutti i nodi nel gruppo HA, immettere il seguente comando:

  ```
  rdqmstatus -m qmname
  ```

  dove *qmname* è il nome dell'RDQM per cui si desidera visualizzare lo stato. Viene visualizzato lo stato di RDQM sul nodo corrente, seguito da un riepilogo dello stato degli altri due nodi dalla prospettiva del nodo corrente.

  La seguente tabella riepiloga le informazioni sul nodo corrente che possono essere restituite dal comando **rdqmstatus** per un RDQM.

Tabella 33. Stato nodo corrente

Attributo Stato	**Valori possibili**	**Quando visualizzato**
Nome del nodo	*NODENAME*	Sempre visualizzato
Stato gestore code	In esecuzione In esecuzione altrove Terminato Non disponibile	Sempre visualizzato
CPU	*n.nn*%	Viene visualizzato solo quando il nodo corrente ha un ruolo primario (ossia, RDQM è in esecuzione su questo nodo)
Memoria	*nnn*MB utilizzati, *y.y*GB assegnati	Viene visualizzato solo quando il nodo corrente ha un ruolo primario (ossia, RDQM è in esecuzione su questo nodo)
File system del gestore code	*nnn*MB utilizzati, *y.y*GB assegnati [*z*%]	Viene visualizzato solo quando il nodo corrente ha un ruolo primario (ossia, RDQM è in esecuzione su questo nodo)
Ruolo HA	Secondario primario sconosciuto	Sempre visualizzato
Stato HA	Tutti i nodi in standby Questo nodo è in standby Nodi remoti in standby Misto *stato dei nodi remoti*	Tutti i nodi in standby Nodo corrente in standby Entrambi i nodi remoti in standby Stato differente per ogni nodo remoto (consultare la tabella successiva per lo stato individuale) Stesso stato per entrambi i nodi remoti (consultare la tabella successiva per tutti i valori)

Tabella 33. Stato nodo corrente (Continua)		
Attributo Stato	**Valori possibili**	**Quando visualizzato**
Controllo HA	Abilitato/a Disabilitato/a Sconosciuto	Sempre visualizzato. Mostra se RDQM è sotto il controllo Pacemaker
Ubicazione preferita HA	Nessuno Questo nodo Sconosciuto *NODENAME*	Sempre visualizzato
Interfaccia IP mobile HA	*nome_interfaccia*	Sempre visualizzato
Indirizzo IP mobile HA	*IPV4_address*	Sempre visualizzato

La seguente tabella riepiloga le informazioni restituite dal comando **rdqmstatus** per gli altri nodi nel gruppo HA.

Tabella 34. Stato altro nodo		
Attributo Stato	**Valori possibili**	**Quando visualizzato**
Nome del nodo	*nodename*	Sempre visualizzato
Stato HA	Normale Sincronizzazione in corso Remoto non disponibile Non congruente In pausa Nodo remoto in standby Sconosciuto	I nodi sono sincronizzati tra loro Sincronizzazione con il nodo remoto Impossibile comunicare con il nodo remoto Non sincronizzato con il nodo remoto e non sincronizzato Replica sospesa Nodo remoto in standby
Sincronizzazione HA in corso	*n.n*%	Visualizzato quando la sincronizzazione è in corso e il comando viene eseguito come `root`
Tempo di sincronizzazione stimato HA	*aaaa - mm - gg hh:mm:ss.nnn*	Visualizzato quando la sincronizzazione è in corso
Dati HA non sincronizzati	*n*KB	Visualizzato quando il nodo remoto non è disponibile o non è congruente

Esempio

Esempio di stato normale sul nodo primario:

```
Node:                                   mqhavm07.expampleco.com
Queue manager status:                    Running
CPU:                                     0.00
Memory:                                  123MB
Queue manager file system:               606MB used, 1.0GB allocated [60%]
HA role:                                 Primary
HA status:                               Normal
HA control:                              Enabled
HA current location:                     This node
HA preferred location:                   This node
```

```
HA floating IP interface:               Eth4
HA floating IP address:                 192.0.2.4


Node:                                   mqhavm08.exampleco.com
HA status:                              Normal


Node:                                   mqhavm09.exampleco.com
HA status:                              Normal
```

Esempio di stato normale su un nodo secondario:

```
Node:                                   mqhavm08.exampleco.com
Queue manager status:                   Running elsewhere
HA role:                                Secondary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    mqhavm07.exampleco.com
HA preferred location:                  mqhavm07.exampleco.com
HA floating IP interface:               Eth4
HA floating IP address:                 192.0.2.4

Node:                                   mqhavm07.exampleco.com
HA status:                              Normal

Node:                                   mqhavm09.exampleco.com
HA status:                              Normal
```

Esempio di stato sul nodo primario quando è in corso la sincronizzazione:

```
Node:                                   mqhavm07.exampleco.com
Queue manager status:                   Running
CPU:                                    0.53
Memory:                                 124MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Synchronization in progress
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA floating IP interface:               Eth4
HA floating IP address:                 192.0.2.4

Node:                                   mqhavm08.exampleco.com
HA status:                              Synchronization in progress
HA synchronization progress:            11.0%
HA estimated time to completion:        2017-09-06 14:55:05

Node:                                   mqhavm09.exampleco.com
HA status:                              Synchronization in progress
HA synchronization progress:            11.0%
HA estimated time to completion:        2017-09-06 14:55:06
```

Esempio di un nodo principale che mostra più stati:

```
Node:                                   mqhavm07.exampleco.com
Queue manager status:                   Running
CPU:                                    0.02
Memory:                                 124MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Mixed
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA floating IP interface:               Eth4
HA floating IP address:                 192.0.2.4

Node:                                   mqhavm08.exampleco.com
HA status:                              Normal

Node:                                   mqhavm09.exampleco.com
HA status:                              Inconsistent
```

Riferimenti correlati

Linux rdqmstatus

Linux V 9.1.0 *Sostituzione di un nodo malfunzionante in una configurazione ad alta disponibilità*

Se uno dei nodi nel tuo gruppo HA ha esito negativo, puoi sostituirlo.

Informazioni su questa attività

Le operazioni da eseguire per sostituire un nodo dipendono dallo scenario:

- Se si sta sostituendo il nodo malfunzionante con un nodo con una configurazione identica, è possibile sostituire il nodo senza interrompere il gruppo HA.
- Se il nuovo nodo ha una configurazione differente, è necessario eliminare e quindi ricreare il gruppo HA. È possibile prima eseguire il backup dei gestori code dal nodo su cui sono in esecuzione, quindi ripristinarli dopo aver rigenerato il gruppo HA.

Procedura

- Se il nodo di sostituzione è configurato per essere simile al nodo non riuscito (stesso nome host, stessi indirizzi IP e così via), completare la seguente procedura sul nuovo nodo:
  a) Creare un file `rdqm.ini` che corrisponda ai file sugli altri nodi, quindi eseguire il comando `rdqmadm -c` (consultare “Definizione del cluster Pacemaker (gruppo HA)” a pagina 536).
  b) Eseguire il comando `crtmqm -sxs` *`qmanager`* per creare nuovamente ciascun gestore code di dati replicati (consultare “Creazione di un RDQM HA” a pagina 539).
- Se il nodo di sostituzione ha una configurazione diversa rispetto al nodo in errore:
  a) Se necessario, eseguire il backup dei gestori code (consultare “Backup e ripristino dei dati del gestore code IBM MQ” a pagina 621).
  b) Eliminare i gestori code di dati replicati dagli altri nodi nel gruppo HA utilizzando il comando **`dltmqm`** (consultare “Eliminazione di un RDQM HA” a pagina 540).
  c) Annullare la configurazione del cluster Pacemaker utilizzando il comando **`rdqmadm -u`** (consultare “Eliminazione del cluster Pacemaker (gruppo HA)” a pagina 539).
  d) Riconfigurare il cluster Pacemaker , incluse le informazioni per il nuovo nodo, utilizzando il comando **`rdqmadm -c`** (consultare “Definizione del cluster Pacemaker (gruppo HA)” a pagina 536).
  e) Se necessario (ossia, se non si dispone dell'accesso SSH agli altri nodi), eseguire il comando `crtmqm -sxs` *`qmanager`* per ricreare ciascun gestore code di dati replicati sugli altri nodi (consultare “Creazione di un RDQM HA” a pagina 539).
  f) Eseguire il comando `crtmqm -sx` *`qmanager`* per creare i gestori code sul nodo di sostituzione.
  g) Se necessario, ripristinare i dati e la configurazione sui propri gestori code (consultare “Backup e ripristino dei dati del gestore code IBM MQ” a pagina 621).

MQ Adv. Linux V 9.1.0 Ripristino di emergenza RDQM

RDQM (gestore code di dati replicati) è disponibile su un sottoinsieme di piattaforme Linux e può fornire una soluzione di ripristino di emergenza.

Consultare Software Product Compatibility Reports per i dettagli completi.

È possibile creare un'istanza primaria di un gestore code di ripristino di emergenza in esecuzione su un server e un'istanza secondaria del gestore code su un altro server che funga da nodo di ripristino. I dati vengono replicati tra le istanze del gestore code. Se si perde il gestore code primario, è possibile creare manualmente l'istanza secondaria nell'istanza primaria e avviare il gestore code, quindi riprendere il lavoro dallo stesso luogo. Non è possibile avviare un gestore code mentre è nel ruolo secondario. La replica dei dati tra i due nodi è gestita da DRBD.

È possibile scegliere tra la replica sincrona e asincrona dei dati tra gestori code primari e secondari. Se si seleziona l'opzione asincrona, le operazioni quali IBM MQ PUT o GET vengono completate e ritornano all'applicazione prima che l'evento venga replicato sul gestore code secondario. La replica asincrona indica che, in seguito a una situazione di recupero, alcuni dati di messaggistica potrebbero essere persi. Ma il gestore code secondario sarà in uno stato congruente e sarà in grado di avviare l'esecuzione immediatamente, anche se viene avviato in una parte leggermente precedente del flusso di messaggi.

Non è possibile aggiungere il ripristino di emergenza a un gestore code esistente, sebbene sia possibile migrare un gestore code esistente in modo che diventi un gestore code RDQM (consultare “Migrazione di un gestore code per diventare un gestore code DR RDQM” a pagina 562). Un gestore code non può essere configurato con il ripristino di emergenza RDQM e l'alta disponibilità RDQM.

È possibile avere diverse coppie di gestori code RDQM in esecuzione su un numero di server differenti. Ad esempio, è possibile disporre di gestori code di ripristino di emergenza primari in esecuzione su nodi differenti, mentre tutti i gestori code di ripristino di emergenza secondari vengono eseguiti sullo stesso nodo. Alcune configurazioni di esempio sono illustrate nei seguenti diagrammi.

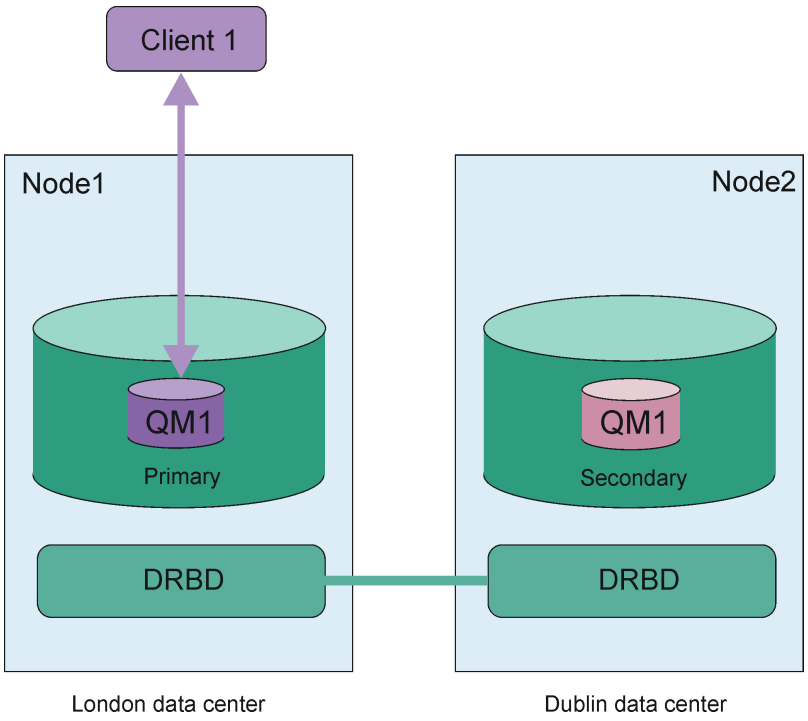


Figura 84. Singola coppia RDQM

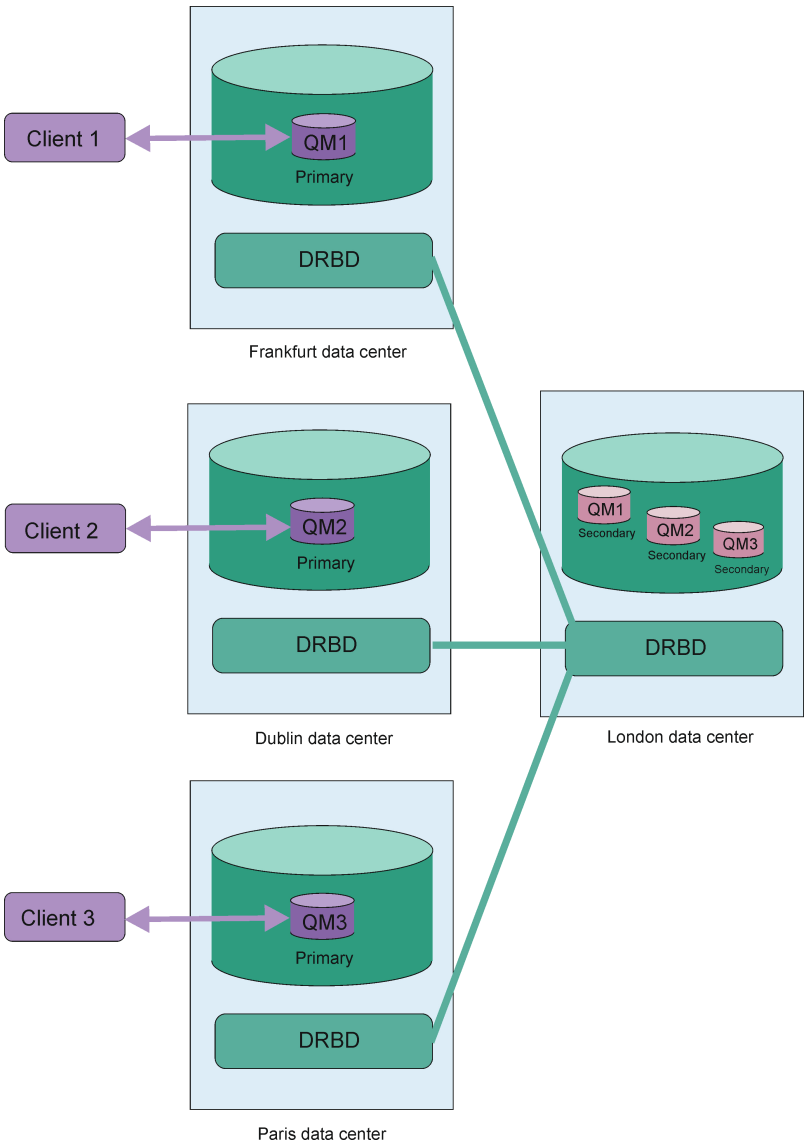


Figura 85. Gestori code secondari nello stesso nodo

Replica, sincronizzazione e istantanee

Mentre i due nodi in una configurazione di ripristino di emergenza sono connessi, tutti gli aggiornamenti ai dati persistenti per un gestore code di ripristino di emergenza vengono trasferiti dall'istanza primaria del gestore code all'istanza secondaria. Questa operazione è nota come **replica**.

Se la connessione di rete tra i due nodi viene persa, le modifiche ai dati persistenti per l'istanza primaria di un gestore code vengono tracciate. Quando la connessione di rete viene ripristinata, viene utilizzato un processo diverso per rendere l'istanza secondaria più rapida possibile. Questa operazione è nota come **sincronizzazione**.

Mentre la sincronizzazione è in esecuzione, i dati sull'istanza secondaria si trovano in uno stato incongruente. Viene eseguita un' **istantanea** dello stato dei dati del gestore code secondario. Se si verifica un errore del nodo principale o della connessione di rete durante la sincronizzazione, l'istanza secondaria ritorna a questa istantanea e il gestore code può essere avviato. Tuttavia, tutti gli aggiornamenti che si sono verificati dopo l'errore di rete originale vengono persi.

Dati partizionati (cervello diviso)

Le configurazioni DR RDQM richiedono l'intervento dell'utente dopo la perdita dell'istanza primaria di un gestore code per promuovere ed eseguire l'istanza secondaria sul nodo di recupero. È responsabilità di chiunque (o qualsiasi altra cosa) promuova l'istanza secondaria per garantire che il precedente gestore code primario sia arrestato. Se il primario originale continua ad essere in esecuzione, potrebbe elaborare i messaggi e, quando viene ripristinata la normale operazione, le due istanze del gestore code hanno viste differenti dei dati. Questo è noto come stato partizionato o split - brain.

Considera le seguenti situazioni:

- Il nodo su cui è in esecuzione il gestore code primario ha esito negativo. L'istanza secondaria viene promossa in modo che diventi l'istanza; non è possibile eseguire azioni per arrestare l'istanza primaria originale perché non è in esecuzione. Quando il nodo originale viene ripristinato o sostituito, il gestore code su tale nodo verrà inizialmente reso secondario e sincronizzato con il gestore code primario sul nodo di recupero. I ruoli dei due gestori code vengono quindi invertiti e le normali operazioni ricominciano. L'unica perdita di dati potenziale in questa situazione è qualsiasi dato che il primario non ha completato la replica sul secondario prima che il nodo non funzionasse.
- Si è verificato un errore di rete che interessa il link di replica tra i nodi che eseguono le istanze primarie e secondarie del gestore code. In questa situazione è necessario assicurarsi di arrestare il primario originale prima di promuovere il secondario. Se il primario originale dispone ancora di un'altra connettività di rete, si hanno effettivamente due istanze primarie in esecuzione contemporaneamente e i dati partizionati possono accumularsi. (Se il link di replica funziona, non è possibile promuovere un gestore code secondario se l'istanza primaria è ancora in esecuzione, il comando ha esito negativo.)
- Si è verificato un errore di rete completo sul nodo che esegue l'istanza primaria del gestore code. Ancora una volta, è necessario assicurarsi di arrestare l'istanza primaria prima di promuovere quella secondaria. Se il primario precedente è ancora in esecuzione quando la rete viene ripristinata, ci saranno due istanze primarie e di nuovo i dati partizionati si accumuleranno.

Quando si esegue un failover gestito, non dovrebbe essere visualizzato uno stato DR `partitioned` per le istanze del gestore code. Un failover gestito termina il gestore code sul nodo primario, quindi avvia il gestore code sul nodo di recupero dopo che i dati sono stati completamente replicati. Uno stato partizionato non è previsto perché il gestore code è terminato e i dati sono sincronizzati tra i nodi prima che vengano avviati sul nodo di ripristino. Se il gestore code viene avviato sul nodo di recupero mentre si verifica una perdita di connettività tra i nodi, è probabile che la divergenza dei dati sia dovuta al fatto che il gestore code era attivo sul nodo principale quando si è persa la connettività. In questo scenario, è previsto che venga riportato uno stato partizionato una volta ripristinata la connettività perché i dati del gestore code non sono stati sincronizzati. Se si verifica uno stato partizionato, potrebbe essere necessario esaminare i due dataset e prendere una decisione informata su quale serie conservare. Consultare “Risoluzione di un problema partizionato (split brain) in DR RDQM” a pagina 575.

Linux V 9.1.0 ***Requisiti per la soluzione RDQM DR***

È necessario soddisfare una serie di requisiti prima di configurare una coppia di gestori code DR (Disaster Recovery) RDQM.

Requisiti di sistema

Prima di configurare RDQM DR, è necessario completare alcune operazioni di configurazione su ciascuno dei server su cui si trovano i gestori code RDQM DR.

- Ogni nodo richiede un gruppo di volumi denominato `drbdpool`. La memoria per ogni gestore code di dati replicati del ripristino di emergenza (DR RDQM) è assegnata come due volumi logici separati per gestore code da questo gruppo di volumi. (Ogni gestore code richiede due volumi logici per supportare l'operazione di ripristino dell'istantanea, quindi ogni DR RDQM viene assegnato poco più del doppio della memoria specificata quando viene creato.) Per prestazioni ottimali, questo gruppo di volumi deve essere costituito da uno o più volumi fisici che corrispondono alle unità disco interne (preferibilmente SSD).
- Dopo aver creato il gruppo di volumi `drbdpool` , non eseguire altre operazioni. IBM MQ gestisce i volumi logici creati in `drbdpool`e come e dove sono montati.

- Ogni nodo richiede un'interfaccia utilizzata per la replica dei dati. Deve avere una larghezza di banda sufficiente per supportare i requisiti di replica dato il carico di lavoro previsto di tutti i gestori code di dati replicati.

  Per la massima tolleranza di errore, questa interfaccia deve essere una NIC (Network Interface Card) indipendente.
- DRBD richiede che ogni nodo utilizzato per RDQM abbia un nome host internet valido (il valore restituito da `uname -n`), come definito da RFC 952 modificato da RFC 1123.
- Se esiste un firewall tra i nodi utilizzati per DR RDQM, il firewall deve consentire il traffico tra i nodi sulle porte utilizzate per la replica.
- Se il sistema utilizza SELinux in una modalità diversa da quella permissiva, è necessario eseguire il seguente comando:

```
semanage permissive -a drbd_t
```

Requisiti di rete

Si consiglia di individuare i nodi utilizzati per il ripristino di emergenza in diversi data center.

È necessario essere consapevoli delle seguenti limitazioni:

- Le prestazioni peggiorano rapidamente con l'aumento della latenza tra i data center. IBM supporterà una latenza fino a 5 ms per la replica sincrona e 50 ms per la replica asincrona.
- I dati inviati attraverso il link di replicazione non sono soggetti ad alcuna ulteriore crittografia oltre a quella che potrebbe essere in atto utilizzando IBM MQ AMS.
- La configurazione di un gestore code RDQM per il ripristino di emergenza comporta un sovraccarico dovuto al requisito di replicare i dati tra i due nodi RDQM. La replica sincrona comporta un sovraccarico maggiore rispetto alla replica asincrona. Quando viene utilizzata la replica sincrona, le operazioni I/O del disco vengono bloccate finché i dati non vengono scritti su entrambi i nodi. Quando viene utilizzata la replica asincrona, i dati devono essere scritti solo nel nodo primario prima che l'elaborazione possa continuare.

Requisiti utente per l'utilizzo dei gestori code

Per creare, eliminare o configurare i gestori code di dati replicati (RDQM), è necessario essere l'utente root o disporre di un ID utente appartenente al gruppo `mqm` a cui viene concessa l'autorizzazione sudo per i seguenti comandi:

- **`crtmqm`**
- **`dltmqm`**
- **`rdqmdr`**

Un utente che appartiene al gruppo `mqm` può visualizzare lo stato di un DR RDQM utilizzando i seguenti comandi:

- **`dspmq`**
- **`rdqmstatus`**

Linux V 9.1.0 ***Creazione di un RDQM di ripristino di emergenza***

Utilizzare il comando **`crtmqm`** per creare un gestore code di dati replicati (RDQM) che agisca come primario o secondario in una configurazione di ripristino di emergenza.

Informazioni su questa attività

È possibile creare un gestore code di dati replicati (RDQM) come utente nel gruppo `mqm` se l'utente può utilizzare sudo. Altrimenti, è necessario creare l'RDQM come root.

È necessario creare un gestore code RDQM DR primario su un nodo. È necessario quindi creare un'istanza secondaria dello stesso gestore code su un altro nodo. Le istanze primarie e secondarie hanno lo stesso nome e devono essere assegnate alla stessa quantità di memoria.

Procedura

- Per creare un DR RDQM primario:
  a) Immettere il seguente comando:

```
crtmqm -rr p [-rt (a | s)] -rl Local_IP -ri Recovery_IP -rn Recovery_Name -rp Port
[other_crtmqm_options] [-fs size] QMname
```

  dove:

  -rr p
  Specifica che si sta creando l'istanza primaria del gestore code.

  -rt a | s
  -rt s specifica che la configurazione DR utilizza la replica sincrona, **-rt a** specifica che la configurazione DR utilizza la replica asincrona. La replica asincrona è il valore predefinito.

  -rl *IP_locale*
  Specifica l'indirizzo IP locale da utilizzare per la replica DR di questo gestore code.

  -ri *IP_recupero*
  Specifica l'indirizzo IP dell'interfaccia utilizzata per la replica sul server che ospita l'istanza secondaria del gestore code.

  -rn *Nome_recupero*
  Specifica il nome del sistema che ospita l'istanza secondaria del gestore code. Il nome è il valore restituito se si esegue `uname -n` su tale server. È necessario creare esplicitamente un gestore code secondario su tale server.

  -rp *Porta*
  Specifica la porta da utilizzare per la replica DR.

  altre opzioni crtmqm_options
  Facoltativamente, è possibile specificare una o più delle seguenti opzioni **crtmqm** generali:

  - -z
  - -q
  - -c *Testo*
  - -d *DefaultTransmissionDefaultTransmission*
  - -h *MaxHandles*
  - -g *ApplicationGroup*
  - -oa *utente*|*gruppo*
  - -t *TrigInt*
  - -u *DeadQ*
  - -x *MaxUMsgs*
  - -lp *LogPri*
  - -ls *LogSec*
  - -lc | -l
  - -lla | -lln
  - -lf *LogFileDimensione*
  - -p *Porta*

  -fs *dimensione*
  Facoltativamente specifica la dimensione del file system da creare per il gestore code, ossia la dimensione del volume logico creato nel gruppo di volumi drbdpool. Viene creato anche un altro

volume logico di tale dimensione, per supportare il ripristino dell'operazione di istantanea, in modo che la memoria totale per il DR RDQM sia poco più del doppio di quella specificata qui.

QMNAME
Specifica il nome del gestore code di dati replicato. Il nome è sensibile al maiuscolo/minuscolo.

Una volta completato il comando, viene emesso il comando che richiede l'input tp sul nodo secondario per creare l'istanza secondaria del gestore code. È inoltre possibile utilizzare il comando **rdqmdr** sul nodo principale per richiamare il comando **crtmqm** che è necessario eseguire sul nodo secondario per creare il gestore code secondario, consultare "Gestione delle caratteristiche primarie e secondarie di RDQM DR" a pagina 568.

- Per creare un DR RDQM secondario:

  a) Immettere il seguente comando sul nodo che deve ospitare le istanze secondarie di RDQM:

```
crtmqm  -rr s [-rt (a | s)] -rl Local_IP -ri Primary_IP -rn Primary_Name  -rp Port
[other_crtmqm_options] [-fs size] QMname
```

Dove:

-rr s
Specifica che si sta creando l'istanza secondaria del gestore code.

-rt a | s
-rt s specifica che la configurazione DR utilizza la replica sincrona, **-rt a** specifica che la configurazione DR utilizza la replica asincrona.

-rl *IP_locale*
Specifica l'indirizzo IP locale da utilizzare per la replica DR di questo gestore code.

-ri *IP_Primario*
Specifica l'indirizzo IP dell'interfaccia utilizzata per la replica sul server che ospita l'istanza primaria del gestore code.

-rn *Nome_Primario*
Specifica il nome del sistema che ospita l'istanza primaria del gestore code. Il nome è il valore restituito se si esegue `uname -n` su tale server.

-rp *Porta*
Specifica la porta da utilizzare per la replica DR.

altre opzioni crtmqm_options
Facoltativamente, è possibile specificare una o più delle seguenti opzioni **crtmqm** generali:

– `-z`

-fs *dimensione*
Specifica la dimensione del filesystem da creare per il gestore code, ossia la dimensione del volume logico creato nel gruppo di volumi drbdpool. Se è stata specificata una dimensione non predefinita durante la creazione del gestore code primario, è necessario specificare lo stesso valore.

QMNAME
Specifica il nome del gestore code di dati replicato. Deve essere uguale al nome specificato per l'istanza primaria del gestore code. Notare che il nome è sensibile al maiuscolo / minuscolo.

Operazioni successive

Dopo aver creato le istanze primarie e secondarie del proprio gestore code, è necessario controllare lo stato su entrambi i nodi per verificare che entrambi siano corretti. Utilizzare il comando **rdqmstatus** su entrambi i nodi. I nodi devono visualizzare lo stato normale come descritto in "Visualizzazione dello stato DR RDQM" a pagina 570. Se non stanno visualizzando questo stato, eliminare l'istanza secondaria e ricrearla, facendo attenzione a utilizzare gli argomenti corretti.

Riferimenti correlati

crtmqm

Linux V 9.1.0 *Eliminazione di un RDQM DR*

Utilizzare il comando **dltmqm** per eliminare un gestore code di dati replicati del ripristino di emergenza (RDQM).

Informazioni su questa attività

È necessario eseguire il comando per eliminare l'RDQM su entrambi i nodi RDQM primario e secondario. RDQM deve essere terminato per primo. È possibile eseguire il comando come un utente mqm se tale utente dispone dei privilegi sudo necessari. Altrimenti, è necessario eseguire il comando come root.

Procedura

- Per eliminare un DR RDQM, immettere il seguente comando:

```
dltmqm RDQM_name
```

Riferimenti correlati

dltmqm

MQ Adv. Linux *Migrazione di un gestore code per diventare un gestore code DR RDQM*

È possibile migrare un gestore code esistente per diventare un gestore code di dati replicati di DR (Disaster Recovery) (RDQM) eseguendo il backup dei relativi dati persistenti, quindi ripristinando i dati su un gestore code RDQM appena creato con lo stesso nome.

Informazioni su questa attività

I gestori code di dati replicati DR richiedono un volume logico dedicato (filesystem) e la configurazione della replica del disco. Questi componenti vengono configurati solo quando viene creato un nuovo gestore code. Un gestore code esistente può essere migrato per utilizzare RDQM eseguendo il backup dei dati persistenti, quindi ripristinando i dati su un gestore code RDQM appena creato con lo stesso nome. Questa procedura conserva la configurazione del gestore code, lo stato e i messaggi persistenti al momento della creazione del backup.

Nota: È possibile migrare un gestore code solo da una versione di IBM MQ uguale o inferiore alla versione in cui è installato RDQM. Anche il sistema operativo e l'architettura devono essere uguali. Altrimenti, è necessario creare un nuovo gestore code sulla piattaforma di destinazione; fare riferimento a Spostamento di un gestore code su un sistema operativo differente.

È necessario soddisfare le seguenti condizioni prima di migrare un gestore code:

- Valutare i requisiti di ripristino di emergenza e consultare “Ripristino di emergenza RDQM” a pagina 555.
- Esaminare le applicazioni e i gestori code che si connettono al gestore code. Considerare le modifiche richieste per instradare le connessioni al nodo RDQM su cui è in esecuzione il gestore code.
- Eseguire il provisioning o identificare i nodi RDQM esistenti per la configurazione scelta. Per informazioni sui requisiti di sistema per RDQM, consultare “Requisiti per la soluzione RDQM DR” a pagina 558.
- Installare IBM MQ Advanced, che include la funzione RDQM, su ciascun nodo.
- Facoltativamente, verificare la configurazione RDQM utilizzando un gestore code di prova, che può quindi essere eliminato. La verifica della configurazione è consigliata per identificare e risolvere eventuali problemi prima di migrare il gestore code.
- Esaminare la configurazione della sicurezza per il gestore code, quindi replicare gli utenti e i gruppi locali richiesti su ciascun nodo RDQM.
- Esaminare il gestore code e la configurazione del canale per determinare se vengono utilizzate le uscite API, le uscite canale o le uscite di conversione dati. Installare le uscite richieste su ciascun nodo RDQM.
- Esaminare i servizi del gestore code che sono stati definiti, quindi installare e configurare i processi richiesti su ciascun nodo RDQM.

Procedura

1. Eseguire il backup del gestore code esistente:
   a) Arrestare il gestore code esistente emettendo un comando di attesa arresto `endmqm -wo` un comando di arresto immediato `endmqm -i`. Questa operazione è importante per garantire la congruenza dei dati nel backup.
   b) Determinare l'ubicazione della directory dei dati del gestore code visualizzando il file di configurazione IBM MQ , `mqs.ini`. Su Linux, questo file si trova nella directory `/var/mqm` . Per ulteriori informazioni su `mqs.ini`, consultare "File di configurazione IBM MQ , mqs.ini" a pagina 84.

      Individuare la sezione `QueueManager` per il gestore code nel file. Se la stanza contiene una chiave denominata `DataPath` , il suo valore è la directory dei dati del gestore code. Se la chiave non esiste, la directory dei dati del gestore code può essere determinata utilizzando i valori delle chiavi `Prefix` e `Directory` . La directory dei dati del gestore code è una concatenazione di questi valori, nel formato *prefisso*/qmgrs/*directory*. Per ulteriori informazioni sulla stanza QueueManager , consultare "Stanza QueueManager del file mqs.ini" a pagina 95.
   c) Creare un backup della directory dei dati del gestore code. Su Linux, è possibile eseguire questa operazione utilizzando il comando **tar** . Ad esempio, per eseguire il back up della directory di dati per un gestore code è possibile utilizzare il seguente comando. Notare l'ultimo parametro del comando, che è un singolo punto (punto):

      ```
      tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
      ```

   d) Determinare l'ubicazione della directory di log del gestore code visualizzando IBM MQ file di configurazione del gestore code `qm.ini`. Questo file si trova nella directory dei dati del gestore code. Per ulteriori informazioni sul file, consultare "File di configurazione del gestore code, qm.ini" a pagina 97.

      La directory di log del gestore code è definita come il valore della chiave `LogPath` nella stanza `Log` . Per informazioni sulla sezione, consultare "Stanza di log del file qm.ini" a pagina 125.
   e) Creare un backup della directory di log del gestore code. Su Linux, è possibile eseguire questa operazione utilizzando il comando tar. Ad esempio, per eseguire il back up della directory di log per un gestore code, è possibile utilizzare il seguente comando. Notare l'ultimo parametro del comando, che è un singolo punto (punto):

      ```
      tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
      ```

   f) Creare un backup dei repository dei certificati utilizzati dal gestore code se non si trovano nella directory dei dati del gestore code. Verificare che sia il file del database delle chiavi che il file stash delle password siano sottoposti a backup. Per informazioni sul repository delle chiavi del gestore code, consultare Il repository delle chiavi SSL/TLS e Individuazione del repository delle chiavi per un gestore code. Per informazioni sull'individuazione dell'archivio chiavi AMS se il gestore code è configurato per utilizzare l'intercettazione MCA (Message Channel Agent) AMS, consultare Intercettazione MCA (Message Channel Agent).
   g) Il gestore code esistente non è più richiesto, quindi può essere eliminato. Tuttavia, laddove possibile, è necessario eliminare il gestore code esistente solo dopo che è stato ripristinato correttamente nel sistema di destinazione. Il differimento dell'eliminazione garantisce che il gestore code possa essere riavviato se il processo di migrazione non viene completato correttamente.

      Nota: Se si rinvia l'eliminazione del gestore code esistente, non riavviarla. È importante che il gestore code rimanga chiuso perché ulteriori modifiche alla relativa configurazione o stato vengono perse durante la migrazione.
2. Preparare il nodo RDQM primario:
   a) Creare un nuovo gestore code RDQM con lo stesso nome del gestore code di cui è stato eseguito il backup. Assicurarsi che il file system assegnato per il gestore code RDQM da **crtmqm** sia abbastanza grande da contenere i dati, i log primari e i log secondari per il gestore code esistente,

oltre a spazio aggiuntivo per l'espansione futura. Per informazioni su come creare un gestore code RDQM, consultare “Creazione di un RDQM di ripristino di emergenza” a pagina 559.

b) Determinare il nodo RDQM primario per il gestore code. Per informazioni su come determinare il nodo primario, vedere rdqmstatus (visualizzazione dello stato RDQM).

c) Sul nodo RDQM primario, se il gestore code RDQM è avviato, arrestarlo utilizzando il comando `endmqm -w` o `endmqm -i` .

d) Determinare l'ubicazione delle directory di dati e di log per il gestore code RDQM (utilizzare i metodi descritti nei passi 1b e 1d).

e) Eliminare il contenuto delle directory di log e dei dati del gestore code RDQM, ma non le directory stesse.

3. Ripristinare il gestore code sul nodo RDQM primario:

a) Copiare i backup dei dati del gestore code e le directory di log nel nodo RDQM primario, oltre a eventuali backup separati dei repository dei certificati utilizzati dal gestore code.

b) Ripristinare il backup della directory di dati del gestore code nella directory di dati vuota per il nuovo gestore code RDQM, assicurando che la proprietà e le autorizzazioni del file siano conservate. Se il backup è stato creato utilizzando il comando tar di esempio nel passaggio 1c , l'utente root può utilizzare il seguente comando per ripristinarlo:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

c) Ripristinare il backup della directory di log del gestore code nella directory di log vuota per il nuovo gestore code RDQM, verificando che le autorizzazioni e la proprietà del file siano conservate. Se il backup è stato creato utilizzando il comando tar di esempio nel passo 1e , l'utente root può utilizzare il seguente comando per ripristinarlo:

```
tar -xvzpf qm-log.tar.gz -C queue_manager_log_dir
```

d) Modificare il file di configurazione del gestori code ripristinato, `qm.ini`, nella directory dei dati per il gestore code RDQM. Aggiornare il valore della chiave `LogPath` nella stanza `Log` per specificare la directory di log per il gestore code RDQM.

Esaminare gli altri percorsi file definiti nel file di configurazione e aggiornarli, se necessario. Ad esempio, potrebbe essere necessario aggiornare i seguenti percorsi:

- Il percorso per i file di log degli errori generati dai servizi di messaggi diagnostici.
- Il percorso per le uscite richieste dal gestore code.
- Il percorso per i file di caricamento switch se il gestore code è un coordinatore della transazione XA.

e) Se il gestore code è configurato per utilizzare l'intercettazione AMS Message Channel Agent (MCA), copiare il keystore AMS nella nuova installazione RDQM, quindi esaminare e aggiornare la configurazione. Il keystore deve essere disponibile su ciascun nodo RDQM, quindi se non è ubicato nel filesystem replicato per il gestore code, deve essere copiato su ciascun nodo. Per ulteriori informazioni, consultare Intercettazione MCA (Message Channel Agent).

f) Verificare che il Gestore code sia visualizzato dal comando **dspmq** e che il suo stato sia riportato come terminato. Il seguente esempio mostra l'output di esempio per un gestore code DR RDQM:

```
$ dspmq -o status -o dr

QMNAME(QM1) STATUS(Ended normally) DRROLE(Primary)
```

g) Verificare che i dati del gestore code ripristinati siano stati replicati sui nodi RDQM secondari utilizzando il comando **rdqmstatus** per visualizzare lo stato per il gestore code. Lo stato DR deve essere riportato come `Normal` su ciascun nodo. Il seguente esempio mostra l'output di esempio per un gestore code DR RDQM:

```
$ rdqmstatus -m QM1
Queue manager status:                   Ended normally
Queue manager file system:              51MB used, 1.0GB allocated [5%]
```

```
DR role:                                Primary
DR status:                              Normal
DR type:                                Synchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
```

h) Avviare il gestore code sul nodo RDQM primario.

i) Connettersi al gestore code e aggiornare il valore dell'attributo del gestore code SSLKEYR per specificare la nuova ubicazione del repository dei certificati del gestore code. Per impostazione predefinita, il valore di questo attributo è impostato su *queue_manager_data_directory*/ssl/key. Il repository certificati deve essere ubicato nella stessa ubicazione su ciascun nodo RDQM. Se il repository non si trova nel file system replicato per il gestore code, deve essere copiato su ciascun nodo.

j) Esaminare le definizioni degli oggetti IBM MQ per il gestore code e aggiornare il valore degli attributi degli oggetti che fanno riferimento alle impostazioni di rete modificate, la directory di installazione di IBM MQ o la directory dei dati del gestore code, inclusi i seguenti oggetti:

- Indirizzi IP locali utilizzati dai listener (attributoIPADDR).
- Indirizzi IP locali utilizzati dai canali (attributoLOCLADDR).
- Indirizzi IP locali definiti per i canali riceventi del cluster (attributoCONNAME).
- Gli indirizzi IP locali definiti per gli oggetti delle informazioni di comunicazione (attributoGRPADDR).
- Percorsi di sistema definiti per le definizioni di processo e oggetto servizio.

k) Arrestare e riavviare il gestore code per rendere effettive le modifiche.

l) Ripetere il passo 3j per gestori code remoti, più le impostazioni equivalenti per le applicazioni, che si connettono al gestore code migrato, incluso:

- Nomi connessione canale (attributoCONNAME).
- Le regole di autenticazione del canale che limitano le connessioni in entrata dal gestore code in base al relativo nome host o indirizzo IP.
- Tabelle CCDT (Client Channel Definition Table), DNS (Domain Name Settings), instradamento di rete o informazioni di connessione equivalenti.

m) Eseguire un failover gestito del gestore code su ciascun nodo RDQM per assicurarsi che la configurazione richiesta sia stata stabilita correttamente, fare riferimento a “Passaggio a un nodo di recupero” a pagina 573.

Ridimensionamento del filesystem per un gestore code DR RDQM
Per ridimensionare il filesystem per un gestore code di dati replicati (RDQM) di DR (Disaster Recovery) esistente, eseguire il backup dei propri dati persistenti, quindi ripristinare i dati su un gestore code RDQM appena creato con lo stesso nome ma con un filesystem di dimensione diversa.

Informazioni su questa attività

I gestori code di dati replicati DR richiedono un volume logico dedicato (filesystem) e la configurazione della replica del disco. Questi componenti vengono configurati solo quando viene creato un nuovo gestore code. Il file system non può essere ridimensionato dopo che è stato creato perché deve avere la stessa dimensione su ogni nodo. Per ridimensionare il filesystem per un gestore code di dati replicati esistente (RDQM), è possibile eseguire il backup dei dati persistenti, quindi ripristinare i dati su un gestore code RDQM appena creato che ha lo stesso nome ma un filesystem di dimensione diversa. Questa procedura conserva la configurazione del gestore code, lo stato e i messaggi persistenti al momento della creazione del backup.

Procedura

1. Eseguire il backup del gestore code RDQM esistente sul nodo RDQM primario:

a) Determinare il nodo RDQM primario per il gestore code. Per informazioni su come determinare il nodo primario, vedere rdqmstatus (visualizzazione dello stato RDQM) .

b) Sul nodo RDQM primario, se il gestore code RDQM è avviato, arrestarlo utilizzando il comando **endmqm -w** o **endmqm -i** .

c) Determinare l'ubicazione della directory dei dati del gestore code visualizzando il file di configurazione IBM MQ , `mqs.ini`. Su Linux, questo file si trova nella directory `/var/mqm` . Per ulteriori informazioni su `mqs.ini`, consultare “File di configurazione IBM MQ , mqs.ini” a pagina 84.

Individuare la sezione `QueueManager` per il gestore code nel file. La directory dei dati del gestore code è il valore della chiave denominata `DataPath`. Per ulteriori informazioni sulla stanza `QueueManager` , consultare “Stanza QueueManager del file mqs.ini” a pagina 95.

d) Creare un backup della directory dei dati del gestore code. Su Linux, è possibile eseguire questa operazione utilizzando il comando **tar** . Ad esempio, per eseguire il back up della directory di dati per un gestore code è possibile utilizzare il seguente comando. Notare l'ultimo parametro del comando, che è un singolo carattere punto (.):

```
tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
```

e) Determinare l'ubicazione della directory di log del gestore code visualizzando IBM MQ file di configurazione del gestore code `qm.ini`. Questo file si trova nella directory dei dati del gestore code. Per ulteriori informazioni sul file, consultare “File di configurazione del gestore code, qm.ini” a pagina 97.

La directory di log del gestore code è definita come il valore della chiave `LogPath` nella stanza Log. Per informazioni sulla sezione, consultare “Stanza di log del file qm.ini” a pagina 125.

f) Creare un backup della directory di log del gestore code. Su Linux, è possibile eseguire questa operazione utilizzando il comando **tar** . Ad esempio, per eseguire il back up della directory di log per un gestore code, è possibile utilizzare il seguente comando. Notare l'ultimo parametro del comando, che è un singolo carattere punto (.):

```
tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
```

g) Eliminare il gestore code RDQM esistente.

2. Ripristinare il gestore code con un filesystem della dimensione richiesta:

a) Creare un nuovo gestore code RDQM con lo stesso nome del gestore code di cui è stato eseguito il backup. Assicurarsi che il file system assegnato per il gestore code RDQM da **crtmqm** sia la dimensione richiesta e che sia sufficientemente grande per contenere i dati, i log primari e i log secondari per il gestore code esistente, più dello spazio aggiuntivo per l'espansione futura. Per informazioni su come creare un gestore code RDQM, consultare “Creazione di un RDQM di ripristino di emergenza” a pagina 559.

b) Determinare il nodo RDQM primario per il gestore code. Per informazioni su come determinare il nodo primario, vedere rdqmstatus (visualizzazione dello stato RDQM).

c) Sul nodo RDQM primario, se il gestore code RDQM è avviato, arrestarlo utilizzando il comando **endmqm -w** o **endmqm -i** .

d) Sul nodo RDQM primario, stabilire la nuova ubicazione delle directory di dati e di log per il gestore code RDQM (utilizzare i metodi descritti ai passi 1c e 1e).

e) Sul nodo RDQM primario, eliminare il contenuto dei dati del gestore code RDQM e le directory di log, ma non le directory stesse.

f) Sul nodo RDQM primario, ripristinare il backup della directory di dati del gestore code nella directory di dati vuota per il nuovo gestore code RDQM, verificando che la proprietà e le autorizzazioni del file siano conservate. Se il backup è stato creato utilizzando il comando **tar** di esempio nel passo 1d , il seguente comando può essere utilizzato dall'utente root per ripristinarlo:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

g) Sul nodo RDQM principale, ripristinare il backup della directory di log del gestore code nella directory di log vuota per il nuovo gestore code RDQM, verificando che la proprietà del file e le autorizzazioni siano conservate. Se il backup è stato creato utilizzando il comando **tar** di esempio nel passo 1f , il seguente comando può essere utilizzato dall'utente root per ripristinarlo:

```
tar -xvzpf qm-log.tar.gz -C queue_manager_log_dir
```

h) Sul nodo RDQM primario, modificare il file di configurazione del gestore code ripristinato, `qm.ini`, nella directory dei dati per il nuovo gestore code RDQM. Aggiornare il valore della chiave `LogPath` nella stanza `Log` per specificare la directory di log per il nuovo gestore code RDQM determinato al passo 2d. Esaminare gli altri percorsi file definiti nel file di configurazione e aggiornarli, se necessario. Ad esempio, potrebbe essere necessario aggiornare i seguenti percorsi:

- Il percorso per i file di log degli errori generati dai servizi di messaggi diagnostici.
- Il percorso per le uscite richieste dal gestore code.
- Il percorso per i file di caricamento switch se il gestore code è un coordinatore della transazione XA.

i) Verificare che il gestore code sia visualizzato dal comando **dspmq** e che il relativo stato sia riportato come ended. Il seguente esempio mostra l'output di esempio per un gestore code DR RDQM:

```
$ dspmq -o status -o dr
QMNAME(QM1) STATUS(Ended normally) DR(Primary)
```

j) Verificare che i dati del gestore code ripristinati siano stati replicati sul nodo RDQM secondario utilizzando il comando **rdqmstatus** per visualizzare lo stato del gestore code. Lo stato DR deve essere riportato come `Normal` su ciascun nodo. Il seguente esempio mostra l'output di esempio per un gestore code DR RDQM sul nodo primario:

```
$ rdqmstatus -m QM1
Queue manager status:                   Running
CPU:                                    0.00
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
DR role:                                Primary
DR status:                              Normal
DR type:                                Synchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
```

Il seguente esempio mostra l'output di esempio per un gestore code DR RDQM sul nodo di recupero:

```
Queue manager status:                   Ended immediately
DR role:                                Secondary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.20.2
DR remote IP address:                   192.168.20.1
```

k) Avviare il gestore code sul nodo RDQM primario.

l) Eseguire una commutazione del gestore code sul nodo di ripristino per assicurarsi che la configurazione richiesta sia stata stabilita correttamente, consultare “Passaggio a un nodo di recupero” a pagina 573.

V 9.1.5 *Archiviazione dello stato dell'applicazione persistente*

È possibile memorizzare le informazioni sullo stato persistente relative alle applicazioni insieme ad altri dati del gestore code.

Ogni gestore code IBM MQ dispone di un filesystem dedicato per il relativo stato persistente, che include sia i dati della coda che il log di recupero. In una configurazione RDQM, il filesystem è supportato da un volume logico replicato tra i sistemi Linux (nodi). Il file system include una directory `userdata` che è possibile utilizzare per memorizzare le informazioni sullo stato persistente per le applicazioni. Quindi, quando un gestore code di dati replicati si sposta per essere eseguito su un altro nodo nella

configurazione RDQM, è disponibile il contesto dell'applicazione e il contesto del gestore code. Vedere Contenuto della directory su Unix e Linux Systems.

Se si sceglie di memorizzare lo stato dell'applicazione nella directory `userdata` , è necessario tenere presente che i dati scritti in questa ubicazione potrebbero consumare lo spazio su disco disponibile assegnato al gestore code. È necessario assicurarsi che sia disponibile spazio su disco sufficiente per il gestore code per scrivere i dati della coda, i log e altre informazioni sullo stato persistente.

La directory `userdata` ha la proprietà utente e gruppo mqm ed è leggibile in modo che gli utenti possano accedervi senza dover far parte del gruppo di amministratori IBM MQ (mqm). Non è possibile modificare le autorizzazioni della directory `userdata` , ma è possibile creare il contenuto in essa con qualsiasi proprietà e autorizzazione richiesti.

Durante un failover del gestore code RDQM, il gestore code viene terminato e il relativo file system viene smontato sul nodo RDQM corrente. Il filesystem viene quindi montato e il gestore code viene riavviato su un altro nodo nella configurazione RDQM. Un file system non può essere smontato se un processo ha un handle aperto per uno dei suoi file. Per garantire che un failover del gestore code possa essere completato, se il filesystem del gestore code non può essere smontato, ai processi che hanno un handle di file aperto viene inviato un segnale SIGTERM, seguito da un SIGKILL se gli handle aperti non vengono rilasciati. Le applicazioni devono essere progettate per rispondere correttamente a SIGTERM. Se le applicazioni o i processi sono configurati come un servizio del gestore code, durante un failover gestito possono essere terminati durante l'arresto del gestore code prima che il filesystem venga smontato. Se un'applicazione o un processo non è configurato come servizio del gestore code o si verifica un failover non gestito, ad esempio una perdita del quorum, è probabile che i segnali vengano inviati per rilasciare il file system.

Linux V 9.1.0 *Gestione delle caratteristiche primarie e secondarie di RDQM DR*

È possibile modificare un gestore code di dati replicati di ripristino di emergenza secondario (DR RDQM) in un DR RDQM primario. È anche possibile modificare un'istanza primaria in un'istanza secondaria.

Informazioni su questa attività

Utilizzare il comando **rdqmdr** per modificare un'istanza secondaria di un RDQM nell'istanza primaria. Potrebbe essere necessario completare questa azione se si perde l'istanza primaria per qualche motivo. È quindi possibile avviare il gestore code e continuare l'esecuzione sul nodo di recupero.

Utilizzare il comando **rdqmdr** anche per modificare un'istanza primaria di un RDQM nell'istanza secondaria. Potrebbe essere necessario completare questa azione, ad esempio, se si stava riconfigurando il sistema.

È inoltre possibile utilizzare **rdqmdr** su un gestore code primario per richiamare il comando esatto necessario per creare un'istanza secondaria di tale gestore code sul nodo di recupero.

È possibile utilizzare il comando **rdqmdr** come utente nel gruppo `mqm` se l'utente può utilizzare sudo. Altrimenti, è necessario essere collegati come root.

Procedura

- Per modificare un'istanza secondaria di un DR RDQM in un'istanza primaria, immettere il comando seguente:

  ```
  rdqmdr -m QMname -p
  ```

  Questo comando non riesce se l'istanza primaria del gestore code è ancora in esecuzione e il collegamento di replica DR è ancora in funzione.
- Per modificare un'istanza principale del gestore code in un'istanza secondaria, immettere il comando seguente:

  ```
  rdqmdr -m QMname -s
  ```

- Per visualizzare il comando **crtmqm** richiesto per configurare l'istanza secondaria di un gestore code, immettere il seguente comando sul nodo primario:

  ```
  rdqmdr -d -m QMname
  ```

  È possibile immettere il comando **crtmqm** restituito sul nodo secondario per creare l'istanza secondaria di RD RDQM.

Linux V 9.1.0 *Avvio, arresto e visualizzazione dello stato di un DR RDQM*

Utilizzare le varianti dei comandi di controllo IBM MQ standard per avviare, arrestare e visualizzare lo stato corrente di un gestore code di dati replicati del ripristino di emergenza (DR RDQM).

Informazioni su questa attività

È necessario eseguire i comandi che avviano, arrestano e visualizzano lo stato corrente di un gestore code di dati replicati (RDQM) come utente appartenente al gruppo `mqm` .

È necessario eseguire i comandi per avviare e arrestare un gestore code sul nodo primario per tale gestore code (ossia, il nodo su cui il gestore code è attualmente in esecuzione).

Procedura

- Per avviare un DR RDQM, immettere il seguente comando sul nodo primario di RDQM:

  ```
  strmqm qmname
  ```

  dove *qmname* è il nome dell'RDQM che si desidera avviare.
- Per arrestare un RDQM, immettere il seguente comando sul nodo primario del RDQM:

  ```
  endmqm qmname
  ```

  dove *qmname* è il nome dell'RDQM che si desidera arrestare.
- Per visualizzare lo stato di un RDQM, immettere il seguente comando:

  ```
  dspmq -m QMname
  ```

  Le informazioni sullo stato che vengono emesse dipendono dal fatto che si esegua il comando sul nodo primario o secondario di RDQM. Se eseguito sul nodo primario, viene visualizzato uno dei normali messaggi di stato restituiti da **dspmq** . Se si esegue il comando su un nodo secondario, viene visualizzato lo stato `Ended immediately` . Ad esempio, se **dspmq** viene eseguito sul nodo RDQM7, potrebbero essere restituite le seguenti informazioni:

  ```
  QMNAME(DRQM8)                           STATUS(Ended immediately)
  QMNAME(DRQM7)                           STATUS(Running)
  ```

  È possibile utilizzare gli argomenti con `dspmq` per stabilire se un RDQM è configurato per il ripristino di emergenza e se è attualmente l'istanza primaria o secondaria:

  ```
  dspmq -m QMname -o (dr | DR)
  ```

  Viene visualizzata una delle seguenti risposte:

  DRROLE()
  Indica che il gestore code non è configurato per il ripristino di emergenza.

  DRROLE(Primary)
  Indica che il gestore code è configurato come DR primario.

  DRROLE(Secondary)
  Indica che il gestore code è configurato come secondario DR.

Riferimenti correlati
dspmq
endmqm
strmqm

Linux V 9.1.0 *Visualizzazione dello stato DR RDQM*

È possibile visualizzare lo stato di tutti i gestori code di dati replicati di ripristino di emergenza (RDQM DR) su un nodo o informazioni dettagliate per un RDQM DR specificato.

Informazioni su questa attività

Utilizzare il comando **rdqmstatus** per visualizzare lo stato di tutti i RDQM DR o dei singoli RDQM.

È necessario essere un utente nel gruppo `mqm` per eseguire il comando **rdqmstatus** . È possibile eseguire il comando su uno dei nodi della coppia DR RDQM.

Procedura

- Per visualizzare lo stato di tutti gli RDQM DR su un nodo, eseguire il seguente comando su tale nodo:

  ```
  rdqmstatus
  ```

  Viene visualizzato lo stato degli RDQM DR sul nodo, ad esempio:

  ```
  Queue manager name:                     DRQM8
  Queue manager status:                   Ended immediately
  DR role:                                Secondary

  Queue manager name:                     DRQM7
  Queue manager status:                   Running
  DR role:                                Primary
  ```

- Per visualizzare lo stato di un particolare RDQM, immettere il seguente comando:

  ```
  rdqmstatus -m  qmname
  ```

  La seguente tabella riepiloga le informazioni restituite.

Tabella 35. Attributi stato

Attributo Stato	**Valori possibili**	**Quando visualizzato**
Stato gestore code	stato (come visualizzato da `dspmq`)	Sempre visualizzato
CPU	*n.nn*%	Visualizzato solo quando RDQM sul nodo corrente ha un ruolo primario
Memoria	*nnn*MB	Visualizzato solo quando RDQM sul nodo corrente ha un ruolo primario
File system del gestore code	*nnn*MB utilizzati, *n.n*GB allocati [*n*%]	Visualizzato solo quando RDQM sul nodo corrente ha un ruolo primario
Ruolo DR	Principale Secondario Sconosciuto	Sempre visualizzato
Stato DR	Normale	Funzionamento normale

Tabella 35. Attributi stato (Continua)

Attributo Stato	Valori possibili	Quando visualizzato
	Sincronizzazione in corso	La sincronizzazione è in corso
	Partizionato	Il gestore code è stato avviato su entrambi i nodi mentre la rete di replica DR non è disponibile
	Sistema remoto non disponibile	La connessione all'altro nodo è stata persa
	Non congruente	Era in corso una sincronizzazione, ma è stata interrotta
	Ripristino all'istantanea	L'utente ha scelto di ripristinare l'istantanea acquisita quando il gestore code è entrato nello stato Incongruente.
	Sistema remoto non configurato	L'istanza primaria di RDQM è stata configurata, ma non è stata configurata alcuna istanza secondaria
	Negoziazione non riuscita	Uno dei nodi è stato impostato sulla replica sincrona e l'altro sulla replica asincrona
Tipo DR	Sincrono o asincrono	Sempre visualizzato
Porta DR	*numero_porta* (la porta TCP/IP utilizzata per replicare i dati per questo gestore code)	Sempre visualizzato
Indirizzo IP locale DR	L'indirizzo IP locale da cui questo gestore code esegue la replica per DR	Sempre visualizzato
Indirizzo IP remoto DR	L'indirizzo IP remoto su cui questo gestore code sta eseguendo la replica per DR	Sempre visualizzato
Dati DR non sincronizzati	*n*KB	Visualizzato quando il nodo remoto non è disponibile o non è congruente
Avanzamento della sincronizzazione DR	*n*%	Visualizzato quando la sincronizzazione è in corso
Tempo stimato DR per il completamento	*AAAA-MM-GG HH:MM:SS*	Visualizzato quando la sincronizzazione è in corso
Avanzamento ripristino istantanea	*n*%	Visualizzato quando lo stato DR è `Reverting to snapshot`. Lo stato viene contato in basso, quindi 0% mostra il completamento

Esempio

Esempio di stato normale sul nodo primario:

```
Queue manager status:                   Running
CPU:                                    0.00
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
DR role:                                Primary
DR status:                              Normal
DR type:                                Synchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
```

Esempio di stato normale su un nodo secondario:

```
Queue manager status:                   Ended immediately
DR role:                                Secondary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.20.2
DR remote IP address:                   192.168.20.1
```

Esempio di stato sul nodo primario quando è in corso la sincronizzazione:

```
Queue manager status:                   Running
CPU:                                    0.53
Memory:                                 124MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
DR role:                                Primary
DR status:                              Synchronization in progress
DR type:                                Synchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
DR synchronization progress:            11.0%
DR estimated time to completion:        2017-09-06 14:55:05
```

Esempio di un nodo primario, che mostra che è partizionato:

```
Queue manager status:                   Running
CPU:                                    0.02
Memory:                                 124MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
DR role:                                Primary
DR status:                              Partitioned
DR type:                                Synchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
```

Riferimenti correlati

Linux rdqmstatus

Linux V 9.1.0 *Funzionamento in un ambiente di ripristino di emergenza*

Esistono diverse situazioni in cui è possibile passare al gestore code secondario in una configurazione di ripristino di emergenza.

Ripristino di emergenza

Dopo la perdita completa del gestore code primario sul sito principale, si avvia il gestore code secondario sul sito di recupero. Le applicazioni si riconnettono al gestore code sul sito di recupero e il gestore code secondario elabora i messaggi dell'applicazione. I passi intrapresi per ripristinare la configurazione precedente dipendono dalla causa dell'errore. Ad esempio, perdita completa del nodo principale rispetto a perdita temporanea.

Per le operazioni da eseguire in seguito ad una perdita temporanea del sito principale, consultare “Passaggio a un nodo di recupero” a pagina 573. Per le operazioni da eseguire dopo un errore permanente, consultare “Sostituzione di un nodo malfunzionante in una configurazione di ripristino di emergenza” a pagina 574.

Supporto test di ripristino di emergenza
È possibile verificare la configurazione del ripristino di emergenza passando temporaneamente all'istanza secondaria e controllando che le applicazioni possano connettersi correttamente. Si segue la stessa procedura di quando si passa da un errore temporaneo del nodo primario a un altro, consultare “Passaggio a un nodo di recupero” a pagina 573.

Ripristino all'istantanea
Se si verifica un errore nel nodo primario mentre è in corso una sincronizzazione, è possibile ripristinare l'istantanea acquisita dei dati del gestore code secondario appena prima dell'inizio della sincronizzazione. Il secondario viene quindi ripristinato ad uno stato congruente e può essere eseguito come primario. Per ripristinare l'istantanea, rendere il secondario come principale, come descritto in “Passaggio a un nodo di recupero” a pagina 573. È necessario controllare che il ripristino dell'istantanea sia stato completato (utilizzando il comando **rdqmstatus**) prima di avviare il gestore code.

Linux V 9.1.0 *Passaggio a un nodo di recupero*

Se si verifica una situazione di emergenza nel sito principale, eseguire le operazioni per passare al sito di ripristino.

Informazioni su questa attività

In seguito alla perdita del gestore code primario sul sito principale, si rende il gestore code secondario sul sito di ripristino nel sito primario e lo si avvia. Le applicazioni si riconnettono al gestore code sul sito di recupero e il gestore code elabora i messaggi dell'applicazione. È possibile utilizzare questa procedura anche per verificare il nodo di recupero.

Importante: È necessario assicurarsi che l'istanza primaria di un gestore code sia arrestata e resa un'istanza secondaria prima di promuovere l'istanza secondaria originale. Altrimenti i dati partizionati possono accumularsi.

È necessario essere collegati come root o come utente che appartiene al gruppo `mqm` e che dispone della configurazione sudo necessaria.

Procedura

1. Se si utilizza questa procedura per verificare il gestore code secondario (ovvero, l'istanza primaria è ancora in esecuzione), è necessario arrestare l'istanza primaria e designarla nuovamente come istanza secondaria:

   ```
   endmqm qmname
   rdqmdr -m qmname -s
   ```

2. Rendere il gestore code secondario primario immettendo il seguente comando sul nodo di recupero:

   ```
   rdqmdr -m qmname -p
   ```

3. Avviare il gestore code mediante il comando:

   ```
   strmqm qmname
   ```

4. Verificare che le proprie applicazioni si riconnettano al gestore code sul gestore code di ripristino. Se sono stati definiti i canali con un elenco di nomi di connessione alternativi, specificando i gestori code primari e secondari, le applicazioni si connetteranno automaticamente al nuovo gestore code primario.

Riferimenti correlati
strmqm
rdqmdr

Linux V 9.1.0 *Sostituzione di un nodo malfunzionante in una configurazione di ripristino di emergenza*

Se si perde uno dei nodi in una configurazione di ripristino di emergenza, è possibile sostituire il nodo e ripristinare la configurazione di ripristino di emergenza seguendo questa procedura.

Informazioni su questa attività

Se si verifica una situazione di emergenza tale che il nodo nel sito principale è irreparabile, è possibile sostituire il nodo in errore mentre il gestore code viene eseguito sul nodo di recupero e quindi ripristinare la configurazione di ripristino di emergenza originale. Il nodo di sostituzione deve assumere l'identità del nodo non riuscito: il nome e l'indirizzo IP devono essere uguali.

È necessario essere collegati come root o come utente che appartiene al gruppo `mqm` e che dispone della configurazione sudo necessaria.

Procedura

A seguito della perdita del gestore code sul sito principale, effettuare le seguenti operazioni:

1. Sul nodo di recupero, eseguire i seguenti comandi per fare in modo che il gestore code secondario assuma il ruolo primario:

   ```
   rdqmdr -m QMname -p
   ```

   Dove *QMname* è il nome del gestore code.
2. Richiamare il comando che sarà necessario eseguire sul nodo primario di sostituzione per riconfigurare il ripristino di emergenza:

   ```
   rdqmdr -m QMname -d
   ```

   Copiare l'emissione di questo comando.
3. Eseguire il seguente comando per avviare il gestore code:

   ```
   strmqm QMname
   ```
4. Assicurarsi che le applicazioni si riconnettano al gestore code sul nodo di recupero. Se sono stati definiti i canali con un elenco di nomi di connessione alternativi, specificando i gestori code primari e secondari, le applicazioni si connetteranno automaticamente al nuovo gestore code primario.
5. Sostituire il nodo in errore sul proprio sito principale e configurarlo in modo che abbia lo stesso nome e indirizzo IP utilizzato per il ripristino di emergenza sul nodo originale. Quindi, configurare il ripristino di emergenza eseguendo il comando **crtmqm** copiato nel passo 2. Ora si dispone di un'istanza secondaria del gestore code e l'istanza primaria sincronizza i suoi dati con l'istanza secondaria.
6. Terminare l'istanza primaria corrente.
7. Una volta completata la sincronizzazione, rendere nuovamente secondaria l'istanza primaria in esecuzione sul nodo di ripristino:

   ```
   rdqmdr -m QMname -s
   ```
8. Sul nodo primario di sostituzione, rendere l'istanza secondaria del gestore code nell'istanza primaria:

   ```
   rdqmdr -m QMname -p
   ```
9. Sul nodo primario di sostituzione, avviare il gestore code:

   ```
   strmqm QMname
   ```

   La configurazione è stata ripristinata come prima dell'errore nel sito principale.

Riferimenti correlati
strmqm
rdqmdr
endmqm

Risoluzione di un problema incongruente in DR RDQM
Uno stato DR di `inconsistent` può essere riportato se la sincronizzazione ha esito negativo tra le istanze primaria e secondaria di un gestore code.

Informazioni su questa attività

Uno stato incongruente viene riportato sull'istanza secondaria di un gestore code poiché la connessione di replica all'istanza primaria viene persa durante un'operazione di sincronizzazione. Potrebbe essere necessario intraprendere un'azione per risolvere questa situazione. Considerare la seguente sequenza di eventi:

1. Gestore code primario DR sincronizzato con il gestore code secondario DR
2. Link di replica perso tra primario e secondario
3. Link di replica ripristinato tra primario e secondario
4. Una risincronizzazione si verifica quando il gestore code secondario DR raggiunge il gestore code primario DR. Durante questo tempo, lo stato DR di `synchronization in progress` viene notificato per entrambi i gestori code.
5. Se la replica viene nuovamente persa durante la risincronizzazione, lo stato sul DR secondario viene riportato come `Inconsistent`.

Se il nodo che ospita il gestore code primario è ancora operativo e il link di replica può essere ripristinato, la risincronizzazione avviene automaticamente. Lo stato incongruente viene risolto senza intraprendere alcuna azione.

Se il nodo che ospita il gestore code primario non è più operativo, è possibile risolvere lo stato incongruente implementando un ripristino all'istantanea sul gestore code secondario. Questa operazione riporta i dati all'ultimo stato valido noto.

Procedura

Per risolvere uno stato incongruente:

1. Sul nodo di recupero, rendere l'istanza secondaria nell'istanza primaria:

   ```
   rdqmdr -m qmname -p
   ```

   Viene avviata l'operazione di ripristino dell'istantanea.
2. Sul nodo di recupero, controllare lo stato del gestore code per verificare quando l'operazione di ripristino dell'istantanea è completa:

   ```
   rdqmstatus -m qmname
   ```
3. Quando lo stato del gestore code è `Normal`, avviare il gestore code:

   ```
   strmqm qmname
   ```

Risoluzione di un problema partizionato (split brain) in DR RDQM
Un problema partizionato può verificarsi se entrambi i gestori code in una coppia di ripristino di emergenza vengono eseguiti contemporaneamente nel ruolo primario.

Informazioni su questa attività

Se è stata promossa l'istanza secondaria di un gestore code sul nodo di recupero mentre l'istanza primaria originale continuava ad essere eseguita sul nodo principale, si dispone effettivamente di due

versioni dello stesso gestore code in esecuzione, ciascuna con la propria vista dei dati del gestore code. Lo stato DR per il gestore code su ciascun nodo è riportato come `Partitioned`.

È necessario decidere quale dei due gestori code ha la vista più corretta dei dati e conservare tale serie eliminando l'altro. Utilizzare il comando **rdqmdr** per completare questa operazione.

Procedura

- Per conservare i dati dal Gestore code sul nodo di recupero:
  a) Verificare che entrambe le istanze del gestore code siano arrestate.
  b) Specificare che il gestore code sul nodo principale è il secondario:

```
rdqmdr -m qmname -s
```

  c) Specificare che il gestore code sul nodo di ripristino è il principale:

```
rdqmdr -m qmname -p
```

  La sincronizzazione inizia con i dati del gestore code sul nodo di recupero copiati sul nodo principale.
  d) Verificare lo stato della sincronizzazione:

```
rdqmstatus -m qmname
```

  e) Una volta completata la sincronizzazione, degradare il gestore code sul nodo di recupero:

```
rdqmdr -m qmname -s
```

  f) Promuovere il gestore code sul nodo principale e avviarlo:

```
rdqmdr -m qmname -p
strmqm qmname
```

- Per conservare i dati dal gestore code sul nodo principale:
  a) Verificare che entrambe le istanze del gestore code siano arrestate.
  b) Specificare che il gestore code sul nodo di ripristino è il secondario:

```
rdqmdr -m qmname -s
```

  c) Specificare che il gestore code sul nodo principale è il principale:

```
rdqmdr -m qmname -p
```

  Inizia la sincronizzazione, con i dati dal gestore code sul nodo principale copiati sul nodo di recupero.
  d) Verificare lo stato della sincronizzazione:

```
rdqmstatus -m qmname
```

  e) Una volta completata la sincronizzazione, avviare il gestore code sul nodo principale:

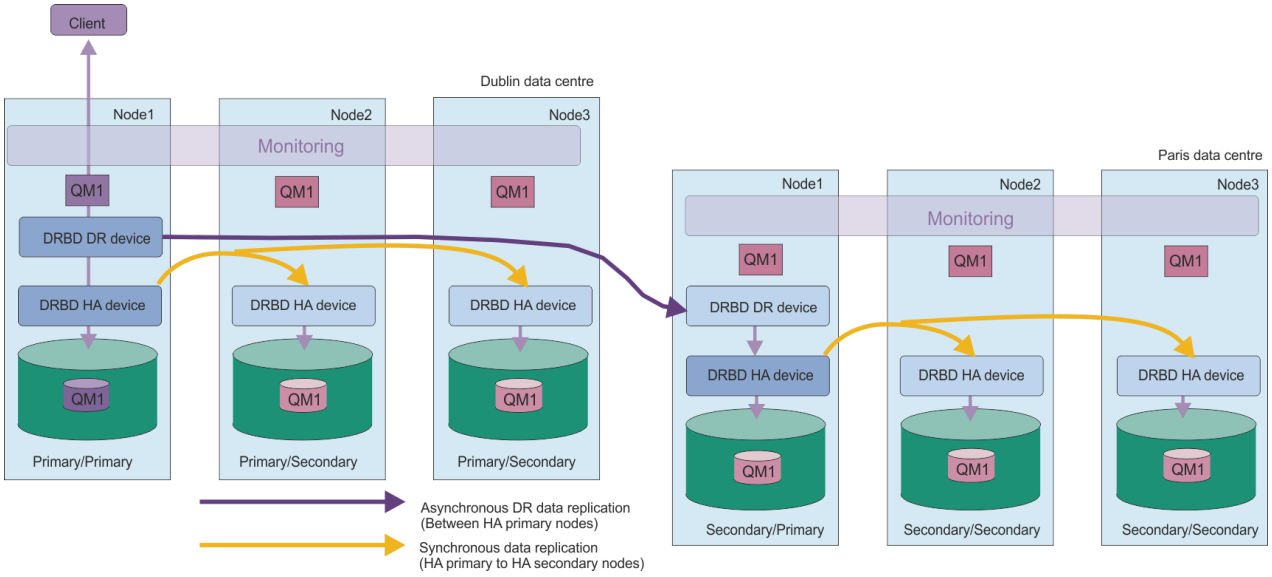
```
strmqm qmname
```

V 9.1.5 Linux RDQM disaster recovery e alta disponibilità

È possibile configurare un gestore code di dati replicati (RDQM) che viene eseguito su un gruppo ad alta disponibilità su un sito, ma può eseguire il failover su un altro gruppo ad alta disponibilità su un altro sito se si verifica una situazione di emergenza che rende il primo gruppo non disponibile. Questo è noto come DR/HA RDQM.

Un RDQM DR/HA combina le funzioni di un RDQM ad elevata disponibilità (consultare “Alta disponibilità RDQM” a pagina 531) e un RDQM di ripristino di emergenza (consultare “Ripristino di emergenza RDQM” a pagina 555).

Il seguente diagramma mostra un esempio di DR/HA RDQM.



La replica tra RDQM DR/HA sul sito principale e il sito di ripristino di emergenza è sempre asincrona. Con la replica asincrona, operazioni come IBM MQ PUT o GET completano e ritornano all'applicazione prima che l'evento venga replicato sul gestore code secondario.

È possibile avere due siti attivi invece di siti 'main' e 'recovery ', se necessario, quindi alcuni dei RDQM DR/HA vengono eseguiti su un sito e alcuni sull'altro durante il normale funzionamento. Se si verifica un'emergenza e un sito diventa non disponibile, tutti gli RDQM DR/HA vengono eseguiti sullo stesso gruppo HA nello stesso sito.

Ogni gruppo HA è configurato nello stesso modo di un gruppo HA ordinario. È possibile definire indirizzi IP mobili per un RDQM DR/HA in ogni gruppo HA. L'indirizzo IP mobile può essere lo stesso o diverso per ogni gruppo HA.

Non è possibile aggiornare un RDQM esistente in modo che sia DR/HA RDQM, è necessario creare un RDQM DR/HA. (Se necessario, è possibile eseguire il backup dei dati di un RDQM esistente, eliminarli, ricrearli come RDQM DR/HA e quindi ripristinare i dati, consultare “Backup e ripristino dei dati del gestore code IBM MQ” a pagina 621.)

Per configurare RDQM DR/HA, è necessario completare le seguenti operazioni principali:

1. Configurare un gruppo HA sul sito 'principale'.
2. Configurare un gruppo HA sul sito 'recovery'.
3. Creare un RDQM primario / primario DR/HA su un nodo del gruppo HA nel sito 'principale'.
4. Creare RDQM DR/HA primari / secondari sugli altri due nodi nel sito 'principale'.
5. Definire un indirizzo IP mobile per un'applicazione per accedere al DR/HA RDQM quando è in esecuzione su uno dei nodi del gruppo HA sul sito 'principale'.
6. Creare un RDQM DR/HA secondario / primario su un nodo del gruppo HA sul sito 'recovery'.
7. Creare RDQM secondario / secondario DR/HA sugli altri due nodi nel sito 'recovery'.
8. Definire un indirizzo IP mobile per un'applicazione per accedere al DR/HA RDQM quando è in esecuzione su uno qualsiasi dei nodi del gruppo HA sul sito 'recovery'.

I dettagli su ciascuno di questi passi sono forniti nei seguenti argomenti.

V 9.1.5 Linux *Requisiti per una soluzione DR/HA RDQM*

I requisiti per la soluzione DR/HA RDQM sono gli stessi della soluzione HA RDQM e della soluzione DR RDQM.

Per i requisiti per le parti HA della configurazione, consultare “Requisiti per la soluzione RDQM HA” a pagina 533.

Per i dettagli della parte DR della configurazione, vedere “Requisiti per la soluzione RDQM DR” a pagina 558.

V 9.1.5 Linux *Configurazione di gruppi HA per RDQM DR/HA*

È necessario creare un gruppo HA sia sul sito principale che su quello di ripristino. Se si dispone di un gruppo HA esistente su entrambi i siti, è possibile creare RDQM DR/HA in tale gruppo HA. (Gli RDQM esistenti continueranno a funzionare come prima.)

La procedura è la stessa descritta per l'alta disponibilità RDQM, consultare “Definizione del cluster Pacemaker (gruppo HA)” a pagina 536.

Quando si definisce un gruppo ad alta disponibilità, specificare gli indirizzi IP utilizzati per il controllo e la replica da ogni nodo nel file `rdqm.ini` . Quando si crea un gruppo HA per supportare RDQM DR/HA, è possibile anche specificare gli indirizzi IP utilizzati per la replica DR dal gruppo HA che si sta definendo e gli indirizzi IP utilizzati per la replica DR dai nodi nell'altro gruppo HA della coppia DR. (Se non si specificano gli indirizzi IP di replica DR nel file `rdqm.ini` , è possibile specificarli nella riga comandi quando si crea un RDQM DR/HA.)

Se si sta configurando un gruppo HA esistente, è possibile aggiungere gli indirizzi IP di replica DR al file `rdqm.ini` esistente. Non è necessario eseguire nuovamente **rdqmadm** dopo l'aggiornamento `rdqm.ini`, ma è necessario aggiornare `rdqm.ini` prima di creare RDQM DR/HA.

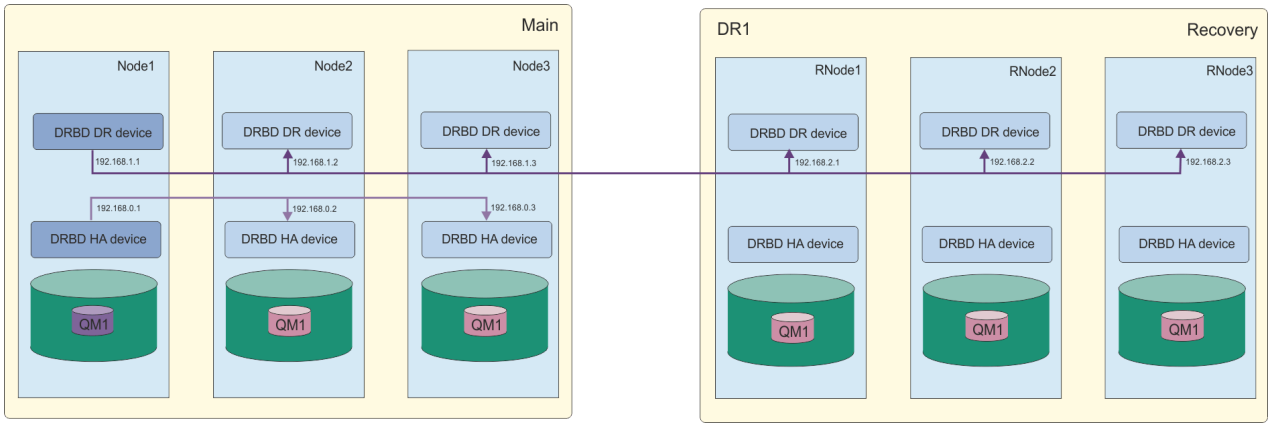
Utilizzare l'attributo `DR_Replication` nelle stanze `Node` per specificare le interfacce di replica DR sul gruppo HA che si sta definendo, ad esempio:

```
Node:
  Name=Node1
  HA_Replication=192.168.0.1
  DR_Replication=192.168.1.1
Node:
  Name=Node2
  HA_Replication=192.168.0.2
  DR_Replication=192.168.1.2
Node:
  Name=Node3
  HA_Replication=192.168.0.3
  DR_Replication=192.168.1.3
```

Utilizzare la sezione `DRGroup` per specificare gli indirizzi di replica DR del gruppo HA remoto, ad esempio:

```
DRGroup:
  Name=DR1
  DR_Replication=192.168.2.1
  DR_Replication=192.168.2.2
  DR_Replication=192.168.2.3
```

Il seguente diagramma illustra questa configurazione:



Se non si specificano gli indirizzi IP di replica DR per i nodi nel gruppo HA locale nel file `rdqm.ini` o sulla riga comandi quando si crea un RDQM DR/HA, le interfacce `HA_Replication` definite per ciascun nodo vengono utilizzate per la replica DR. È necessario specificare gli indirizzi di replica DR del gruppo HA remoto nel file `rdqm.ini` o sulla riga comandi **`crtmqm`** .

V 9.1.5 Linux *Creazione di RDQM DR/HA*

Utilizzare il comando **`crtmqm`** per creare un gestore code di dati replicati (RDQM) in una configurazione DR/HA.

Informazioni su questa attività

È possibile creare un RDQM DR/HA come utente nel gruppo `mqm` se l'utente può utilizzare sudo. Altrimenti, è necessario creare l'RDQM come root.

È necessario creare un numero di RDQM DR/HA:

- Sul gruppo HA sul sito 'principale':
  - Sul nodo in cui si desidera che il gestore code venga eseguito in condizioni normali, creare il DR/HA RDQM primario / primario.
  - Su ciascuno degli altri due nodi nel gruppo HA, creare un RDQM DR/HA primario / secondario.
- Sul gruppo HA sul sito 'recovery':
  - Sul nodo in cui verrà eseguito il gestore code se si verifica un failover sul sito di recupero, creare il DR/HA RDQM secondario / primario. È possibile utilizzare l'output del comando quando è stato creato il gestore code primario / primario sul sito 'principale'.
  - Su ognuno degli altri due nodi nel gruppo HA, creare un RDQM secondario / secondario DR/HA.

A tutte le istanze del gestore code deve essere assegnato lo stesso nome e la stessa quantità di memoria.

Procedura

- Per creare il DR/HA RDQM primario / primario:

  a) Immettere il seguente comando:

```
crtmqm -sx -rr p
              [-rl DRLocalIP1,DRLocalIP2,DRLocalIP3]
              (-ri DRRemoteIP1,DRRemoteIP2,DRRemoteIP3 | -rn GroupName)
              -rp DRPort
              [-z] [-q] [-c Text] [-d DefXmitQ] [-h MaxHandles]
              [-g ApplicationGroup] [-oa user|group]
              [-t TrigInt] [-u DeadQ] [-x MaxUMsgs]
              [-lp LogPri] [-ls LogSec]
              [-lc | -ll | -lla | -lln] [-lf LogFileSize]
              [-p Port] [-fs FilesystemSize] QMgrName
```

  Dove:

-sx
Indica che il ruolo HA iniziale è primario.

-rr p
Indica che il ruolo DR iniziale è primario.

-rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
Facoltativamente, specificare gli indirizzi IP delle interfacce DR sui tre nodi sul sito locale (ovvero, il sito 'principale'). Se non specificato, vengono utilizzati gli indirizzi IP specificati nel file `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Specificare gli indirizzi IP delle interfacce DR sui tre nodi sul sito remoto (ovvero, il sito 'recovery'). È necessario specificare questo parametro o il parametro `-rn` .

-rn *GroupName*
Specificare il nome del gruppo HA remoto come specificato nel file `rdqm.ini` . È necessario specificare `-ri` o `-rn`.

-rp *Porta*
Specifica la porta da utilizzare per la replica DR.

altre opzioni crtmqm_options
Facoltativamente, è possibile specificare una o più delle seguenti opzioni **crtmqm** generali:

- -z
- -q
- -c *Testo*
- -d *DefaultTransmissionDefaultTransmission*
- -h *MaxHandles*
- -g *ApplicationGroup*
- -oa utente | gruppo
- -t *TrigInt*
- -u *DeadQ*
- -x *MaxUMsgs*
- -lp *LogPri*
- -ls *LogSec*
- -lc | -l
- -lla | -lln
- -lf *LogFileDimensione*
- -p *Porta*

-fs *dimensione*
Facoltativamente, specifica la dimensione del file system da creare per il gestore code, ossia la dimensione del volume logico creato nel gruppo di volumi drbdpool. Viene creato anche un altro volume logico di tale dimensione, per supportare il ripristino dell'operazione di istantanea, in modo che la memoria totale per il DR RDQM sia poco più del doppio di quella specificata qui.

QMNAME
Specifica il nome del gestore code di dati replicato. Il nome è sensibile al maiuscolo/minuscolo.

Una volta completato il comando, viene emesso il comando che è possibile immettere sul sito di recupero per creare l'istanza secondaria / primaria del gestore code.

- Per creare un RDQM DR/HA primario / secondario sugli altri due nodi nel gruppo HA:

  a) Immettere il comando seguente su ciascun nodo:

```
crtmqm -sxs -rr p
             [-rl DRLocalIP1,DRLocalIP2,DRLocalIP3]
             (-ri DRRemoteIP1,DRRemoteIP2,DRRemoteIP3 | -rn GroupName)
```

```
              -rp DRPort
              [-fs FilesystemSize] QMgrName
```

Dove:

-sxs
Indica che il ruolo HA iniziale è secondario.

-rr p
Indica che il ruolo DR iniziale è primario.

-rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
Facoltativamente, specificare gli indirizzi IP delle interfacce DR sui tre nodi sul sito locale (ovvero, il sito 'principale'). Se non specificato, vengono utilizzati gli indirizzi IP specificati nel file `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Specificare gli indirizzi IP delle interfacce DR sui tre nodi sul sito remoto (ovvero, il sito 'recovery'). È necessario specificare questo parametro o il parametro `-rn` .

-rn *GroupName*
Specificare il nome del gruppo HA remoto come specificato nel file `rdqm.ini` . È necessario specificare `-ri` o `-rn`.

-rp *Porta*
Specifica la porta da utilizzare per la replica DR.

-fs *dimensione*
Specifica la dimensione del file system da creare per il gestore code, ovvero la dimensione del volume logico creato nel gruppo di volumi drbdpool. Se è stata specificata una dimensione non predefinita quando si crea l'RDQM primario / primario, è necessario specificare qui lo stesso valore.

QMNAME
Specifica il nome dell'RDQM primario / secondario. Deve essere uguale al nome specificato per l'istanza primaria / primaria di RDQM. Notare che il nome è sensibile al maiuscolo / minuscolo.

- Per creare un RDQM DR/HA secondario / primario sul nodo su cui verrà eseguito il gestore code in caso di failover sul sito di ripristino:

  a) Utilizzare l'output del comando quando si è creato il DR/HA primario / primario sul sito principale oppure immettere il seguente comando:

```
crtmqm -sx -rr s
              [-rl DRLocalIP1,DRLocalIP2,DRLocalIP3]
              (-ri DRRemoteIP1,DRRemoteIP2,DRRemoteIP3 | -rn GroupName)
              -rp DRPort
              [-fs FilesystemSize] QMgrName
```

-sx
Indica che il ruolo HA iniziale è primario.

-rr s
Indica che il ruolo DR iniziale è secondario.

-rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
Facoltativamente, specificare gli indirizzi IP delle interfacce DR sui tre nodi sul sito locale (ovvero, il sito 'recovery'). Se non specificato, vengono utilizzati gli indirizzi IP specificati nel file `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Specificare gli indirizzi IP delle interfacce DR sui tre nodi sul sito remoto (ovvero, il sito 'principale'). È necessario specificare questo parametro o il parametro `-rn` .

-rn *GroupName*
Specificare il nome del gruppo HA remoto come specificato nel file `rdqm.ini` . È necessario specificare `-ri` o `-rn`.

-rp *Porta*
Specifica la porta da utilizzare per la replica DR.

-fs *dimensione*
Facoltativamente, specifica la dimensione del file system da creare per il gestore code, ossia la dimensione del volume logico creato nel gruppo di volumi drbdpool. Viene creato anche un altro volume logico di tale dimensione, per supportare il ripristino dell'operazione di istantanea, in modo che la memoria totale per il DR RDQM sia poco più del doppio di quella specificata qui.

QMNAME
Specifica il nome del gestore code di dati replicato. Il nome è sensibile al maiuscolo/minuscolo.

- Per creare un RDQM secondario / secondario HA/DR sugli altri due nodi sul sito di ripristino:

  a) Immettere il comando seguente su ciascun nodo:

```
crtmqm -sxs -rr s
             [-rl DRLocalIP1,DRLocalIP2,DRLocalIP3]
             (-ri DRRemoteIP1,DRRemoteIP2,DRRemoteIP3 | -rn GroupName)
             -rp DRPort
             [-fs FilesystemSize] QMgrName
```

-sxs
Indica che il ruolo HA iniziale è primario.

-rr s
Indica che il ruolo DR iniziale è secondario.

-rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
Facoltativamente, specificare gli indirizzi IP delle interfacce DR sui tre nodi sul sito locale. Se non specificato, vengono utilizzati gli indirizzi IP specificati nel file `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Specificare gli indirizzi IP delle interfacce DR sui tre nodi sul sito remoto. È necessario specificare questo parametro o il parametro `-rn` .

-rn *GroupName*
Specificare il nome del gruppo HA remoto come specificato nel file `rdqm.ini` . È necessario specificare `-ri` o `-rn`.

-rp *Porta*
Specifica la porta da utilizzare per la replica DR.

-fs *dimensione*
Facoltativamente, specifica la dimensione del file system da creare per il gestore code, ossia la dimensione del volume logico creato nel gruppo di volumi drbdpool. Viene creato anche un altro volume logico di tale dimensione, per supportare il ripristino dell'operazione di istantanea, in modo che la memoria totale per il DR RDQM sia poco più del doppio di quella specificata qui.

QMNAME
Specifica il nome del gestore code di dati replicato. Il nome è sensibile al maiuscolo/minuscolo.

Operazioni successive

Una volta create tutte le RDQM DR/HA, è necessario controllare lo stato sulle istanze primaria / primaria e secondaria / primaria per verificare che siano tutte corrette. Utilizzare il comando **rdqmstatus** sui nodi. I nodi devono visualizzare lo stato normale come descritto in "Visualizzazione dello stato del gruppo DR/HA RDQM e HA" a pagina 584. Se non stanno visualizzando questo stato, eliminare l'istanza secondaria / primaria e ricrearla, facendo attenzione a utilizzare gli argomenti corretti.

Attività correlate

"Creazione di RDQM DR/HA" a pagina 579
Utilizzare il comando **crtmqm** per creare un gestore code di dati replicati (RDQM) in una configurazione DR/HA.

Riferimenti correlati

crtmqm

V 9.1.5 Linux *Eliminazione di un RDQM DR/HA*

Utilizzare il comando **dltmqm** per eliminare un gestore code di dati replicati DR/HA (RDQM).

Informazioni su questa attività

È necessario eseguire il comando per eliminare l'RDQM sia sul nodo primario / primario che sul nodo secondario / primario. RDQM deve essere terminato per primo. È possibile eseguire il comando come un utente mqm se tale utente dispone dei privilegi sudo necessari. Altrimenti, è necessario eseguire il comando come root.

Procedura

- Per cancellare un RDQM DR/HA, immettere il seguente comando:

```
dltmqm RDQM_name
```

Riferimenti correlati

dltmqm

V 9.1.5 Linux *Creazione di un indirizzo IP mobile*

È possibile creare indirizzi IP mobili per ciascuno dei gruppi HA in una configurazione RDQM DR/HA.

Un indirizzo IP mobile consente a un client di utilizzare lo stesso indirizzo IP per un RDQM DR/HA indipendentemente dal nodo in un gruppo HA su cui è in esecuzione. Se i tuoi due gruppi HA hanno reti private / isolate per la connettività dell'applicazione, è possibile definire lo stesso indirizzo IP mobile per entrambi i gruppi. Devi ancora definire tale indirizzo IP mobile due volte, tuttavia, una volta su ognuno dei gruppi HA.

Gli indirizzi IP mobili vengono creati ed eliminati utilizzando lo stesso metodo di un RDQM HA. Consultare “Creazione ed eliminazione di un indirizzo IP mobile” a pagina 548.

V 9.1.5 Linux *Avvio, arresto e visualizzazione dello stato di un RDQM DR/HA*

Utilizzare le varianti dei comandi di controllo IBM MQ standard per avviare, arrestare e visualizzare lo stato corrente di un RDQM DR/HA.

Informazioni su questa attività

È necessario eseguire i comandi che avviano, arrestano e visualizzano lo stato corrente di un RDQM DR/HA come un utente che appartiene ai gruppi `mqm` e `haclient` .

È necessario eseguire i comandi per avviare e arrestare un gestore code sul nodo primario per tale gestore code.

Procedura

- Per avviare un RDQM, immettere il seguente comando sul nodo primario di RDQM:

```
strmqm qmname
```

  dove *qmname* è il nome del DR/HA RDQM che si desidera avviare.

  RDQM viene avviato e Pacemaker avvia la gestione di RDQM. È necessario specificare l'opzione `-ns` con `strmqm` se si desidera specificare altre opzioni `strmqm` .
- Per arrestare un RDQM, immettere il seguente comando sul nodo primario del DR/HA RDQM:

```
endmqm qmname
```

  dove *qmname* è il nome dell'RDQM che si desidera arrestare.

  Pacemaker cessa di gestire RDQM, quindi l'RDQM viene terminato. Tutti gli altri parametri **endmqm** possono essere utilizzati quando si arresta un RDQM.
- Per visualizzare lo stato di un RDQM, immettere il seguente comando:

```
dspmq -m QMname
```

Le informazioni sullo stato che vengono emesse dipendono dal fatto che si esegua il comando sul nodo primario o secondario di RDQM. Se eseguito sul nodo primario, viene visualizzato uno dei normali messaggi di stato restituiti da **dspmq** . Se si esegue il comando su un nodo secondario, viene visualizzato lo stato `Ended immediately` . Ad esempio, se **dspmq** viene eseguito sul nodo RDQM7, potrebbero essere restituite le seguenti informazioni:

```
QMNAME(DRQM8)                           STATUS(Ended immediately)
QMNAME(DRQM7)                           STATUS(Running)
```

È possibile utilizzare gli argomenti con `dspmq` per stabilire se un RDQM è configurato per il ripristino di emergenza e se è attualmente l'istanza primaria o secondaria:

```
dspmq -m QMname -o (dr | DR)
```

Viene visualizzata una delle seguenti risposte:

DRROLE()
Indica che il gestore code non è configurato per il ripristino di emergenza.

DRROLE(Primary)
Indica che il gestore code è configurato come DR primario.

DRROLE(Secondary)
Indica che il gestore code è configurato come secondario DR.

Utilizzare il comando **dspmq -o all** per visualizzare le informazioni sul ripristino di emergenza e sull'alta disponibilità per RDQM DR/HA. Ad esempio, se si esegue **dspmq -o all** sul nodo in cui è in esecuzione DR/HA RDQM, vengono visualizzate le seguenti informazioni sullo stato:

```
QMNAME(TESTQM1)                                           STATUS(Running) HA(Replicated)
DRROLE(Primary)
```

Riferimenti correlati
dspmq (visualizza gestori code)
endmqm (fine gestore code)
strmqm (avvio gestore code)

V 9.1.5 Linux *Visualizzazione dello stato del gruppo DR/HA RDQM e HA*

È possibile visualizzare lo stato HA e il ruolo DR dei gestori code di dati replicati DR/HA (RDQM).

Informazioni su questa attività

Utilizzare il comando **rdqmstatus** per visualizzare lo stato di singoli RDQM o ottenere una panoramica dello stato di tutti gli RDQM noti al gruppo HA.

È necessario essere un utente nei gruppi `mqm` e `haclient` per eseguire il comando **rdqmstatus** . È possibile eseguire il comando su uno qualsiasi dei nodi in uno dei gruppi HA.

Procedura

- Per visualizzare lo stato di un nodo e gli RDQM che fanno parte della configurazione HA:

  ```
  rdqmstatus
  ```

  Viene visualizzata l'identità del nodo su cui è stato eseguito il comando e lo stato degli RDQM nella configurazione HA, più il ruolo DR corrente, ad esempio:

  ```
  Node:                                   main-alice

  Queue manager name:                     RDQM1
  Queue manager status:                   Running elsewhere
  ```

```
HA current location:                    main-charlie

Queue manager name:                     RDQM9
Queue manager status:                   Running elsewhere
HA current location:                    main-bob
DR role:                                Primary

Queue manager name:                     RDQM7
Queue manager status:                   Running
HA current location:                    This node
DR role:                                Primary
```

In questo esempio RDQM7 e RDQM8 sono entrambi RDQM DR/HA, mentre RDQM1 è un RDQM HA, che non è configurato per passare a un sito di ripristino di emergenza.

- Per visualizzare lo stato di un particolare gestore code su tutti i nodi nel gruppo HA, immettere il seguente comando:

```
rdqmstatus -m qmname
```

dove *qmname* è il nome dell'RDQM per cui si desidera visualizzare lo stato. Viene visualizzato lo stato di RDQM sul nodo corrente, seguito da un riepilogo dello stato degli altri due nodi dalla prospettiva del nodo corrente.

La seguente tabella riepiloga le informazioni sul nodo corrente che possono essere restituite dal comando **rdqmstatus** per un RDQM.

Tabella 36. Stato nodo corrente

Attributo Stato	**Valori possibili**	**Quando visualizzato**
Nome nodo	*NODENAME*	Sempre visualizzato
Stato gestore code	stato del gestore code (uno degli stati validi per il comando **dspmq**)	Sempre visualizzato
CPU	*n.nn*%	Visualizzato solo quando RDQM è in esecuzione su questo nodo
Memoria	*nnn*MB utilizzati	Visualizzato solo quando RDQM è in esecuzione su questo nodo
File system del gestore code	*nnn*MB utilizzati, *y.y*GB assegnati [*z*%]	Visualizzato solo quando RDQM è in esecuzione su questo nodo
Ruolo HA	Primario Secondario V 9.1.5 Secondario in sospeso Sconosciuto	Sempre visualizzato
Stato HA	Tutti i nodi in standby Questo nodo è in standby Nodi remoti in standby Misto	Tutti i nodi in standby Nodo corrente in standby Entrambi i nodi remoti in standby Stato differente per ogni nodo remoto
Controllo HA	Abilitato/a Disabilitato/a Sconosciuto	Sempre visualizzato. Mostra se RDQM è sotto il controllo Pacemaker

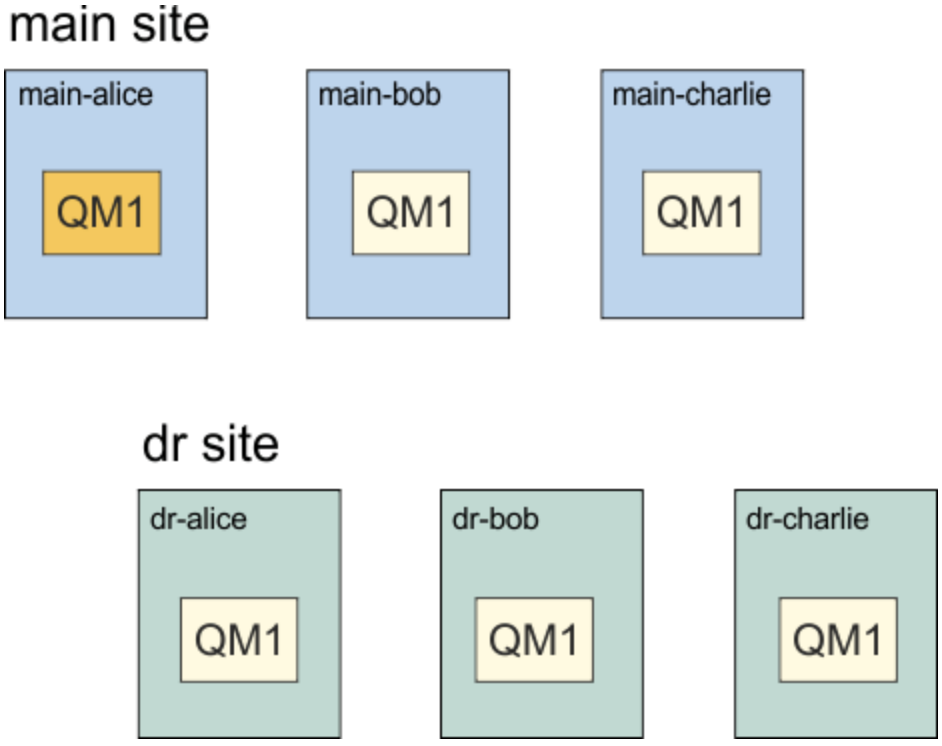
Tabella 36. Stato nodo corrente (Continua)

Attributo Stato	**Valori possibili**	**Quando visualizzato**
Ubicazione preferita HA	Nessuna Questo nodo Sconosciuto *NODENAME*	Sempre visualizzato
Interfaccia IP mobile HA	*nome_interfaccia*	Sempre visualizzato
Indirizzo IP mobile HA	*IPV4_address*	Sempre visualizzato
Ruolo DR	Primario Secondario Sconosciuto	Sempre visualizzato
Stato DR	Normale Sincronizzazione in corso Partizionato Sistema remoto non disponibile Non congruente Ripristino all'istantanea Sistema remoto non configurato Negoziazione non riuscita	Va tutto bene. Sincronizzazione in corso. L'utente ha avviato la coda su ciascun nodo mentre il La rete di replica DR era non disponibile. La connessione all'altro nodo è stato perso. Era in corso una sincronizzazione ma è stata interrotta. L'utente ha scelto di tornare a l'istantanea che è stata acquisita quando il gestore code ha immesso il Stato incongruente. Il primario è stato configurato Ma il secondario non l'ha fatto. La negoziazione iniziale tra i nodi primario e secondario non è riuscita. Ciò può essere causato da tipi di replica incompatibili o se il nodo secondario è configurato con una dimensione del file system inferiore.
Stato DR (su nodo secondario HA)	Consultare *HA_Primary_Node*	Visualizzato sui nodi secondari HA come stato DR è noto solo sul nodo primario HA.
Porta DR	La porta TCP/IP utilizzata per replicare i dati per questo gestore code.	Sempre visualizzato.
Indirizzo IP locale DR	L'indirizzo IP locale che verrà utilizzato da questo gestore code per la replica DR	Sempre visualizzato.
Elenco indirizzi IP remoti DR	Gli indirizzi IP remoti che questo gestore code utilizzerà per la replica DR. Un elenco separato da virgole di tre indirizzi IP.	Sempre visualizzato.

Tabella 36. Stato nodo corrente (Continua)		
Attributo Stato	**Valori possibili**	**Quando visualizzato**
Indirizzo IP remoto corrente DR	L'IP remoto corrente a cui è connesso questo gestore code per la replica DR.	Per un primario HA con una connessione DR attiva.
Indirizzo IP remoto corrente DR (su nodo secondario HA)	Consultare *HA_Primary_Node*	Visualizzato su un nodo secondario HA come la connessione DR è solo sul nodo primario HA
Dati DR non sincronizzati	*x*KB	Visualizzato quando il nodo remoto non è disponibile o è incongruente.
Avanzamento della sincronizzazione DR	*s*%	Visualizzato quando è in corso una sincronizzazione.
Tempo stimato DR per il completamento	*aaaa-mm-gg hh:mm:ss*	Visualizzato quando è in corso una sincronizzazione.
Avanzamento ripristino istantanea	*s*%	Visualizzato quando lo stato DR è "Ripristino istantanea"

Esempio

Questi esempi illustrano il comando **`rdqmstatus -m qm1`** eseguito su vari nodi della seguente configurazione DR/HA:



Esempio di stato normale su un nodo primario DR e primario HA:

```
Node:                                   main-alice
Queue manager status:                   Running
CPU:                                    0.00%
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
```

```
HA preferred location:                  This node
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.1.1
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           192.168.2.1

Node:                                   main-bob
HA status:                              Normal

Node:                                   main-charlie
HA status:                              Normal
```

Esempio di stato normale su un nodo che è il DR primario e un HA secondario:

```
Node:                                   main-bob
Queue manager status:                   Running elsewhere
HA role:                                Secondary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    main-alice
HA preferred location:                  main-alice
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              See main-alice
DR port:                                3000
DR local IP address:                    192.168.1.2
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           See main-alice

Node:                                   main-alice
HA status:                              Normal

Node:                                   main-charlie
HA status:                              Normal
```

Esempio di stato normale su un nodo che è il secondario DR e un primario HA:

```
Node:                                   dr-alice
Queue manager status:                   Ended immediately
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Secondary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.2.1
DR remote IP address list:              192.168.1.1,192.168.1.2,192.168.1.3
DR current remote IP address:           192.168.1.1

Node:                                   dr-bob
HA status:                              Normal

Node:                                   dr-charlie
HA status:                              Normal
```

Esempio di stato normale su un nodo che è il secondario DR e un secondario HA:

```
Node:                                   dr-bob
Queue manager status:                   Ended immediately
HA role:                                Secondary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    dr-alice
HA preferred location:                  dr-alice
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Secondary
DR status:                              See dr-alice
DR port:                                3000
```

```
DR local IP address:                    192.168.2.2
DR remote IP address list:              192.168.1.1,192.168.1.2,192.168.1.3
DR current remote IP address:           See dr-alice

Node:                                   dr-alice
HA status:                              Normal

Node:                                   dr-charlie
HA status:                              Normal
```

Esempio di sincronizzazione DR in corso su un nodo che è un primario DR e un primario HA:

```
Node:                                   main-alice
Queue manager status:                   Running
CPU:                                    0.00%
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.1.1
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           192.168.2.1
DR synchronization progress:            11.0%
DR estimated time to completion:        2018-09-06 14:55:05

Node:                                   main-bob
HA status:                              Normal

Node:                                   main-charlie
HA status:                              Normal
```

Esempio di DR partizionato su un nodo che è un DR primario e HA primario:

```
Node:                                   main-alice
Queue manager status:                   Running
CPU:                                    0.00%
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              Partitioned
DR port:                                3000
DR local IP address:                    192.168.1.1
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           192.168.2.1
DR out of sync data:                    372KB

Node:                                   main-bob
HA status:                              Normal

Node:                                   main-charlie
HA status:                              Normal
```

Riferimenti correlati

Linux rdqmstatus

Linux V 9.1.0 *Funzionamento in un ambiente DR/HA*

Quando si opera in un ambiente DR/HA ci sono considerazioni separate per l'alta disponibilità e il ripristino di emergenza.

Se il nodo su cui è in esecuzione un RDQM DR/HA ha esito negativo, l'RDQM esegue automaticamente il failover su un altro nodo in tale gruppo HA. Se l'intero sito ha esito negativo, è necessario avviare manualmente RDQM sul nodo preferito nel gruppo HA sul sito di ripristino. Le considerazioni qui riportate sono le stesse di un normale RDQM DR, consultare "Funzionamento in un ambiente di ripristino di emergenza" a pagina 572 per ulteriori informazioni.

Se uno dei nodi ha esito negativo completamente e deve essere sostituito, consultare "Sostituzione di un nodo malfunzionante in una configurazione di ripristino di emergenza" a pagina 574 e "Sostituzione di un nodo malfunzionante in una configurazione ad alta disponibilità" a pagina 555 per istruzioni.

V 9.1.5 Linux

Sostituzione di un nodo non riuscito in una configurazione DR/HA

Se uno dei nodi in uno dei tuoi gruppi HA ha esito negativo, puoi sostituirlo.

Informazioni su questa attività

La procedura varia a seconda se il nodo che si sta sostituendo è un nodo primario o un nodo secondario nella configurazione DR. In entrambi i casi, il nuovo nodo deve avere una configurazione identica al nodo che si sta sostituendo, ovvero, deve avere lo stesso nome host, gli stessi indirizzi IP e così via.

Si potrebbe anche incontrare la situazione in cui si è completamente perso il gruppo HA nel proprio sito principale o di ripristino e si deve sostituire l'intero gruppo HA.

Procedura

- Per un nodo di sostituzione primario nella configurazione DR, completare la seguente procedura sul nuovo nodo:
  a) Creare un file `rdqm.ini` che corrisponda ai file sugli altri nodi, quindi eseguire il comando `rdqmadm -c` (consultare "Definizione del cluster Pacemaker (gruppo HA)" a pagina 536).
  b) Eseguire il comando `crtmqm -sxs -rr p` *qmanager* per ricreare ogni DR/HA RDQM (consultare "Creazione di RDQM DR/HA" a pagina 579).
- Per un nodo di sostituzione secondario nella configurazione DR, completare la seguente procedura sul nuovo nodo:
  a) Creare un file `rdqm.ini` che corrisponda ai file sugli altri nodi, quindi eseguire il comando `rdqmadm -c` (consultare "Definizione del cluster Pacemaker (gruppo HA)" a pagina 536).
  b) Eseguire il comando `crtmqm -sx -rr s` *qmanager* per ricreare ciascun RDQM DR/HA (consultare "Creazione di RDQM DR/HA" a pagina 579).
- Per sostituire un intero gruppo HA, completare la seguente procedura:
  a) Se si perde l'intero gruppo HA sul sito primario DR (ovvero, il sito principale), è necessario seguire la procedura per eseguire un failover gestito sul sito secondario DR per continuare ad eseguire RDQM DR/HA (consultare "Funzionamento in un ambiente di ripristino di emergenza" a pagina 572). (Se si perde un intero gruppo HA nel sito di ripristino, i RDQM DR/HA continuano ad essere eseguiti nel sito principale senza l'intervento dell'utente.)
  b) Creare nuovamente il gruppo HA sui tre nodi di sostituzione, come descritto in "Configurazione di gruppi HA per RDQM DR/HA" a pagina 578.
  c) Ricreare le RDQM DR/HA sul nuovo gruppo HA come descritto in "Creazione di RDQM DR/HA" a pagina 579.
  d) Se necessario, eseguire un failover gestito dal sito di ripristino al sito principale.

V 9.1.5 Linux

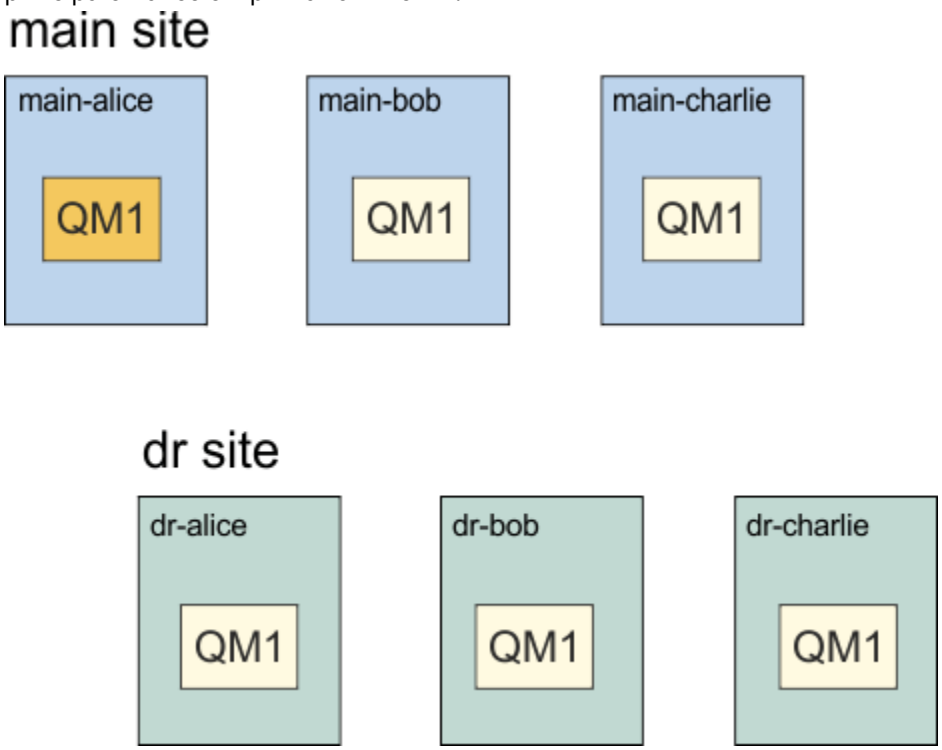
Esempio di lavoro DR/HA RDQM

Questo esempio mostra come creare ed eliminare DR/HA RDQM.

Creazione di un RDQM DR/HA

La configurazione di esempio ha due siti, denominati 'main' e 'dr '. Ogni sito ha tre nodi, denominati 'alice', 'bob' e 'charlie '. I nodi hanno un nome completo composto dal nome e dal nome del sito, quindi 'main-alice', 'dr-alice' e così via.

La seguente procedura crea un RDQM DR/HA denominato QM1 che viene eseguito su main - alice. Il nodo principale - alice è il primario HA e DR.



Se gli indirizzi IP DR locali e remoti sono specificati nel file `rdqm.ini` , non è necessario specificare alcun indirizzo IP sulla riga comandi e un RDQM DR/HA denominato QM1 può essere creato eseguendo il seguente comando su main - alice:

```
crtmqm -sx -rr p -rn DR1 -rp 7001 QM1
```

Se gli indirizzi IP DR locali sono specificati nel file `rdqm.ini` , gli indirizzi IP DR remoti possono essere specificati sulla riga comandi:

```
crtmqm -sx -rr p -ri 192.168.2.1,192.168.2.2,192.168.2.3 -rp 7001 QM1
```

Se non viene specificato alcun indirizzo IP DR nel file `rdqm.ini` , è possibile specificare sia gli indirizzi IP DR remoti che quelli locali sulla riga comandi:

```
crtmqm -sx -rr p -rl 192.168.1.1,192.168.1.2,192.168.1.3 -ri
192.168.2.1,192.168.2.2,192.168.2.3 -rp 7001 QM1
```

L'output in risposta alla creazione di QM1 è il seguente:

```
Creating replicated data queue manager configuration.
Secondary queue manager created on 'main-bob'.
Secondary queue manager created on 'main-charlie'.
IBM MQ queue manager created.
Directory '/var/mqm/vols/qm1/qmgr/qm1' created.
The queue manager is associated with installation 'Installation1'.
Creating or replacing default objects for queue manager 'QM1'.
Default objects statistics : 83 created. 0 replaced. 0 failed.
Completing setup.
Setup completed.
Enabling replicated data queue manager.
Replicated data queue manager enabled.
Issue the following command on the remote HA group to create the DR/HA secondary queue manager:
```

```
crtmqm -sx -rr s -rl 192.168.2.1,192.168.2.2,192.168.2.3 -ri
192.168.1.1,192.168.1.2,192.168.1.3 -rp 7001 -fs 3072M QM1
```

Copiare il comando dal messaggio per creare l'istanza secondaria DR di QM1 su dr-alice:

```
crtmqm -sx -rr s -rl 192.168.2.1,192.168.2.2,192.168.2.3 -ri
192.168.1.1,192.168.1.2,192.168.1.3 -rp 7001 -fs 3072M QM1
```

Il seguente messaggio viene emesso su dr-alice:

```
Creating replicated data queue manager configuration.
Secondary queue manager created on 'dr-bob'.
Secondary queue manager created on 'dr-charlie'.
IBM MQ secondary queue manager created.
Enabling replicated data queue manager.
```

Verifica il DR secondario

Per verificare le funzioni di ripristino di emergenza di QM1, eseguire il seguente comando su main - alice per rendere QM1 l'istanza secondaria DR:

```
rdqmdr -m QM1 -s
Queue manager 'QM1' has been made the DR secondary on this node.
```

Eseguire il seguente comando su dr-alice per rendere QM1 l'istanza primaria DR su tale nodo:

```
rdqmdr -m QM1 -p
Queue manager 'QM1' has been made the DR primary on this node.
```

Eliminazione di un RDQM DR/HA

Per eliminare il DR/HA RDQM denominato QM1, terminare prima il gestore code su main - alice:

```
endmqm -w QM1
Replicated data queue manager disabled.
Waiting for queue manager 'QM1' to end.
IBM MQ queue manager 'QM1' ended.
```

Quindi, eseguire il seguente comando su main - alice per eliminare QM1:

```
dltmqm QM1
Removing replicated data queue manager configuration.
Secondary queue manager deleted on 'main-bob'.
Secondary queue manager deleted on 'main-charlie'.
IBM MQ queue manager 'QM1' deleted.
```

Infine, è necessario eliminare QM1 su dr-alice:

```
dltmqm QM1
Removing replicated data queue manager configuration.
Secondary queue manager deleted on 'dr-bob'.
Secondary queue manager deleted on 'dr-charlie'.
IBM MQ queue manager 'QM1' deleted.
```

Concetti correlati

“Funzionamento in un ambiente DR/HA” a pagina 589
Quando si opera in un ambiente DR/HA ci sono considerazioni separate per l'alta disponibilità e il ripristino di emergenza.

Attività correlate

“Creazione di RDQM DR/HA” a pagina 579
Utilizzare il comando **crtmqm** per creare un gestore code di dati replicati (RDQM) in una configurazione DR/HA.

“Eliminazione di un RDQM DR/HA” a pagina 582

Utilizzare il comando **dltmqm** per eliminare un gestore code di dati replicati DR/HA (RDQM).

Registrazione: verifica che i messaggi non vengano persi

IBM MQ registra tutte le modifiche significative ai dati permanenti controllati dal gestore code in un log di ripristino.

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, IBM MQ si basa anche sul sistema disco che ospita i file, inclusi i file di log. Se il sistema disco è esso stesso inaffidabile, le informazioni, incluse le informazioni di log, possono ancora essere perse.

Avvertenza: Non è possibile spostare i log di ripristino su un sistema operativo differente.

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 IBM MQ è composto 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 diverse estensioni di log che contengono i dati registrati. È possibile definirne il numero e la dimensione (come spiegato in “Stanza LogDefaults del file mqs.ini” a pagina 93) oppure utilizzare il valore predefinito di sistema di tre estensioni primarie e due secondarie.

Ciascuna delle tre estensioni primaria e secondaria assume il valore predefinito di 16 MB.

Quando si crea un gestore code, il numero di estensioni log preassegnate è il numero di estensioni log *primarie* assegnate. Se non si specifica un numero, viene utilizzato il valore predefinito.

IBM MQ utilizza due tipi di registrazione:

- Circolare
- Lineare

  Il numero di estensioni di log utilizzate con la registrazione lineare può essere molto elevato, a seconda della frequenza della registrazione dell'immagine multimediale.

Per ulteriori informazioni, consultare “Tipi di registrazione” a pagina 594.

Windows In IBM MQ for Windows, se il percorso di log non è stato modificato, le estensioni di log vengono create nella directory:

```
C:\ProgramData\IBM\MQ\log\QMgrName
```

ULW Nei sistemi IBM MQ per UNIX and Linux , se il percorso di log non è stato modificato, le estensioni di log vengono create nella directory:

```
/var/mqm/log/QMgrName
```

IBM MQ inizia con queste estensioni di log primarie, ma se lo spazio di log primario non è sufficiente, alloca le estensioni di log *secondarie* . Lo fa dinamicamente e li rimuove quando la richiesta di spazio di log si riduce. Per impostazione predefinita, è possibile assegnare fino a due estensioni di log secondarie. È possibile modificare questa allocazione predefinita, come descritto in "Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms" a pagina 83.

Le estensioni log sono precedute dalla lettera S o dalla lettera R. Le estensioni attive, inattive e superflue hanno come prefisso S, mentre le estensioni di riutilizzo hanno come prefisso R.

Quando si esegue il backup o il ripristino del gestore code, eseguire il backup e il ripristino di tutte le estensioni attive, inattive e superflue, insieme al file di controllo log.

Nota: Non è necessario eseguire il backup e ripristinare le estensioni di riutilizzo.

Il file di controllo log

Il file di controllo di log contiene le informazioni necessarie per descrivere lo stato delle estensioni di log, come la dimensione e l'ubicazione e il nome della successiva estensione disponibile.

Importante: 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.

Il file di controllo log si trova nel percorso di log ed è denominato `amqhlctl.lfh`. Quando si esegue il backup o il ripristino del gestore code, assicurarsi che venga eseguito il backup e il ripristino del file di controllo log, insieme alle estensioni di log.

Tipi di registrazione

In IBM MQ sono disponibili due modalità di gestione dei record delle attività del gestore 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.

IBM 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 recupero 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 596.

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 conserva i dati di log in una sequenza continua di file di log.

I file di log possono essere:

- Riutilizzati, ma solo quando non sono più necessari per il ripristino del riavvio o del supporto.
- Archiviato manualmente per analisi e storage a lungo termine.

La frequenza delle immagini dei supporti determina quando i file di log lineari possono essere riutilizzati ed è un fattore importante nella quantità di spazio su disco che deve essere disponibile per i file di log lineari.

È possibile configurare il gestore code per eseguire automaticamente le immagini dei supporti periodici, in base all'ora o all'utilizzo del log, oppure è possibile pianificare manualmente le immagini dei supporti.

L'amministratore decide la politica da implementare e le implicazioni sull'utilizzo dello spazio su disco. I file di log necessari per il ripristino del riavvio devono essere sempre disponibili, mentre i file di log necessari solo per il ripristino del supporto possono essere archiviati in una memoria a più lungo termine, ad esempio nastro.

Se l'amministratore abilita la gestione automatica dei log e le immagini dei supporti automatici, la registrazione lineare si comporta in modo simile a un log circolare molto grande, ma con la ridondanza migliorata contro i malfunzionamenti dei supporti abilitata dal ripristino dei supporti.

V 9.1.0 Da IBM MQ 9.1.0 è possibile modificare un tipo di log esistente per un gestore code, da lineare a circolare o da circolare a lineare utilizzando il comando migmqlog .

Estensioni log lineari non attive

Multi V 9.1.0

Da IBM MQ 9.1.0, se si utilizza la gestione log automatica, inclusa l'archiviazione, il programma di registrazione tiene traccia delle estensioni log lineari non attive.

Attenzione: Se si sta utilizzando la gestione automatica dei log, senza archiviazione, l'utilizzo di un gestore code di backup non è supportato per questo processo.

ULW Quando un'estensione di log non è più richiesta per il recupero e, se necessario, viene archiviata, il programma di registrazione eliminerà l'estensione di log o la riutilizzerà.

Un'estensione di log riutilizzata viene ridenominata per essere la successiva nella sequenza di log. Viene scritto periodicamente il messaggio AMQ7490 , che indica quante estensioni sono state create, eliminate o riutilizzate.

Il programma di registrazione sceglie il numero di estensioni da mantenere pronte per il riutilizzo e quando eliminare tali estensioni.

Log attivo

Esistono diversi file che si dice siano *attivi* sia nella registrazione lineare che nella registrazione circolare. Il log attivo è la quantità massima di spazio di log, indipendentemente dal fatto che si stia utilizzando la registrazione circolare o lineare, a cui potrebbe fare riferimento il ripristino di riavvio.

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 599 per informazioni sulla definizione del numero.)

Si noti che lo spazio di log attivo non include lo spazio richiesto per il ripristino del supporto e che il numero di file di log utilizzati con la registrazione lineare può essere molto grande, a seconda del flusso di messaggi e della frequenza delle immagini del supporto.

Log inattivo

Quando un file di log non è più necessario per riavviare il ripristino, diventa *inattivo*. I file di log che non sono richiesti per riavviare il ripristino o il ripristino del supporto, possono essere considerati come file di log superflui.

Quando si utilizza la gestione log automatica, il gestore code controlla l'elaborazione di questi file di log superflui. Se è stata selezionata la gestione manuale del log, diventa responsabilità dell'amministratore gestire (ad esempio, eliminare e archiviare) i file di log superflui se non sono più di interesse per l'operazione.

Fare riferimento a “Gestione dei log” a pagina 605 per ulteriori informazioni sulla disposizione dei file di log.

File di log secondari

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 il numero di file secondari disponibili viene utilizzato, le richieste per la maggior parte delle ulteriori operazioni che richiedono l'attività di log verranno rifiutate con un codice di ritorno MQRC_RESOURCE_PROBLEM restituito all'applicazione e qualsiasi transazione di lunga durata verrà considerata per il rollback asincrono.

Attenzione: 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 gestori code di registrazione circolare e di registrazione lineare supportano il ripristino del riavvio. Indipendentemente da quanto bruscamente l'istanza precedente del gestore code viene terminata (ad esempio, un'interruzione dell'alimentazione) al riavvio, il gestore code ripristina il suo stato persistente allo stato transazionale corretto al momento della chiusura.

Il ripristino del riavvio dipende dal mantenimento dell'integrità del disco. Allo stesso modo, il sistema operativo deve garantire l'integrità del disco indipendentemente da quanto bruscamente potrebbe verificarsi la chiusura di un sistema operativo.

Nell'evento altamente insolito in cui l'integrità del disco non viene mantenuta, la registrazione lineare (e il ripristino dei supporti) fornisce ulteriori opzioni di ridondanza e recuperabilità. Con una tecnologia sempre più comune, come RAID, è sempre più raro soffrire di problemi di integrità del disco e molte aziende configurano la registrazione circolare e utilizzano solo il ripristino di riavvio.

IBM MQ è progettato come un classico gestore risorse Write Ahead Logging. Gli aggiornamenti persistenti alle code messaggi si verificano in due fasi:

1. I record di log che rappresentano l'aggiornamento vengono scritti in maniera affidabile nel log di ripristino
2. Il file o i buffer della coda vengono aggiornati in un modo che è il più efficiente per il sistema, ma non necessariamente coerente.

I file di log possono quindi diventare più aggiornati del buffer della coda sottostante e dello stato del file.

Se a questa situazione è stato consentito di continuare senza interruzione, è necessario un volume molto elevato di ripetizione del log per rendere congruente lo stato della coda in seguito a un ripristino da un arresto anomalo.

IBM MQ utilizza `checkpoints` per limitare il volume di ripetizione del log richiesto in seguito a un ripristino da un arresto anomalo. L'evento chiave che controlla se un file di log è definito attivo o meno è un `checkpoint`.

Un punto di controllo IBM MQ è un punto:

- Di congruenza tra il log di recupero e i file oggetto.
- Ciò identifica una posizione nel log, da cui è garantita la ripetizione di inoltro dei record di log successivi per ripristinare la coda allo stato logico corretto nel momento in cui il gestore code potrebbe essere terminato.

Durante un punto di controllo, IBM MQ elimina i vecchi aggiornamenti ai file delle code, come richiesto, per limitare il volume dei record di log che devono essere riprodotti per riportare le code ad uno stato congruente dopo un recupero da un arresto anomalo.

Il punto di controllo completo più recente contrassegna un punto nel log da cui deve essere eseguita la ripetizione durante il recupero da caduta. La frequenza del checkpoint è quindi un compromesso tra il sovraccarico dei checkpoint di registrazione e il miglioramento del tempo di recupero potenziale implicito da tali checkpoint.

La posizione nel log dell'inizio del punto di controllo completo più recente è uno dei fattori chiave per determinare se un file di log è attivo o inattivo. L'altro fattore chiave è la posizione nel log del primo record di log relativo al primo aggiornamento persistente effettuato da una transazione attiva corrente.

Se un nuovo punto di controllo viene registrato nel secondo file di log o in quello successivo e nessuna transazione corrente fa riferimento a un record di log nel primo file di log, il primo file di log diventa inattivo. Nel caso di registrazione circolare, il primo file di log è ora pronto per essere riutilizzato. In caso di registrazione lineare, il primo file di log sarà in genere ancora richiesto per il ripristino del supporto.

Se si configura la registrazione circolare o la gestione log automatica, il gestore code gestirà i file di log inattivi. Se si configura la registrazione lineare con la gestione manuale dei log, questa diventa un'attività amministrativa per gestire i file inattivi in base ai requisiti dell'operazione.

IBM MQ genera automaticamente i punti di controllo. Essi vengono presi nei seguenti orari:

- Quando il gestore code viene avviato
- Alla chiusura
- Quando lo spazio di registrazione è insufficiente
- Multi Dopo che sono state registrate 50.000 operazioni dal momento in cui è stato eseguito il punto di controllo precedente
- z/OS Dopo che *number_of_operations* è stato registrato da quando è stato eseguito il punto di controllo precedente, dove *number_of_operations* è il numero di operazioni impostato nella proprietà **LOGLOAD** .

Quando IBM MQ viene riavviato, trova l'ultimo record di checkpoint nel log. Queste informazioni vengono conservate nel file del punto di controllo aggiornato alla fine di ogni punto di controllo. 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.

Multi I messaggi AMQ7229 e AMQ7230 vengono emessi per indicare l'avanzamento della fase di riproduzione.

Per sapere quali operazioni eseguire il backout o il commit, IBM MQ accede a ciascun record di log attivo associato a una transazione incompleta. Questa è nota come fase di recupero.

Multi 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.

Multi Il messaggio AMQ7233 viene emesso per indicare l'avanzamento della fase di risoluzione.

z/OS Su z/OS, il riavvio dell'elaborazione è composto da varie fasi.

1. L'intervallo di registrazione per il recupero viene stabilito, in base al recupero del supporto richiesto per le serie di pagine e al record di registrazione meno recente richiesto per il ripristino delle unità di lavoro e per l'ottenimento dei blocchi per le unità di lavoro in dubbio.
2. Una volta determinato l'intervallo di log, la lettura del log in avanti viene eseguita per portare le serie di pagine allo stato più recente e anche per bloccare i messaggi relativi alle unità di lavoro in dubbio o in corso.
3. Quando la lettura del log di inoltro è stata completata, i log vengono letti all'indietro per eseguire il backout di tutte le unità di lavoro che erano in fase di elaborazione o in fase di backout al momento dell'errore.

z/OS Un esempio dei messaggi che potrebbero essere visualizzati:

```
CSQR001I +MQOX RESTART INITIATED
CSQR003I +MQOX RESTART - PRIOR CHECKPOINT RBA=00000001E48C0A5E
CSQR004I +MQOX RESTART - UR COUNTS -  806
IN COMMIT=0, INDOUBT=0, INFLIGHT=0, IN BACKOUT=0
CSQR030I +MQOX Forward recovery log range  815
from RBA=00000001E45FF7AD to RBA=00000001E48C1882
CSQR005I +MQOX RESTART - FORWARD RECOVERY COMPLETE -  816
IN COMMIT=0, INDOUBT=0
CSQR032I +MQOX Backward recovery log range  817
from RBA=00000001E48C1882 to RBA=00000001E48C1882
CSQR006I +MQOX RESTART - BACKWARD RECOVERY COMPLETE -  818
INFLIGHT=0, IN BACKOUT=0
CSQR002I +MQOX RESTART COMPLETED
```

Nota: Se c'è una grande quantità di log da leggere, i messaggi CSQR031I (recupero inoltro) e CSQR033I (recupero all'indietro) vengono emessi periodicamente per mostrare l'avanzamento.

In Figura 86 a pagina 598, tutti i record precedenti all'ultimo checkpoint, Checkpoint 2, non sono più necessari per IBM 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.

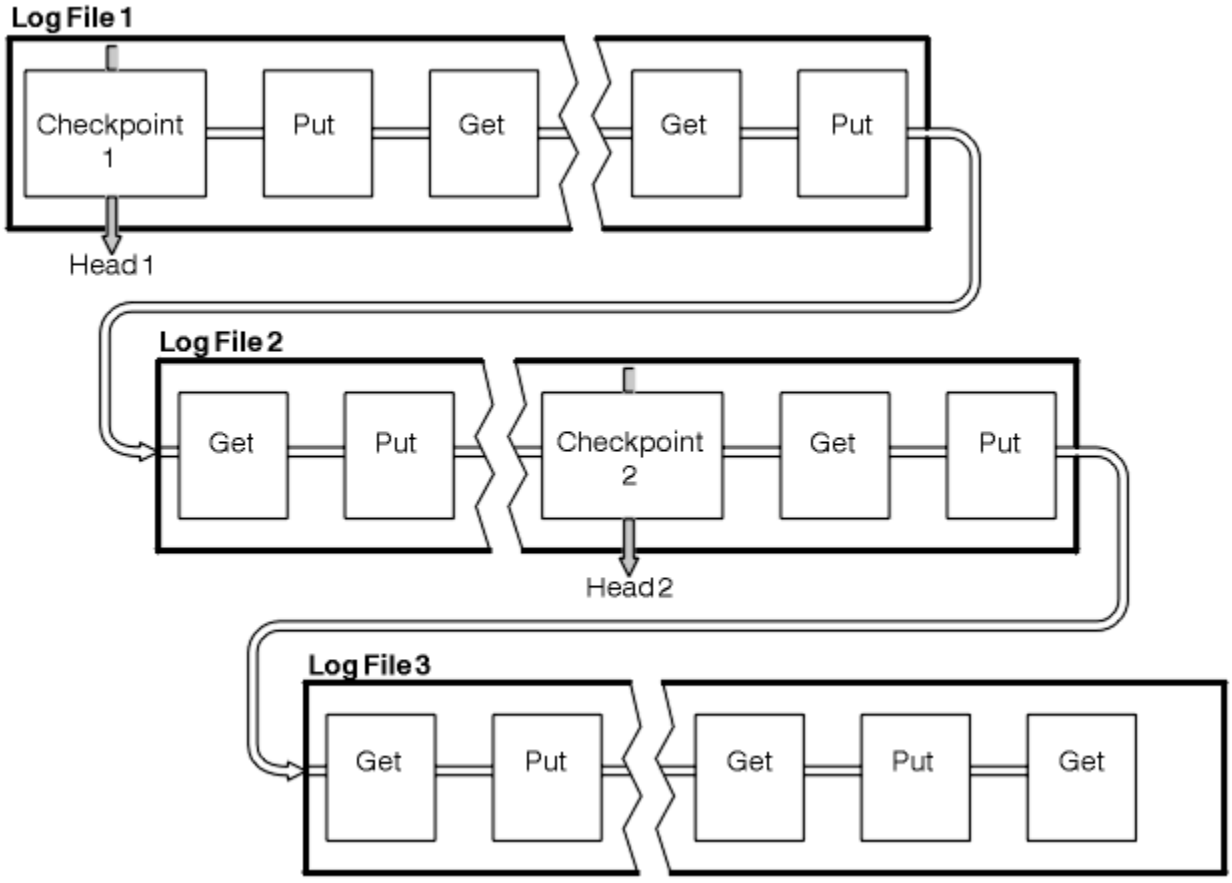


Figura 86. Checkpoint

Checkpoint con transazioni di lunga durata

Come una transazione di lunga durata influisce sul riutilizzo dei file di log.

Figura 87 a pagina 599 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, a LR 2, la parte principale del log si sposta logicamente al 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 potrebbero essere utilizzati per evitare che i log si riempiano.

Le attività che sono interamente sotto il controllo del gestore code, ad esempio il punto di controllo, sono pianificate per provare a mantenere l'attività nel log primario.

Tuttavia, quando è richiesto lo spazio di log secondario per supportare il comportamento al di fuori del controllo del gestore code (ad esempio, la durata di una delle transazioni), il gestore code tenta di utilizzare qualsiasi spazio di log secondario definito, per consentire il completamento di tale attività.

Se tale attività non viene completata entro il periodo di tempo in cui l'80% dello spazio di log totale è in uso, il gestore code avvia l'azione per recuperare spazio di log, indipendentemente dal fatto che ciò abbia un impatto sull'applicazione.

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.

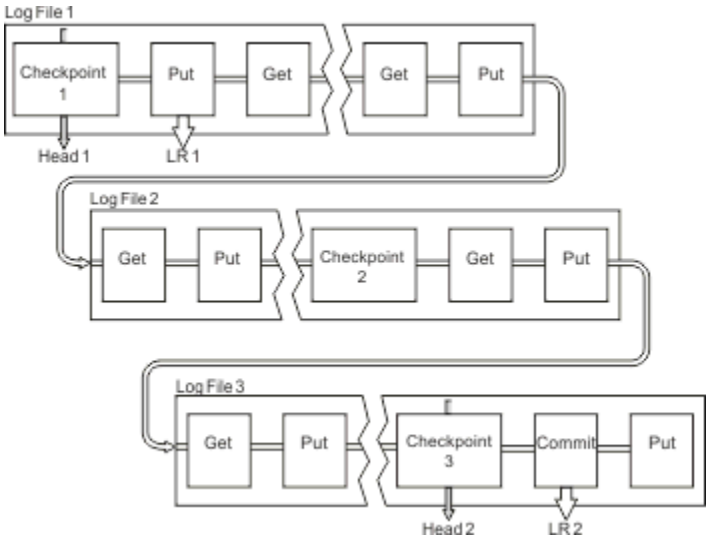


Figura 87. Checkpoint con una transazione di lunga durata

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 stimare la dimensione del Log attivo richiesto dal gestore code. La dimensione del log attivo 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 possono essere creati per l'utilizzo quando i file di log primari stanno diventando pieni

Note:

1. È possibile modificare il numero di file di log primari e secondari ogni volta che il gestore code viene avviato, anche se non è possibile notare immediatamente l'effetto della modifica apportata ai log secondari.
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 superare 511 su sistemi UNIX and Linux o 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 ripristino del riavvio. 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 lo spazio di log primario e secondario. 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.

   Consultare “Quanto deve essere grande il mio log attivo?” a pagina 600 per informazioni sul numero di log da assegnare. Le estensioni di log principali vengono utilizzate in sequenza e tale sequenza non cambia.

   Ad esempio, se hai tre log principali 0, 1e 2, l'ordine di utilizzo è 0,1,2 seguito da 1,2,0, 2,0,1, torna a 0,1,2 e così via. Tutti i log secondari assegnati vengono intervallati come richiesto.
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.

   V 9.1.0 Il gestore code tenta di pianificare i checkpoint in un modo che mantiene l'utilizzo del log all'interno delle estensioni primarie.

Per ulteriori informazioni, consultare “Stanza LogDefaults del file mqs.ini” a pagina 93.

Quanto deve essere grande il mio log attivo?

Stima della dimensione del log attivo necessaria per un gestore code.

La dimensione del log attivo è limitata da:

```
logsize = (primaryfiles + secondaryfiles) * logfilepages * 4096
```

Il log dovrebbe essere abbastanza grande da gestire la transazione in esecuzione da più tempo quando il gestore code scrive la quantità massima di dati al secondo sul disco.

Se la transazione in esecuzione da più tempo per N secondi e la quantità massima di dati al secondo scritti sul disco dal gestore code è di B byte al secondo nel log, il log deve essere almeno:

```
logsize >= 2 * (N+1) * B
```

È probabile che il gestore code stia scrivendo la quantità massima di dati al secondo sul disco quando si sta eseguendo il carico di lavoro di picco o quando si stanno registrando le immagini dei supporti.

Se una transazione viene eseguita per un periodo di tempo tale che l'estensione del log contenente il primo record di log non è contenuta nel log attivo, il gestore code esegue il rollback delle transazioni attive una alla volta, a partire dalla transazione con il record di log più vecchio.

Il gestore code deve rendere inattive le vecchie estensioni di log prima che venga utilizzato il numero massimo di file primari e secondari e il gestore code deve assegnare un'altra estensione di log.

Decidere per quanto tempo si desidera eseguire la transazione con esecuzione più lunga, prima che al gestore code sia consentito eseguire il rollback. La transazione con esecuzione più lunga potrebbe essere in attesa di un traffico di rete lento o, nel caso di una transazione mal progettata, in attesa di input dell'utente.

È possibile analizzare il tempo di esecuzione della transazione più lungo, immettendo il seguente comando **runmqsc** :

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

L'immissione del comando `dspmqtrn -a` mostra tutti i comandi XA e non XA in tutti gli stati.

L'immissione di questo comando elenca la data e l'ora in cui è stato scritto il primo record di log per tutte le transazioni correnti.

Attenzione: Ai fini del calcolo della dimensione del log, è l'ora in cui è stato scritto il primo record di log che conta, non l'ora in cui è stata avviata l'applicazione o la transazione. Arrotondare la lunghezza della transazione con esecuzione più lunga al secondo più vicino. Ciò è dovuto alle ottimizzazioni nel gestore code.

Il primo record di log può essere scritto molto tempo dopo l'avvio dell'applicazione, se l'applicazione inizia, ad esempio, con l'emissione di una chiamata MQGET che attende per un periodo di tempo prima di ricevere effettivamente un messaggio.

Esaminando l'output massimo di data e ora osservato dal

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

il comando immesso in origine, dalla data e ora correnti, è possibile stimare per quanto tempo viene eseguita la transazione in esecuzione più a lungo.

Assicurarsi di eseguire questo comando **runmqsc** ripetutamente mentre le transazioni con esecuzione più lunga sono in esecuzione nel carico di lavoro di picco in modo da non sottovalutare la lunghezza della transazione con esecuzione più lunga.

In IBM MQ 8.0 utilizzare gli strumenti del sistema operativo, ad esempio **iostat** su piattaforme UNIX .

Da IBM MQ 9.0, è possibile rilevare i byte al secondo che il gestore code sta scrivendo nel log immettendo il seguente comando:

```
amqsrua -m qmgr -c DISK -t Log
```

I byte logici scritti, mostrano i byte al secondo scritti dal gestore code nel log. Ad esempio:

```
$ amqsrua -m mark -c DISK -t Log
Publication received PutDate:20160920 PutTime:15383157 Interval:4 minutes,39.579 seconds
Log - bytes in use 37748736
Log - bytes max 50331648
Log file system - bytes in use 316243968
Log file system - bytes max 5368709120
Log - physical bytes written 4334030848 15501948/sec
Log - logical bytes written 3567624710 12760669/sec
Log - write latency 411 uSec
```

In questo esempio, i byte logici al secondo scritti nel log sono 12760669/sec o circa 12 MiB al secondo.

Utilizzo di

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

ha mostrato che la transazione con esecuzione più lunga era:

```
CONN(57E14F6820700069)
```

```
EXTCONN(414D51436D61726B2020202020202020)
TYPE(CONN)
APPLTAG(msginteg_r)                     UOWLOGDA(2016-09-20)
UOWLOGTI(16.44.14)
```

Poiché la data e l'ora correnti erano 2016-09-20 16.44.19, questa transazione era in esecuzione da 5 secondi. Tuttavia, è necessario tollerare le transazioni in esecuzione per 10 secondi prima che il gestore code esegua il rollback. Quindi la dimensione del log dovrebbe essere:

```
2 * (10 + 1) * 12 = 264 MiB
```

.

Il numero di file di log deve essere in grado di contenere la dimensione di log massima prevista (calcolata nel testo precedente). Questo sarà:

Numero minimo di file di log = (dimensione log richiesta) / (**LogFilePages** * dimensione pagina file di log (4096))

Utilizzando il valore predefinito **LogFilePages**, che è 4096, e la stima della dimensione del log di 264MiB, calcolata nel testo precedente, il numero minimo di file di log dovrebbe essere:

```
264MiB / (4096 x 4096) = 16.5
```

cioè 17 file di log.

Se si dimensiona il log in modo che il carico di lavoro previsto venga eseguito all'interno dei file primari:

- I file secondari forniscono una certa contingenza nel caso in cui sia necessario ulteriore spazio di log.
- La registrazione circolare utilizza sempre i file primari preassegnati, che è marginalmente più veloce dell'allocazione e della deallocazione dei file secondari.
- Il gestore code utilizza solo lo spazio rimanente nei file primari per calcolare quando eseguire il successivo checkpoint.

Pertanto, nell'esempio precedente, impostare i seguenti valori in modo che il workload venga eseguito all'interno dei file di log primari:

- **LogFilePages** = 4096
- **LogPrimaryFiles** = 17
- **LogSecondaryFiles** = 5

Tieni presente quanto segue:

- In questo esempio, 5 secondario è più del 20% dello spazio di log attivo.

  V 9.1.0 Da IBM MQ 9.1.0, il programma di registrazione tenta di mantenere il carico di lavoro solo nei file primari. Di conseguenza, il programma di registrazione pianifica i punti di controllo quando una frazione dei soli file primari è piena.

  V 9.1.0 Avere i file secondari è una contingenza, nel caso in cui ci siano transazioni di esecuzione inaspettatamente lunga.

  Tenere presente che il gestore code esegue un'azione per ridurre l'utilizzo dello spazio di log quando più dell ' 80% dello spazio di log totale è in uso.
- Eseguire lo stesso calcolo se si utilizza la registrazione lineare o circolare.

  Non fa alcuna differenza se si sta calcolando la dimensione di un log attivo lineare o circolare, poiché il concetto di log attivo significa lo stesso sia nella registrazione lineare che nella registrazione circolare.
- Le estensioni di log necessarie solo per il ripristino del supporto non si trovano all'interno del log attivo e pertanto non vengono conteggiate nel numero dei file primari e secondari.
- V 9.1.0 Da IBM MQ 9.1.0 il campo *LOGUTIL* di DISPLAY QMSTATUS LOG è disponibile per aiutarti a calcolare, approssimativamente, la dimensione del log attivo richiesto.

Questo campo è progettato per consentire all'utente di effettuare una stima ragionevole della dimensione del log richiesta senza eseguire costantemente il campionamento per determinare la durata delle transazioni più lunghe in esecuzione o la velocità di trasmissione massima del gestore code.

Quanto dovrei rendere grandi le mie pagine LogFile?

Generalmente, rendere le pagine LogFilesufficientemente grandi in modo da poter aumentare facilmente la dimensione del log attivo senza raggiungere il numero massimo di file primari. Alcuni file di log di grandi dimensioni sono preferibili a molti file di log di piccole dimensioni poiché alcuni file di log di grandi dimensioni consentono una maggiore flessibilità per aumentare la dimensione del log, se necessario.

Per la registrazione lineare, file di log molto grandi potrebbero rendere la variabile delle prestazioni. Con file di log molto grandi c'è un passo più grande per creare e formattare un nuovo file di log, o per archiviarne uno vecchio. Questo è più di un problema con la gestione dei log di archivio e manuale perché con la gestione dei log automatica i nuovi file di log vengono creati raramente.

Cosa succede se il mio log è troppo piccolo?

Punti da considerare quando si stima la dimensione minima del log.

Se si rende il log troppo piccolo:

- Le transazioni di lunga durata verranno ripristinate.
- Il punto di controllo successivo deve essere avviato prima della fine del punto di controllo precedente.

Importante: Non importa quanto sia imprecisa la stima della dimensione del log, l'integrità dei dati viene mantenuta.

Consultare “Utilizzo del punto di controllo per garantire il ripristino completo” a pagina 596 per una spiegazione dei punti di controllo. Se la quantità di spazio di log rimasta nelle estensioni di log attive sta diventando breve, il gestore code pianifica i punti di controllo più frequentemente.

Un punto di controllo richiede una certa quantità di tempo; non è istantaneo. Più dati devono essere registrati nel punto di controllo, più tempo impiega il punto di controllo. Se il log è un piccolo punto di controllo può sovrapporsi, il che significa che il punto di controllo successivo è richiesto prima che il punto di controllo precedente sia terminato. Se ciò si verifica, vengono scritti dei messaggi di errore.

Se viene eseguito il backout delle transazioni di lunga durata o i punti di controllo si sovrappongono, il gestore code continua l'elaborazione del carico di lavoro. Le transazioni di breve durata continuano ad essere eseguite normalmente.

Tuttavia, il gestore code non è in esecuzione in modo ottimale e le prestazioni potrebbero essere ridotte. È necessario riavviare il gestore code con spazio di log sufficiente.

Cosa succede se il mio log è troppo grande?

Punti da considerare quando si stima la dimensione massima del log.

Se il log è troppo grande:

- È possibile aumentare il tempo impiegato per un riavvio di emergenza, anche se ciò è improbabile.
- Si sta utilizzando spazio su disco non necessario.
- Le transazioni a esecuzione molto lunga sono tollerate.

Importante: Non importa quanto sia imprecisa la stima della dimensione del log, l'integrità dei dati viene mantenuta.

V 9.1.0 Per facilitare la stima della dimensione massima del log, è possibile utilizzare le statistiche di utilizzo del log. Per ulteriori informazioni, consultare “Decidere come impostare IMGLOGLN e IMGINTVL” a pagina 609 e ALTER QMGR.

Consultare “Utilizzo del punto di controllo per garantire il ripristino completo” a pagina 596 per una descrizione del modo in cui il gestore code legge il log al riavvio. Il gestore code riproduce il log dall'ultimo punto di controllo, quindi risolve tutte le transazioni che erano attive al termine del gestore code.

Per risolvere una transazione, il gestore code legge nuovamente tutti i record di log associati a tale transazione. Questi record di log potrebbero essere precedenti all'ultimo punto di controllo.

Assegnando al gestore code un log molto grande, si fornisce al gestore code l'autorizzazione a leggere ogni record di log al riavvio, anche se di solito il gestore code non deve eseguire questa operazione. Potenzialmente, nell'improbabile eventualità che ciò accada, tale processo potrebbe richiedere molto tempo.

Se il checkpoint è stato inaspettatamente arrestato prima della chiusura del gestore code, ciò aumenta notevolmente il tempo di riavvio per un gestore code con un log di grandi dimensioni. La limitazione della dimensione del log limita il tempo di riavvio di emergenza.

Per evitare questi problemi è necessario assicurarsi che:

- Il tuo carico di lavoro può adattarsi comodamente in un log che non è eccessivamente grande.
- Si evitano transazioni di lunga durata.

V 9.1.0 *Quanto deve essere grande il file system del log?*

Stima della dimensione del file system di log necessaria per un gestore code.

È importante che il file system del log sia sufficientemente grande, in modo che il gestore code disponga di spazio sufficiente per scrivere il log. Se il gestore code riempie completamente il filesystem di log, scriverà FFDC, eseguirà il rollback delle transazioni e potrebbe terminare improvvisamente il gestore code.

La quantità di spazio su disco riservata per il log deve essere almeno pari a quella del log attivo. Esattamente quanto più grande dipende da:

- La scelta del tipo di log (lineare o circolare)
- La dimensione del log attivo (file primari, file secondari, pagine del file di log)
- La scelta della gestione dei log (manuale, automatica o di archivio)
- I tuoi piani di emergenza nel caso di un oggetto danneggiato.

Se si sceglie un log circolare, il file system di log deve essere

```
LogFilesystemSize >= (PrimaryFiles + SecondaryFiles + 1) * LogFileSize
```

Ciò consente al gestore code di scrivere in tutti i file primari e secondari. In circostanze eccezionali, il gestore code potrebbe scrivere un'estensione aggiuntiva oltre il numero di secondari. L'algoritmo precedente ne tiene conto.

Se si sceglie un log lineare, il file system del log deve essere significativamente più grande del log attivo.

Se si sceglie la gestione manuale dei log, il gestore code continua a scrivere su nuove estensioni di log quando ne ha bisogno ed è responsabilità dell'utente eliminarle (e archiviarle) quando non sono più necessarie.

Quanto più grande deve essere il file system di log dipende in gran parte dalla strategia di eliminazione delle estensioni superflue o inattive.

È possibile decidere di archiviare ed eliminare le estensioni non appena diventano inattive (non necessarie per riavviare il ripristino) oppure è possibile decidere di archiviare ed eliminare solo le estensioni superflue (non necessarie per il supporto o riavviare il ripristino).

Se si stanno archiviando ed eliminando solo estensioni superflue, e se si dispone di un oggetto danneggiato, **MEDIALOG** non si sposterà in avanti, quindi nessun' altra estensione diventerà superflua. Si arresterà l'archiviazione e l'eliminazione delle estensioni fino a quando non si risolve il problema, forse ripristinando l'oggetto.

A meno che non si arresta il carico di lavoro, il tempo necessario per risolvere il problema dipende dalla dimensione del filesystem di log. Pertanto, è consigliabile avere un filesystem di log generoso quando si utilizza la registrazione lineare.

Se si sceglie un log lineare e la gestione dei log di archivio o automatica, il gestore code riutilizza le estensioni di log.

Le estensioni di log disponibili per essere riutilizzate hanno come prefisso la lettera R. Quando un'immagine del supporto viene registrata, poiché sono archiviate estensioni superflue, il gestore code può quindi riutilizzare tali estensioni.

Quindi, le estensioni di riutilizzo sono inferiori alla lunghezza dei dati scritti nel log tra le immagini del supporto:

```
ReuseExtents <= LogDataLengthBetweenMediaImages
```

Quando si registrano automaticamente le immagini del supporto magnetico e si imposta **IMGLOGLN**, `LogDataLengthBetweenMediaImages` può essere due volte **IMGLOGLN** perché **IMGLOGLN** non è un valore massimo fisso.

Quando si registrano manualmente le immagini del supporto o si registrano automaticamente per intervallo, `LogDataLengthBetweenMediaImages` dipende dal carico di lavoro e dall'intervallo tra le immagini.

Oltre alle estensioni attive e alle estensioni di riutilizzo, ci sono estensioni inattive (necessarie solo per il recupero dei supporti) e superflue (non necessarie per il riavvio o il ripristino dei supporti).

Quando si utilizza la gestione dei log di archivio o automatica, il gestore code non riutilizza le estensioni necessarie per il ripristino del supporto. Quindi, il numero di estensioni inattive dipende dalla frequenza con cui si stanno prendendo le immagini multimediali e se si stanno prendendo manualmente o automaticamente.

IMGINTVL e **IMGLOGLN** sono destinazioni, non un minimo o un massimo fisso tra le immagini del supporto. Tuttavia, quando si stima la dimensione massima del file system di log potrebbe essere necessario, è improbabile che le immagini di supporto automatiche vengano registrate più di due volte **IMGINTVL** o **IMGLOGLN** a parte.

Quando si ridimensiona il file system di log utilizzando la gestione automatica o di log di archivio, è necessario considerare anche cosa potrebbe accadere se una coda o un altro oggetto è danneggiato. In tal caso, il gestore code non è in grado di eseguire un'immagine del supporto dell'oggetto danneggiato e **MEDIALOG** non procederà.

Se il carico di lavoro continua, il log inattivo crescerà in modo illimitato poiché l'estensione più vecchia necessaria per il ripristino del supporto è ancora necessaria e non può essere riutilizzata. Se il carico di lavoro continua, si avrà fino a quando il file system del log non si riempie completamente per risolvere il problema, prima che il gestore code inizi a eseguire il rollback delle transazioni e potrebbe anche terminare bruscamente.

Quindi, per la gestione dei log di archiviazione e automatica:

```
LogFilesystemSize > (PrimaryFiles + SecondaryFiles +
(((TimeBetweenMediaImages *2) + TimeNeededToResolveDamagedObject) * ExtentsUsedPerHour))
* LogFilePages
```

Nota: L'algoritmo precedente presuppone che **SET LOG ARCHIVED** venga richiamato per ogni estensione, non appena non è più necessario per il ripristino del supporto, per la gestione del log di archiviazione.

Gestione dei log

V 9.1.0 Da IBM MQ 9.1.0, IBM MQ supporta la gestione automatica dei log e il ripristino automatico dei supporti dei log lineari. I log circolari sono quasi autogestiti, ma a volte necessitano di un intervento per risolvere i problemi di spazio.

Nota: IBM i La gestione dei log di archiviazione e automatica non sono validi su IBM i.

Nella 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 la quantità di spazio su disco utilizzato ridurla, perché lo spazio allocato viene rapidamente riutilizzato.

V 9.1.0 Da IBM MQ 9.1.0 è possibile eliminare i file secondari quando si utilizza la registrazione circolare. Per ulteriori informazioni, consultare RESET QMGR **TYPE(REDUCELOG)** .

Nella registrazione lineare, 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.

Multi Se il log si riempie, viene emesso il messaggio AMQ7463 . Inoltre, se il log si riempie poiché una transazione di lunga durata ha impedito il rilascio dello spazio, viene emesso il messaggio AMQ7465 .

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.

Nel tempo, i record di log meno recenti scritti non sono più necessari per riavviare il gestore code.

Quando viene rilevata una transazione di lunga durata, l'attività viene pianificata per eseguire il rollback asincrono di tale transazione. Se, per qualche motivo imprevisto, il rollback asincrono ha avuto esito negativo, alcune chiamate MQI restituiscono MQRC_RESOURCE_PROBLEM in tale situazione.

Si noti che 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.

Un'applicazione per cui è stato eseguito il rollback di una transazione 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 utilizza troppo spazio di log, lo spazio di log viene rilasciato e il gestore code continua a funzionare normalmente.

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 che contiene il log si riempie, il gestore code emette il messaggio AMQ6709 e viene eseguito un record di errore.

I file di log vengono creati alla loro dimensione fissa, piuttosto che essere estesi quando i record di log vengono scritti in essi. Ciò significa che IBM MQ può esaurire lo spazio su disco solo quando sta creando un nuovo file; non può esaurire lo spazio quando scrive un record nel log. IBM MQ sa sempre quanto spazio è disponibile nei file di log esistenti e gestisce di conseguenza lo spazio all'interno dei file.

V 9.1.0 Da IBM MQ 9.1.0, quando si utilizza la registrazione lineare, è possibile utilizzare:

- Gestione automatica delle estensioni di log.

  Consultare DISPLAY QMSTATUS per ulteriori informazioni sui nuovi attributi di log.

  Inoltre, consultare i seguenti comandi o i relativi equivalenti PCF:

  - Gestore code RESET
  - SET LOG per piattaforme distribuite
- Le opzioni che controllano l'utilizzo delle immagini multimediali.

  Consultare il comando ALTER QMGR e ALTER QUEUES per ulteriori informazioni su:

  - IMGINTVL
  - IMGLOGLN
  - IMGRCOVO
  - COCOVIMG
  - IMGSCHED

La registrazione circolare restituisce un problema di risorse.

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 richiede che tutte le estensioni 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.

Informazioni specifiche per la registrazione circolare

Se si utilizza la registrazione circolare, verificare che vi sia spazio sufficiente per conservare i file di log durante la configurazione del sistema (consultare “Stanza LogDefaults del file mqs.ini” a pagina 93 e “Stanza di log del file qm.ini” a pagina 125). 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.

Informazioni specifiche per la registrazione lineare

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. I seguenti metodi determinano quali file di log sono ancora richiesti:

Messaggi di evento del programma di registrazione
Quando si verifica un evento significativo, ad esempio un'immagine del supporto di registrazione, vengono generati messaggi di evento del programma di registrazione. 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 Amministrazione tramite comandi MQSCe per informazioni sui comandi PCF, consultare Automazione delle attività di amministrazione.

Messaggi del gestore code
Periodicamente, il gestore code emette una coppia di messaggi per indicare quali file di log sono necessari:

- Il messaggio AMQ7467I 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 AMQ7468I fornisce il nome del file di log più vecchio necessario per il ripristino del supporto.

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.

Informazioni applicabili a entrambi i tipi di registrazione

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.

Se non è possibile trovare alcun file di log necessario, viene emesso il messaggio dell'operatore AMQ6767E . Rendere il file di log e tutti i file di log successivi disponibili per il gestore code e ritentare l'operazione.

Ripulitura automatica delle aree di log - solo registrazione lineare

Multi V 9.1.0

Da IBM MQ 9.1.0 è possibile utilizzare la gestione automatica delle estensioni di log lineari non più richieste per il recupero.

Si utilizza l'attributo **LogManagement** nella stanza Log del file qm.ini o utilizzando IBM MQ Explorer, per impostare la gestione automatica. Per ulteriori informazioni, consulta "Stanza di log del file qm.ini" a pagina 125.

Consultare il parametro LOG di **DISPLAY QMSTATUS** per ulteriori dettagli sull'operazione del log e i seguenti comandi per l'utilizzo del log:

- Gestore code RESET
- Impostazione log

Acquisizione automatica delle immagini multimediali - solo registrazione lineare

V 9.1.0

Da IBM MQ 9.1.0 c'è uno switch generale per controllare se il gestore code scrive automaticamente le immagini dei supporti, il valore predefinito è che lo switch non è stato impostato.

È possibile controllare se si verifica l'imaging del supporto automatico e la frequenza del processo, utilizzando i seguenti attributi del gestore code:

IMGSCHED
Indica se il gestore code scrive automaticamente le immagini dei supporti

IMGINTVL
Frequenza per la scrittura di immagini multimediali, in minuti

IMGLOGLN
Megabyte di log scritti dalla precedente immagine del supporto di un oggetto.

Se si ha un momento critico durante il giorno quando il carico di lavoro è molto pesante e si desidera essere sicuri che la velocità di trasmissione del sistema non sia influenzata dall'utilizzo di immagini di supporto automatiche, è possibile disattivare temporaneamente l'imaging del supporto automatico impostando **IMGSCHED***(MANUAL)*.

È possibile commutare **IMGSCHED** in qualsiasi momento durante il carico di lavoro.

Attenzione: MEDIALOG non verrà spostato in avanti se non si stanno utilizzando le immagini del supporto, quindi è necessario archiviare le estensioni o assicurarsi di disporre di spazio su disco sufficiente.

È inoltre possibile controllare le immagini dei supporti automatici e manuali per altri oggetti definiti dall'utente:

- Informazioni di autenticazione
- Canale
- Connessione client
- Listener
- Elenco nomi
- Processo

- Coda alias
- Coda locale
- Servizio
- Argomento

Per gli oggetti di sistema interni, ad esempio il catalogo oggetti e l'oggetto del gestore code, il gestore code scrive automaticamente le immagini dei supporti in base alle esigenze.

Consultare ALTER QMGR per ulteriori informazioni sugli attributi.

È inoltre possibile abilitare o disabilitare le immagini dei supporti automatici e manuali solo per le code dinamiche locali e permanenti. A tale scopo, utilizzare l'attributo coda **IMGRCOVQ** .

Consultare ALTER QUEUES per ulteriori informazioni sull'attributo **IMGRCOVQ** .

Note:

1. Le immagini dei supporti sono supportate solo se si utilizza la registrazione lineare. Se sono state abilitate le immagini di supporto automatiche, ma si sta utilizzando la registrazione circolare, viene emesso un messaggio di errore e l'attributo delle immagini di supporto automatico del gestore code è disabilitato.
2. Se sono state abilitate immagini di supporti automatici, ma non è stata specificata una frequenza, minuti o megabyte di log, viene emesso un messaggio di errore e non viene scritta alcuna immagine di supporti automatici.
3. È possibile registrare manualmente un'immagine di supporto utilizzando rcdmqimg una volta impostato **IMGSCHED***(AUTO)*, se lo si desidera.

   Ciò consente di prendere immagini multimediali in un momento adatto per la propria azienda, ad esempio, quando il sistema è silenzioso. L'imaging del supporto automatico tiene conto di queste immagini del supporto manuale, poiché l'utilizzo di un'immagine del supporto manuale reimposta l'intervallo e la lunghezza del log, prima di cui viene presa la successiva immagine del supporto automatico.
4. Da IBM MQ 9.1.0, il gestore code scrive i messaggi persistenti solo nelle immagini del supporto, non nei messaggi non persistenti. Ciò può ridurre la dimensione delle immagini dei supporti durante la migrazione a IBM MQ 9.1.0 o versioni successive

Decidere come impostare IMGLOGLN e IMGINTVL

V 9.1.0

Rendere **IMGLOGLN** e **IMGINTVL** abbastanza grandi, in modo che il gestore code spende solo una frazione del tempo di registrazione delle immagini dei supporti, ma abbastanza piccoli in modo che:

- Gli oggetti danneggiati possono essere recuperati in un periodo di tempo ragionevole e
- Abbastanza piccolo in modo che il tuo log si adatti al tuo disco senza esaurire lo spazio.

Se si imposta **IMGLOGLN**, si consiglia di rendere **IMGLOGLN** molte volte la quantità di dati nelle code e molte volte la velocità dei dati del carico di lavoro. Maggiore è il valore di **IMGLOGLN**, minore è il tempo impiegato dal gestore code per la registrazione delle immagini dei supporti.

Allo stesso modo, se si imposta **IMGINTVL**, si consiglia di rendere **IMGINTVL** molte volte il tempo impiegato dal gestore code per registrare un'immagine del supporto. Puoi scoprire quanto tempo ci vuole per registrare un'immagine multimediale registrandone una manualmente.

Se si rendono **IMGLOGLN** e **IMGINTVL** troppo grandi, il recupero di un oggetto danneggiato potrebbe richiedere molto tempo, poiché tutte le estensioni dall'ultima immagine del supporto devono essere riprodotte.

Rendere **IMGLOGLN** e **IMGINTVL** sufficientemente piccoli, in modo che il tempo massimo impiegato per ripristinare un oggetto danneggiato sia accettabile.

Rendendo **IMGLOGLN** e **IMGINTVL** molto grandi, significa che il log cresce molto perché le immagini dei supporti vengono registrate raramente.

Attenzione: Assicurarsi che un log di questa dimensione si adatti comodamente al file system di log, poiché il carico di lavoro verrà ripristinato se il file system di log si riempie completamente.

È possibile impostare sia **IMGINTVL** che **IMGLOGLN**. Ciò può essere utile per garantire che le immagini dei supporti automatici vengano prese regolarmente durante un carico di lavoro pesante (controllato da **IMGLOGLN**), ma vengono ancora prese occasionalmente quando il carico di lavoro è molto leggero (controllato da **IMGINTVL**).

IMGINTVL e **IMGLOGLN** sono destinazioni per l'intervallo e la lunghezza dei dati di log tra cui vengono prese le immagini dei supporti automatici.

Questi attributi non devono essere considerati come un valore massimo o minimo fisso. Infatti, il gestore code potrebbe decidere di pianificare un'immagine del supporto automatico prima, se il gestore code percepisce che si tratta di un buon momento:

- Poiché la coda è vuota, prendere l'immagine del supporto è il più efficiente in termini di prestazioni e
- Un'immagine del supporto non è stata registrata per un certo periodo di tempo

A volte, il divario tra le immagini dei supporti automatici potrebbe essere un po' più lungo di **IMGINTVL** e **IMGLOGLN**, o di entrambi.

Il divario tra le immagini del supporto potrebbe essere maggiore di **IMGLOGLN** se la quantità di dati nelle code si sta avvicinando a **IMGLOGLN**. Il divario tra le immagini del supporto potrebbe essere maggiore di **IMGINTVL** se la registrazione di un'immagine del supporto richiede quasi il tempo **IMGINTVL** .

Questa non è una buona pratica perché il gestore code impiega la maggior parte del tempo a registrare immagini multimediali.

Quando si utilizza la registrazione automatica dell'immagine del supporto, il gestore code registra un'immagine del supporto per ogni oggetto e coda singolarmente, quindi il gestore code tiene traccia dell'intervallo e della lunghezza del log tra le immagini separatamente per ogni oggetto.

Gradualmente nel tempo, la registrazione di immagini multimediali diventa sfalsata, invece di registrare immagini multimediali per tutti gli oggetti allo stesso tempo. Questa sbalorditiva propaga l'impatto sulle prestazioni della registrazione delle immagini multimediali ed è un ulteriore vantaggio dell'utilizzo della registrazione automatica delle immagini multimediali rispetto alla registrazione manuale.

Acquisizione manuale di immagini multimediali - solo registrazione lineare

La registrazione di un'immagine di supporto di una coda implica la scrittura di tutti i messaggi persistenti da tale coda nel log. Per le code contenenti grandi volumi di dati di messaggi, ciò implica la scrittura di una grande quantità di dati nel log e questo processo può influire sulle prestazioni del sistema mentre sta accadendo.

È probabile che la registrazione delle immagini dei supporti di altri oggetti sia relativamente rapida, poiché l'immagine dei supporti di altri oggetti non contiene dati utente.

È necessario considerare attentamente quando registrare le immagini dei supporti delle code, in modo che il processo non interferisca con il carico di lavoro di picco.

È necessario registrare regolarmente l'immagine del supporto di tutti gli oggetti per aggiornare l'estensione del log meno recente necessaria per il ripristino del supporto.

Un buon momento per registrare l'immagine del supporto di una coda è quando è vuota, perché a quel punto non viene scritto alcun dato di messaggio nel log. Al contrario, un momento negativo è quando la coda è molto profonda o ha messaggi molto grandi su di essa.

Un buon momento per registrare l'immagine del supporto di una coda è quando il sistema è silenzioso; mentre un momento non corretto è durante il carico di lavoro di picco. Se il carico di lavoro è sempre

silenzioso a mezzanotte, ad esempio, è possibile decidere di registrare le immagini multimediali a mezzanotte ogni notte.

Sfalsare la registrazione di ciascuna delle code può diffondere l'impatto sulle prestazioni e quindi ridurne l'effetto. Più tempo è stato dall'ultima registrazione delle immagini multimediali, più diventa importante registrarle, man mano che aumenta il numero di estensioni di log richieste per il ripristino dei supporti.

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.

Ad esempio, per ottenere un'immagine di supporto di tutti i tuoi oggetti nel tuo gestore code, esegui il comando **rcdmqimg** come mostrato nei seguenti esempi:

Windows **SUWindows**

```
rcdmqimg -m QMNAME -t all *
```

Linux UNIX **SUUNIX 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 618. **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.

La registrazione manuale delle immagini dei supporti con **rcdmqimg** per gestire lo spazio di log non è richiesta, se si è scelto di utilizzare la registrazione lineare con l'imaging dei supporti automatico controllato dal gestore code.

Nota: I messaggi AMQ7467 e AMQ7468 possono essere emessi anche quando si esegue il comando `rcdmqimg` .

Immagini di supporti parziali

V 9.1.0

Si consiglia di utilizzare i messaggi IBM MQ solo per i dati che si prevede vengano utilizzati nel prossimo futuro, in modo che ogni messaggio si trovi in una coda per un periodo di tempo relativamente breve.

Al contrario, non è consigliabile utilizzare i messaggi IBM MQ per memorizzare i dati a lungo termine come un database.

È anche buona norma assicurarsi che le code siano relativamente basse e che non sia buona pratica avere code profonde i cui messaggi sono stati in coda per un lungo periodo di tempo.

Seguendo queste linee guida, si abilita il gestore code per ottimizzare le prestazioni della registrazione automatica delle immagini multimediali.

La registrazione dell'immagine del supporto di una coda vuota è molto efficiente (dal punto di vista delle prestazioni), mentre prendere l'immagine del supporto di una coda con una grande quantità di dati su di essa è molto inefficiente, perché tutti questi dati devono essere scritti nel log nell'immagine del supporto.

Per le code poco profonde con messaggi immessi di recente su di esso, il gestore code può effettuare un'ulteriore ottimizzazione.

Se tutti i messaggi attualmente presenti nella coda sono stati inseriti nel passato recente, il gestore code potrebbe essere in grado di registrare l'immagine del supporto per un determinato periodo di tempo (*punto di recupero*) prima dell'inserimento di tutti i messaggi e quindi di registrare l'immagine della coda vuota. Questo processo è molto basso in termini di prestazioni.

Se tutti i messaggi che si trovavano nella coda al punto di ripristino sono stati successivamente ricevuti, non è necessario registrare tali messaggi nell'immagine del supporto, poiché non si trovano più nella coda.

Questa viene definita *immagine di supporto parziale*. Quindi, nel caso improbabile in cui la coda debba essere ripristinata, tutti i record di log relativi a questa coda dall'ultima immagine del supporto verranno riprodotti, in modo da ripristinare tutti i messaggi immessi di recente.

Anche se ci fossero alcuni messaggi nella coda al punto di ripristino, che sono attualmente nella coda (e quindi devono essere registrati nell'immagine del supporto parziale), è ancora più efficiente registrare questa immagine del supporto parziale più piccola, piuttosto che un'immagine del supporto completo di tutti i messaggi.

Garantire che i messaggi rimangano in coda per un breve periodo di tempo potrebbe migliorare le prestazioni della registrazione automatica delle immagini multimediali.

Determinazione dei file di log superflui - solo registrazione lineare
Per la registrazione circolare, non eliminare mai i dati dalla directory di log. 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 più vecchio necessario, sono disponibili tre posti da utilizzare:

- Comando DISPLAY QMSTATUS
- Messaggi di evento del programma di registrazione e, infine
- Messaggi di log degli errori

Per il comando DISPLAY QMSTATUS, per stabilire l'estensione del log meno recente necessaria per:

- Riavviare il gestore code, immettere il comando `DISPLAY QMSTATUS RECLOG`.
- Eseguire il ripristino del supporto, immettere il comando `DISPLAY QMSTATUS MEDIALOG`.
- V 9.1.0 Determinare il nome per la notifica di archiviazione, immettere il comando `DISPLAY QMSTATUS ARCHLOG`.

V 9.1.0 È possibile ridurre il numero di estensioni di log secondarie quando si utilizza la registrazione circolare immettendo il comando **RESET QMGR TYPE(REDUCELOG)**.

In generale, un numero di file di log inferiore implica un log meno recente. A meno che non si abbia un turnover del 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.

Attenzione: Il file di log viene riportato a capo, quindi il numero successivo dopo 9 999 999 è zero.

Ubicazione file di log
Quando si sceglie un percorso per i propri file di log, tenere presente che l'operazione è gravemente compromessa se IBM 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.

È necessario posizionare i file di log su un'unità disco separata dai dati del gestore code.

L'integrità dei dati su questo dispositivo è fondamentale - dovresti consentire la ridondanza integrata.

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, si potrebbe essere costretti a tornare all'ultimo backup del proprio sistema IBM MQ .

V 9.1.3 *Coldstart: Cosa fare se le estensioni di log sono mancanti o corrotte*

Se l'azienda perde alcune o tutte le estensioni di log necessarie per riavviare il ripristino, il gestore code non sarà in grado di riprodurre il log di recupero e quindi non sarà in grado di riavviarlo. Se si richiede il riavvio del gestore code quando il log di ripristino è danneggiato in qualsiasi modo, a discapito del mantenimento dell'integrità dei dati, è possibile farlo, anche se fortemente sconsigliato. Questo processo è noto come *avvio a freddo* di un gestore code.

Importante: L'avvio a freddo di un gestore code deve essere considerato solo in circostanze eccezionali e comporta rischi di integrità dei dati come descritto in questa pagina. IBMsuggerisce di ricreare un gestore code, preferendo l'avvio a freddo, in risposta a file di dati danneggiati.

Se è richiesto un avvio a freddo per motivi operativi, contattare il rappresentante del supporto IBM per esaminare la causa principale del problema. È necessario sostituire un gestore code avviato a freddo con un gestore code ricostruito quanto prima.

Gli effetti di coldstart

Su coldstart, il gestore code crea un log di recupero vuoto e si basa sui dati presenti nei file di coda e in altri file di oggetto nello stato esistente. Poiché i dati nei file della coda possono essere incongruenti, i messaggi potrebbero essere persi, duplicati, danneggiati o incongruenti.

Il gestore code memorizza la configurazione di tutti gli altri oggetti persistenti nel log di ripristino e nei file di oggetti. Anche altri dati di stato interni vengono registrati nel log di ripristino, quindi su coldstart, i dati di stato interni vengono reimpostati e tutti gli altri dati di configurazione potrebbero non essere accurati.

Gli effetti di coldstart sono imprevedibili e di ampia portata, quindi si dovrebbe evitare un coldstart a meno che non sia assolutamente necessario. Dopo l'avvio a freddo, le informazioni nei file della coda e dell'oggetto possono essere così incongruenti che il gestore code non verrà riavviato.

Se il gestore code non viene riavviato, non esiste un modo semplice per rilevare i dati del messaggio o la configurazione su cui è possibile fare affidamento e gli elementi che non è possibile utilizzare. Inoltre, dopo un avvio a freddo, le code potrebbero essere danneggiate e quindi diventare completamente inutilizzabili.

Inoltre, se è possibile ottenere da, o inserire in, una particolare coda, i messaggi su di essa potrebbero essere danneggiati, mancanti o duplicati. Le transazioni e i canali potrebbero essere bloccati in dubbio. Anche se il coldstart del gestore code viene eseguito correttamente e le code sembrano intatte, gli effetti imprevedibili del coldstart potrebbero non essere realizzati fino a molto tempo dopo.

Cosa fare se è necessario eseguire il coldstart

L'esecuzione di un avvio a freddo non deve essere considerata una pratica operativa standard e IBM sconsiglia vivamente di eseguire questa operazione. Tuttavia, se si è in una posizione in cui è assolutamente necessario avviare a freddo un gestore code, contattare Supporto IBM MQ .

Il processo di avvio a freddo di un gestore code era molto più complicato per un gestore code lineare rispetto a un gestore code circolare. In IBM MQ 9.1.3, il processo coldstart è stato molto semplificato e non implica più la copia o la ridenominazione delle estensioni di log.

Da IBM MQ 9.1.3, contatta il supporto IBM , che ti fornirà una chiave che passi al comando **strmqm** per avviare a freddo un gestore code.

Attenzione: Il comando IBM MQ 9.1.3 coldstart comporta ancora gli stessi rischi di perdita dell'integrità dei dati di un coldstart manuale e IBM sconsiglia vivamente di eseguire questa operazione.

Eliminare le future partenze a freddo: una richiesta

Il comando strmqm richiede una chiave per eseguire il comando coldstart, poiché IBM MQ desidera che l'utente contatti il supporto IBM MQ se è necessario eseguire il comando coldstart, poiché IBM MQ è interessato a comprendere come si è arrivati a questa situazione.

Chiaramente coldstart è qualcosa che è meglio evitare. IBM MQ ha compiuto notevoli sforzi per assicurarsi che non sia necessario eseguire il coldstart del proprio gestore code e IBM desidera scoprire se il prodotto può fare di più per ridurre il coldstart.

Precauzioni per evitare un avvio a freddo

Il metodo di registrazione predefinito quando si crea un gestore code è la registrazione circolare. Con la registrazione circolare si consente al gestore code un numero particolare di estensioni di log primario e secondario di una determinata dimensione. Creare il file system di log abbastanza grande da contenere tutte le estensioni di log primario e secondario e non è mai necessario gestirle.

In alternativa, è possibile utilizzare la registrazione lineare rispetto a quella circolare. La registrazione lineare consente di recuperare code e altri oggetti, nell'improbabile caso in cui vengano danneggiati. Ma per impostazione predefinita, la registrazione lineare richiede di eliminare le estensioni di log che non sono più necessarie per il riavvio o il recupero del supporto. Si fa riferimento a questo come alla gestione del log manuale.

Quando si gestiscono le estensioni di log in questo modo, è possibile eliminare inavvertitamente troppe estensioni di log e quindi finire per dover eseguire il comando coldstart. Per ridurre questo rischio, utilizzare la gestione log automatica, in modo che il gestore code gestisca le estensioni log per conto dell'utente.

La procedura ottimale consiste nell'inserire il log di ripristino in un file system di log separato che contiene solo il log di ripristino. Se si inserisce il log di ripristino nello stesso filesystem del resto del gestore code, è possibile che il filesystem si riempia accidentalmente, forse a causa di file di coda di grandi dimensioni. Rendere la directory di log per il gestore code un file system separato oppure specificare un file system di log differente utilizzando l'opzione della riga comandi **-ld** nel comando **crtmqm** .

Se il filesystem che contiene i file della coda si riempie, potrebbe non essere possibile inserire tali code, ma il gestore code continua l'esecuzione. Se il file system che contiene il log di ripristino si riempie, il gestore code termina bruscamente e non si riavvierà fino a quando non si libera spazio.

Fare attenzione a non eliminare le estensioni di log necessarie per riavviare il ripristino, altrimenti potrebbe essere necessario eseguire il comando coldstart. A volte si potrebbe scoprire che è necessario eseguire il coldstart perché il disco non è riuscito che contiene il relativo log di ripristino. La procedura ottimale è quella di inserire il log di ripristino su un disco replicato e quindi ridurre il rischio di un arresto anomalo del disco.

Lo spostamento dei messaggi e della configurazione in un nuovo gestore code di sostituzione evita la possibilità di problemi in corso con un gestore code che è stato precedentemente avviato a freddo.

Tenere presente quali gestori code sono stati precedentemente avviati a freddo, anche se sono stati avviati a freddo molto tempo fa e sono stati arrestati, riavviati e migrati nel frattempo. Quando si contatta il supporto IBM , indicare se il gestore code è stato precedentemente avviato a freddo e, in tal caso, fornire quante più informazioni possibili su ciò che ha causato il requisito di un avvio a freddo.

Utilizzo del log per il ripristino

Puoi utilizzare le informazioni dai log per aiutarti a recuperare da errori.

Esistono diversi modi in cui i dati possono essere danneggiati. IBM MQ ti aiuta a recuperare 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

IBM MQ può eseguire il ripristino da errori di comunicazioni e perdita di alimentazione. A volte può anche recuperare da altri tipi di problemi, come l'eliminazione involontaria di un file.

In caso di errore di comunicazione, i messaggi persistenti rimangono nelle code 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 IBM MQ ripristina le code allo stato di cui è stato eseguito il commit al momento dell'errore. Ciò garantisce che nessun messaggio persistente venga perso. I messaggi non persistenti vengono eliminati; non sopravvivono quando IBM MQ si arresta bruscamente.

Recupero degli oggetti danneggiati

Esistono modi in cui un oggetto IBM 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

V 9.1.0 Da IBM MQ 9.1.0, su un gestore code di registrazione lineare, è possibile registrare le immagini dei supporti solo per gli oggetti che sono recuperabili. Ad esempio, è necessario considerare le opzioni **IMGRCOVO** e **IMGRCOVQ** .

V 9.1.0 Allo stesso modo, è possibile recuperare solo un sottoinsieme di oggetti, definiti come supporti recuperabili, da immagini di supporti su un gestore code di registrazione lineare. Nel caso in cui un oggetto, che non è definito come un supporto ripristinabile, sia danneggiato, le opzioni per tale oggetto sono le stesse di quelle per un gestore code di registrazione circolare.

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 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 MQ .

V 9.1.0 Il gestore code registra automaticamente le immagini dei supporti se è impostato **IMGSCHED***(AUTO)* . Per ulteriori informazioni, consultare ALTER QMGR per informazioni su **IMGINTVL** e **INGLOGLN**.

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 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 MQ viene danneggiato, le uniche azioni valide che possono essere eseguite 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.

Quali file oggetto esistono

V 9.1.0

Il gestore code memorizza gli attributi degli oggetti definiti in **runmqsc** in file su disco. Questi file di oggetti si trovano nelle sottodirectory nella directory di dati del gestore code.

Linux UNIX Ad esempio, su piattaforme UNIX e Linux , i canali sono memorizzati in `/var/mqm/qmgrs/qmgr/channel`.

I dati in questi file oggetto sono l'immagine supporto degli oggetti. Se questi file oggetto vengono eliminati o danneggiati, l'oggetto memorizzato in quel file è danneggiato. Utilizzando un gestore code di registrazione lineare, gli oggetti danneggiati possono essere recuperati dal log utilizzando il comando rcrmqobj .

La maggior parte dei file oggetto contiene solo gli attributi dell'oggetto, quindi i file canale contengono gli attributi dei canali. Le eccezioni sono:

- Catalogo

  Il catalogo di oggetti cataloga tutti gli oggetti di tutti i tipi ed è memorizzato in `qmanager/QMQMOBJCAT`.
- File di sincronizzazione

  Il file di sincronizzazione contiene dati di stato interni associati a tutti i canali.
- Code

  I file di coda contengono sia i messaggi su quella coda che gli attributi di quella coda.

Notare che non vi è alcun oggetto di catalogo o syncfile esposto in **runmqsc** o IBM MQ Explorer.

Il catalogo e il gestore code possono essere registrati, ma non recuperati. Se questi oggetti vengono danneggiati, il gestore code termina preventivamente e questi oggetti vengono ripristinati automaticamente al riavvio.

Le sottoscrizioni non vengono elencate negli oggetti da registrare o ripristinare, poiché le sottoscrizioni durevoli vengono memorizzate su una coda di sistema. Per registrare o ripristinare sottoscrizioni durevoli, registrare o ripristinare SYSTEM.DURABLE.SUBSCRIBER.QUEUE .

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 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 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 ripristinarlo dall'immagine del supporto utilizzando il comando **rcrmqobj** (per ulteriori dettagli, consultare rcrmqobj).

V 9.1.0 Se una coda (o un altro oggetto) viene danneggiato, **MEDIALOG** non si sposterà in avanti. Questo perché **MEDIALOG** è l'estensione meno recente richiesta per il ripristino del supporto. Se il tuo carico di lavoro continua, **CURRLOG** continuerà ad andare avanti e quindi verranno scritte nuove estensioni. A seconda della tua configurazione (inclusa la tua impostazione **LogManagement**), questo potrebbe iniziare a riempire il tuo file system di log. Se il file system di log si riempie completamente, viene eseguito il rollback delle transazioni e il gestore code potrebbe terminare bruscamente. Quindi, quando una coda viene danneggiata, si potrebbe avere solo una quantità limitata di tempo per agire prima che il gestore code termini. La quantità di tempo a disposizione dipende dalla frequenza con cui il carico di lavoro sta causando la scrittura di nuove estensioni da parte del gestore code e dalla quantità di spazio libero disponibile nel file system del log.

V 9.1.0 Se si utilizza la gestione manuale del log, è possibile che si stiano archiviando estensioni non necessarie per il ripristino del riavvio e quindi eliminarle dal file system del log, anche se sono ancora necessarie per il recupero del supporto. Ciò è accettabile fino a quando è possibile ripristinarle dall'archivio quando necessario. Questa politica non determina il riempimento del file system di log quando una coda viene danneggiata e **MEDIALOG** smette di procedere. Tuttavia, se si archiviano ed eliminano solo le estensioni che non sono necessarie per il riavvio o il ripristino del supporto, il file system del log inizia a riempirsi se una coda viene danneggiata.

V 9.1.0 Se si utilizza la gestione dei log di archiviazione o automatica, il gestore code non riutilizzerà le estensioni ancora necessarie per il recupero del supporto, anche se è possibile che siano state archiviate e che abbiano inviato una notifica al gestore code utilizzando SET LOG ARCHIVED. Di conseguenza, se una coda viene danneggiata, il file system di log inizierà a riempirsi.

V 9.1.0 Se una coda viene danneggiata, verranno scritti gli FFDC OBJECT DAMAGED e **MEDIALOG** smetterà di procedere. L'oggetto danneggiato può essere identificato da FFDC o perché è l'oggetto con il più vecchio **MEDIALOG** quando si visualizza il suo stato in **runmqsc**.

V 9.1.0 Se il file system di log è pieno e si è preoccupati che il carico di lavoro venga ripristinato perché il file system di log sta diventando pieno, il ripristino dell'oggetto o la sospensione del carico di lavoro potrebbe impedire che ciò accada.

Protezione dei file di log IBM 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 MQ . Se un utente elimina inavvertitamente i file di log che un gestore code deve riavviare, IBM 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 MQ). Possono quindi danneggiare, forse a causa dell'inesperienza, un gestore code in esecuzione o inattivo in un modo rispetto al quale IBM 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 opzioni riportate di seguito 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, ricavato 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 avviare la formattazione dei record di log da una determinata estensione del file di log. In tal caso, dmpmqlog prevede di trovare 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 `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.
loginactive	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.
LogRecdLogRecd	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 IBM 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.

ChkPtLSN	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 corrispondere al MQGET corrispondente utilizzato per ottenere 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 da una rappresentazione del descrittore del messaggio (eyecatcher MD) e quindi i 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 finale *Put Message* .

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.
QPriorità	La priorità del messaggio richiamato dalla coda.

Avvia transazione
Indica l'inizio di una nuova transazione. Un TranType di MQI indica una transazione solo IBM 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.

Transazione di rollback
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:

Nome RM	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
Registra la creazione di un oggetto IBM MQ .

ObjName	Il nome dell'oggetto creato.
UserId	L'ID utente che esegue la creazione.

Elimina oggetto
Questo registra l'eliminazione di un oggetto IBM MQ .

ObjName	Il nome dell'oggetto che è stato eliminato.

Backup e ripristino dei dati del gestore code IBM MQ

È possibile proteggere i gestori code da possibili danneggiamenti causati da errori hardware eseguendo il backup dei gestori code e dei dati del gestore code, eseguendo solo il backup della configurazione del gestore code e utilizzando un gestore code di backup.

Informazioni su questa attività

Avvertenza: È necessario prestare molta attenzione se si sposta un gestore code su un sistema operativo diverso. Per ulteriori informazioni, consultare Spostamento di un gestore code su un sistema operativo diverso .

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.

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 è in grado di riavviarsi o di essere ripristinato dal log. Se si esegue il backup della configurazione del gestore code, è 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.

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 viene aggiornato regolarmente, il log del gestore code di backup può contenere i 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.

Procedura

- Per eseguire il backup e ripristinare i dati del gestore code, consultare:
  - “Backup dei dati del gestore code” a pagina 622.
  - “Ripristino dei dati del gestore code” a pagina 623.
- Per eseguire il backup e il ripristino della configurazione del gestore code, consultare:
  - “Backup della configurazione del gestore code” a pagina 624
  - “Ripristino della configurazione del gestore code” a pagina 625
- Per creare, aggiornare e avviare un gestore code di backup, consultare “Utilizzo di un gestore code di backup” a pagina 626.

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

Prima di avviare il backup del gestore code, verificare 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:

Procedura

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, consultare "Modifica delle informazioni di configurazione IBM MQ nei file .ini su Multiplatforms" a pagina 83.

   Nota: I nomi visualizzati nella directory vengono trasformati per garantire che siano compatibili con la piattaforma su cui si utilizza IBM MQ. Per ulteriori informazioni sulle trasformazioni dei nomi, consultare Informazioni sui nomi file di IBM MQ.
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 593, e i file di configurazione come descritto in "File di inizializzazione e di configurazione" a pagina 225. Alcune delle directory potrebbero essere vuote, ma sono necessarie tutte per ripristinare il backup in un secondo momento.

   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.
3. Conservare le proprietà dei file.

   Linux UNIX Per i sistemi IBM MQ for UNIX e Linux , è possibile eseguire questa operazione con il comando **tar** . (Se si dispone di code più grandi di 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 IBM WebSphere MQ 7.5 e versioni successive, assicurarsi di eseguire un backup del file `qm.ini` e delle voci del Registro di sistema. Le informazioni sul gestore code sono memorizzate nel file `qm.ini` e possono essere utilizzate per ripristinare una versione precedente di IBM MQ.

Attività correlate

Arresto di un gestore code

"Backup dei file di configurazione dopo la creazione di un gestore code" a pagina 14

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

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

Prima di iniziare il backup, verificare che il gestore code non sia in esecuzione.

Quando si ripristina un backup di un gestore code in un cluster, consultare "Ripristino di un gestore code cluster" a pagina 354 e Cluster: disponibilità, più istanze e ripristino di emergenza per ulteriori informazioni.

Nota: Quando si esegue l'aggiornamento a una versione successiva di IBM MQ, 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 IBM MQ.

Procedura

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.

   Accertarsi di disporre di un file di controllo log e dei file di log.

   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.
4. Aggiornare i file di informazioni di configurazione.

   Verificare che i IBM MQ e i file di configurazione del gestore code siano congruenti in modo che IBM MQ possa ricercare i dati ripristinati nelle ubicazioni corrette.
5. Controllare la struttura di directory risultante per assicurarsi di disporre di tutte le directory richieste.

   Per ulteriori informazioni sulle directory e le sottodirectory IBM MQ , consultare Directory structure on Windows systems e Directory content on UNIX and Linux systems.

Risultati

Se è stato eseguito il backup e il ripristino corretto dei dati, il gestore code verrà avviato.

Multi Backup della configurazione del gestore code

Il backup della configurazione del gestore code può essere utile per ricreare un gestore code dalle relative definizioni se la configurazione del gestore code e i dati di log vengono persi a causa dell'errore hardware e il gestore code non è in grado di riavviare o di essere ripristinato dal log.

Informazioni su questa attività

ULW Su UNIX, Linux, and Windows, puoi utilizzare il comando **dmpmqcfg** per eseguire il dump della configurazione di un gestore code IBM MQ .

IBM i In IBM i, è possibile utilizzare il comando Dump di MQ Configuration (**DMPMQMCFG**) per eseguire il dump degli oggetti di configurazione e delle autorizzazioni per un gestore code.

Procedura

1. Assicurarsi che il programma di gestione code sia in esecuzione.
2. A seconda della piattaforma, utilizzare uno dei comandi riportati di seguito per eseguire il back up della configurazione del gestore code:

   - ULW Su UNIX, Linux, and Windows: eseguire il comando Dump MQ Configuration, **dmpmqcfg**utilizzando l'opzione di formattazione predefinita (- f mqsc) MQSC e tutti gli attributi (-a), utilizzare il reindirizzamento dell'output standard per memorizzare le definizioni in un file. Ad esempio:

     ```
     dmpmqcfg -m MYQMGR -a > /mq/backups/MYQMGR.mqsc
     ```

- IBM i Su IBM i: eseguire il comando di configurazione Dump MQ (**DMPMQMCFG**) utilizzando l'opzione di formattazione predefinita OUTPUT (*MQSC) e EXPATTR (*ALL), utilizzare TOFILE e TOMBR per memorizzare le definizioni in un membro del file fisico. Ad esempio:

```
DMPMQMCFG MQMNAME(MYQMGR) OUTPUT(*MQSC) EXPATTR(*ALL) TOFILE(QMQMSAMP/QMQSC)
TOMBR(MYQMGRDEF)
```

Attività correlate

“Ripristino della configurazione del gestore code” a pagina 625
È possibile ripristinare la configurazione per un gestore code da un backup verificando prima che il gestore code sia in esecuzione e quindi eseguendo il comando appropriato per la propria piattaforma.

Riferimenti correlati

dmpmqcfg (configurazione gestore code dump)
Dump della configurazione di MQ (DMP MQMCFG)

Multi Ripristino della configurazione del gestore code

È possibile ripristinare la configurazione per un gestore code da un backup verificando prima che il gestore code sia in esecuzione e quindi eseguendo il comando appropriato per la propria piattaforma.

Informazioni su questa attività

ULW Su UNIX, Linux, and Windows, è possibile utilizzare il comando **runmqsc** per ripristinare la configurazione di un gestore code IBM MQ .

IBM i Su IBM i, è possibile utilizzare il comando **STRMQMMQSC** per ripristinare le autorizzazioni e gli oggetti di configurazione per un gestore code.

Procedura

1. Assicurarsi che il programma di gestione code sia in esecuzione.

   Tenere presente che, se i danni ai dati e ai log non sono recuperabili in altri modi, è possibile che il gestore code sia stato ricreato.
2. A seconda della piattaforma, utilizzare uno dei comandi seguenti per ripristinare la configurazione del gestore code:

   - ULW Su UNIX, Linux, and Windows, eseguire **runmqsc** rispetto al gestore code, utilizzare il reindirizzamento di immissione standard per ripristinare le definizioni da uno script generato dal comando Dump di MQ Configuration (**dmpmqcfg**) (consultare “Backup della configurazione del gestore code” a pagina 624). Ad esempio:

     ```
     runmqsc MYQMGR < /mq/backups/MYQMGR.mqsc
     ```

   - IBM i Su IBM i: eseguire **STRMQMMQSC** sul gestore code e utilizzare i parametri **SRCMBR** e **SRCFILE** per ripristinare le definizioni dal membro del file fisico generato dal comando Dump di configurazione MQ (**DMPMQMCFG**) (vedere “Backup della configurazione del gestore code” a pagina 624). Ad esempio:

     ```
     STRMQMMQSC MQMNAME(MYQMGR) SRCFILE(QMQMSAMP/QMQSC) SRCMBR(MYQMGR)
     ```

Attività correlate

“Backup della configurazione del gestore code” a pagina 624

Il backup della configurazione del gestore code può essere utile per ricreare un gestore code dalle relative definizioni se la configurazione del gestore code e i dati di log vengono persi a causa dell'errore hardware e il gestore code non è in grado di riavviare o di essere ripristinato dal log.

Riferimenti correlati

dmpmqcfg (configurazione gestore code dump)
runmqsc (esecuzione comandi MQSC)
Dump della configurazione di MQ (DMP MQMCFG)
Comandi di avvio IBM MQ (STRMQMMQSC)

Utilizzo di un gestore code di backup

Un gestore code esistente può avere un gestore code di backup dedicato per scopi di ripristino di emergenza.

Informazioni su questa attività

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. Il gestore code esistente non deve essere arrestato per i file di log da copiare, tuttavia è necessario copiare un file di log solo se il gestore code ha terminato la scrittura su di esso; consultare “Aggiornamento di un gestore code di backup” a pagina 627 per informazioni su come assicurarsi che uno specifico file di log non venga più scritto, in modo che possa essere copiato in modo sicuro.

Nota: 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.

Importante: Una volta che il vecchio gestore code di backup è diventato il nuovo gestore code attivo, per qualsiasi motivo, non esiste più un gestore code di backup. Si tratta effettivamente di una forma di replica asincrona, per cui si prevede che il nuovo gestore code attivo sia logicamente in ritardo rispetto al vecchio gestore code attivo. Pertanto, il vecchio gestore code attivo non funge più da backup per il nuovo gestore code attivo.

Procedura

- Per informazioni sull'utilizzo di un gestore code di backup, consultare i seguenti argomenti:
  - “Creazione di un gestore code di backup” a pagina 626
  - “Aggiornamento di un gestore code di backup” a pagina 627
  - “Avvio di un gestore code di backup” a pagina 628

Concetti correlati

“Registrazione: verifica che i messaggi non vengano persi” a pagina 593
IBM MQ registra tutte le modifiche significative ai dati permanenti controllati dal gestore code in un log di ripristino.

Creazione di un gestore code di backup

Creare un gestore code di backup come una copia inattiva del gestore code esistente.

Informazioni su questa attività

Importante: È possibile utilizzare un gestore code di backup solo quando si utilizza la registrazione lineare.

Un 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.

Procedura

1. Creare un gestore code di backup per il gestore code esistente utilizzando il comando di controllo **crtmqm**.
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 622.
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 comando di controllo **strmqm** sul gestore code di backup come mostrato nel seguente esempio:

   ```
   strmqm -r BackupQMName
   ```

   Questo comando contrassegna il gestore code come gestore code di backup all'interno di IBM MQe riproduce tutte le estensioni di log copiate per portare il gestore code di backup al passo con il gestore code esistente.

Riferimenti correlati

crtmqm (crea gestore code)
strmqm (avvio gestore code)

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.

Informazioni su questa attività

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 prima di eseguire il backup.

Avvertenza: Se si copia una serie di log non contigui nella directory di log del gestore code di backup, vengono riprodotti solo i log fino al punto in cui viene trovato il primo log mancante.

Procedura

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 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 (ma non incluso) all'estensione corrente indicata in “2” a pagina 627. Copiare solo i file di estensione log, quelli che iniziano con "S. ..".
4. Eseguire il comando di controllo **strmqm** sul gestore code di backup come mostrato nel seguente esempio:

   ```
   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.

Riferimenti correlati
RESET QMGR
VISUALIZZAZIONE QMSTATUS
strmqm (avvio gestore code)

Avvio di un gestore code di backup

È possibile sostituire un gestore code di backup con un gestore code non recuperabile.

Informazioni su questa attività

Quando si ripristina un backup di un gestore code in un cluster, consultare “Ripristino di un gestore code cluster” a pagina 354 e Cluster: disponibilità, più istanze e ripristino di emergenza per ulteriori informazioni.

Se un gestore code non recuperabile ha un gestore code di backup dedicato, è possibile attivare il gestore code di backup al posto del gestore code non recuperabile.

Quando un gestore code non recuperabile viene sostituito con un gestore code di backup, è possibile che alcuni dei 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.

Nota: Anche se i file di log e i dati del gestore code si trovano in directory differenti, assicurarsi di 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. Anche se inizia, è probabile che i tuoi dati siano corrotti.

Procedura

1. Eseguire il comando di controllo **strmqm** per attivare il gestore code di backup come mostrato nel seguente esempio:

   ```
   strmqm -a BackupQMName
   ```

   Il gestore code di backup è attivato. Ora che è attivo, il gestore code di backup non può più essere aggiornato.
2. Eseguire il comando di controllo **strmqm** per avviare il gestore code di backup come mostrato nel seguente esempio:

   ```
   strmqm BackupQMName
   ```

   IBM MQ considera questo come un ripristino di riavvio e utilizza il log dal gestore code di backup. Durante l'ultimo aggiornamento al gestore code di backup, si verificherà la ripetizione, pertanto verrà eseguito il rollback solo delle transazioni attive dall'ultimo punto di controllo registrato.
3. Riavviare tutti i canali.
4. Controllare la struttura di directory risultante per assicurarsi di disporre di tutte le directory richieste.

Per ulteriori informazioni sulle directory e le sottodirectory IBM MQ , consultare Pianificazione del supporto del file system.

5. Accertarsi di disporre di un file di controllo log e dei file di log. Verificare inoltre che IBM MQ e i file di configurazione del gestore code siano congruenti in modo che IBM MQ possa ricercare i dati ripristinati nelle posizioni corrette.

Risultati

Se il backup e il ripristino dei dati sono stati eseguiti correttamente, il gestore code viene avviato.

Attività correlate

“Riavvio dei canali arrestati” a pagina 217

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

Riferimenti correlati

strmqm (avvio gestore code)

Modifiche al ripristino da errori cluster (su server diversi da z/OS)

Da IBM WebSphere MQ 7.1 in poi, il gestore code riesegue le operazioni che hanno causato problemi, fino a quando i problemi non vengono risolti. Se, dopo cinque giorni, i problemi non vengono risolti, il gestore code si arresta per evitare che la cache diventi più obsoleta.

Prima di IBM WebSphere MQ 7.1, se un gestore code ha rilevato un problema con il gestore del repository locale che gestisce un cluster, ha aggiornato il log degli errori. In alcuni casi, ha quindi interrotto la gestione dei cluster. Il gestore code ha continuato a scambiare i messaggi delle applicazioni con un cluster, basandosi sulla sua cache sempre più obsoleta di definizioni di cluster. Da IBM WebSphere MQ 7.1 in poi, il gestore code riesegue le operazioni che hanno causato problemi, fino a quando i problemi non vengono risolti. Se, dopo cinque giorni, i problemi non vengono risolti, il gestore code si arresta per evitare che la cache diventi più obsoleta. Man mano che la cache diventa più obsoleta, causa un numero maggiore di problemi. Il comportamento modificato relativo agli errori cluster in 7.1 o versioni successive non si applica a z/OS.

Ogni aspetto della gestione del cluster viene gestito per un gestore code dal processo del gestore repository locale, `amqrrmfa`. Il processo viene eseguito su tutti i gestori code, anche se non sono presenti definizioni cluster.

Prima di IBM WebSphere MQ 7.1, se il gestore code rilevava un problema nel gestore repository locale, arrestava il gestore repository dopo un breve intervallo. Il gestore code ha continuato l'esecuzione, elaborando i messaggi dell'applicazione e le richieste per aprire le code e pubblicare o sottoscrivere gli argomenti.

Con il gestore repository arrestato, la cache delle definizioni di cluster disponibili per il gestore code è diventata più obsoleta. Nel tempo, i messaggi sono stati instradati verso la destinazione non corretta e le applicazioni non sono riuscite. Le applicazioni non sono riuscite ad aprire le code del cluster o gli argomenti di pubblicazione che non erano stati propagati al gestore code locale.

A meno che un amministratore non abbia controllato i messaggi del repository nel log degli errori, potrebbe non rendersi conto che la configurazione del cluster aveva dei problemi. Se l'errore non è stato riconosciuto per un periodo di tempo ancora più lungo e il gestore code non ha rinnovato l'appartenenza al cluster, si sono verificati ulteriori problemi. L'instabilità ha influito su tutti i gestori code nel cluster e il cluster sembrava instabile.

Da IBM WebSphere MQ 7.1 in poi, IBM MQ adotta un approccio diverso alla gestione degli errori del cluster. Invece di arrestare il gestore repository e continuare senza di esso, il gestore repository esegue nuovamente le operazioni non riuscite. Se il gestore code rileva un problema con il gestore repository, segue una delle due linee di azione.

1. Se l'errore non compromette l'operazione del gestore code, il gestore code scrive un messaggio nel log degli errori. Rieseguire l'operazione non riuscita ogni 10 minuti fino a quando l'operazione non ha esito positivo. Per impostazione predefinita, si dispone di cinque giorni per gestire l'errore; in caso contrario, il gestore code scrive un messaggio nel log degli errori e si arresta. Puoi posticipare la chiusura di cinque giorni.

2. Se l'errore compromette l'operazione del gestore code, quest' ultimo scrive un messaggio nel log degli errori e si arresta immediatamente.

Un errore che compromette il funzionamento del gestore code è un errore che il gestore code non è stato in grado di diagnosticare o un errore che potrebbe avere conseguenze imprevedibili. Questo tipo di errore spesso si verifica quando il gestore code scrive un file FFST . Gli errori che compromettono il funzionamento del gestore code potrebbero essere causati da un bug in IBM MQ, o da un amministratore o da un programma, che esegue operazioni impreviste, come terminare un processo IBM MQ .

Il punto della modifica nel comportamento di ripristino da errore è quello di limitare il tempo in cui il gestore code continua l'esecuzione con un numero crescente di definizioni cluster incongruenti. Con l'aumentare del numero di incongruenze nelle definizioni di cluster, aumenta la probabilità di un comportamento anomalo dell'applicazione.

La scelta predefinita di arrestare il gestore code dopo cinque giorni rappresenta un compromesso tra la limitazione del numero di incongruenze e la disponibilità del gestore code fino a quando non vengono rilevati e risolti i problemi.

È possibile estendere il tempo prima che il gestore code venga arrestato per un periodo di tempo indefinito, mentre si corregge il problema o si attende la chiusura pianificata del gestore code. La permanenza di cinque giorni mantiene il gestore code in esecuzione per un lungo fine settimana, dandoti il tempo per reagire a eventuali problemi o prolungare il tempo prima di riavviare il gestore code.

Azioni correttive

Si dispone di una scelta di azioni per gestire i problemi di ripristino degli errori cluster. La prima scelta consiste nel monitorare e correggere il problema, la seconda nel monitorare e posticipare la correzione del problema e la scelta finale consiste nel continuare a gestire il ripristino da errori del cluster come nelle release precedenti a IBM WebSphere MQ 7.1.

1. Monitorare il log degli errori del gestore code per i messaggi di errore AMQ9448 e AMQ5008e correggere il problema.

   AMQ9448 indica che il gestore repository ha restituito un errore dopo l'esecuzione di un comando. Questo errore contrassegna l'inizio di un nuovo tentativo di esecuzione del comando ogni 10 minuti ed eventualmente l'arresto del gestore code dopo cinque giorni, a meno che l'arresto non venga posticipato.
   AMQ5008 indica che il gestore code è stato arrestato perché manca un processo IBM MQ . AMQ5008 risulta dall'arresto del gestore repository dopo cinque giorni. Se il gestore repository si arresta, il gestore code si arresta.
2. Monitorare il log degli errori del gestore code per il messaggio di errore AMQ9448e posticipare la correzione del problema.

   Se si disabilita il richiamo dei messaggi da `SYSTEM.CLUSTER.COMMAND.QUEUE`, il gestore repository interrompe il tentativo di eseguire i comandi e continua indefinitamente senza elaborare alcun lavoro. Tuttavia, tutti gli handle che il gestore repository detiene nelle code vengono rilasciati. Poiché il gestore repository non viene arrestato, il gestore code non viene arrestato dopo cinque giorni.
   Eseguire un comando MQSC per disabilitare il richiamo dei messaggi da `SYSTEM.CLUSTER.COMMAND.QUEUE`:
   ```
   ALTER QLOCAL(SYSTEM.CLUSTER.COMMAND.QUEUE) GET(DISABLED)
   ```
   Per riprendere la ricezione dei messaggi da `SYSTEM.CLUSTER.COMMAND.QUEUE` eseguire un comando MQSC:
   ```
   ALTER QLOCAL(SYSTEM.CLUSTER.COMMAND.QUEUE) GET(ENABLED)
   ```
3. Ripristinare il gestore code allo stesso comportamento di ripristino da errore del cluster precedente a IBM WebSphere MQ 7.1.

   È possibile impostare un parametro di ottimizzazione del gestore code per mantenere il gestore code in esecuzione se il gestore repository si arresta.

Il parametro di ottimizzazione è `TolerateRepositoryFailure`, nella stanza `TuningParameters` del file `qm.ini` . Per impedire l'arresto del gestore code, se il gestore repository viene arrestato, impostare `TolerateRepositoryFailure` su TRUE; consultare Figura 88 a pagina 631.

Riavviare il gestore code per abilitare l'opzione `TolerateRepositoryFailure` .

Se si è verificato un errore del cluster che impedisce il corretto avvio del gestore repository e quindi l'avvio del gestore code, impostare `TolerateRepositoryFailure` su TRUE per avviare il gestore code senza il gestore repository.

Considerazione speciale

Prima di IBM WebSphere MQ 7.1, alcuni amministratori che gestivano i gestori code che non facevano parte di un cluster arrestavano il processo `amqrrmfa` . L'arresto di `amqrrmfa` non ha influito sul gestore code.

L'arresto di `amqrrmfa` in IBM WebSphere MQ 7.1 o versioni successive causa l'arresto del gestore code, poiché viene considerato un errore del gestore code. Non è necessario arrestare il processo `amqrrmfa` in 7.1 o versioni successive, a meno che non si imposti il parametro di ottimizzazione del gestore code, `TolerateRepositoryFailure`.

Esempio

```
TuningParameters:
        TolerateRepositoryFailure=TRUE
```

Figura 88. Impostare `TolerateRepositoryFailure` su TRUE in qm.ini

Concetti correlati

File di configurazione del gestore code, qm.ini

Configurazione delle risorse JMS

Uno dei modi in cui un'applicazione di JMS può creare e configurare le risorse necessarie per connettersi a IBM MQ e accedere alle destinazioni per l'invio o la ricezione di messaggi è utilizzando JNDI (Java Naming and Directory Interface) per richiamare gli oggetti gestiti da un'ubicazione all'interno del servizio di denominazione e directory denominato spazio dei nomi JNDI. Prima che un'applicazione JMS possa richiamare gli oggetti gestiti da uno spazio nomi JNDI, è necessario creare e configurare gli oggetti gestiti.

Informazioni su questa attività

È possibile creare e configurare gli oggetti gestiti in IBM MQ utilizzando uno dei seguenti strumenti:

IBM MQ Explorer
È possibile utilizzare IBM MQ Explorer per creare e gestire le definizioni di oggetti JMS memorizzate in LDAP, in un file system locale o in altre ubicazioni.

Strumento di amministrazione IBM MQ JMS
Lo strumento di amministrazione IBM MQ JMS è uno strumento della riga comandi che è possibile utilizzare per creare e configurare gli oggetti IBM MQ JMS memorizzati in LDAP, in un file system locale o in altre ubicazioni. Lo strumento di gestione JMS utilizza una sintassi simile a **runmqsc**e supporta anche gli script.

Lo strumento di gestione utilizza un file di configurazione per impostare i valori di determinate proprietà. Viene fornito un file di configurazione di esempio, che è possibile modificare per adattarlo al sistema prima di iniziare utilizzando lo strumento per configurare le risorse JMS . Per ulteriori informazioni sul file di configurazione, consultare “Configurazione dello strumento di amministrazione JMS” a pagina 638.

Le applicazioni IBM MQ JMS distribuite in WebSphere Application Server devono accedere agli oggetti JMS dal repository JNDI del server delle applicazioni. Pertanto, se si utilizza la messaggistica JMS tra WebSphere Application Server e IBM MQ, è necessario creare oggetti in WebSphere Application Server che corrispondono agli oggetti creati in IBM MQ.

IBM MQ Explorer e lo strumento di amministrazione IBM MQ JMS non possono essere utilizzati per gestire oggetti IBM MQ JMS memorizzati in WebSphere Application Server. Invece, è possibile creare e configurare gli oggetti gestiti in WebSphere Application Server utilizzando uno dei seguenti strumenti:

WebSphere Application Server Console di gestione
La console di amministrazione WebSphere Application Server è uno strumento basato sul web che è possibile utilizzare per gestire gli oggetti di IBM MQ JMS in WebSphere Application Server.

Client di script wsadmin WebSphere Application Server
Il client di script WebSphere Application Server wsadmin fornisce comandi specializzati per la gestione di oggetti IBM MQ JMS in WebSphere Application Server.

Se si desidera utilizzare un'applicazione JMS per accedere alle risorse di un gestore code IBM MQ da WebSphere Application Server, è necessario utilizzare il provider di messaggistica IBM MQ in WebSphere Application Server, che contiene una versione di IBM MQ classes for JMS. L'adattatore di risorse IBM MQ fornito con WebSphere Application Server viene utilizzato da tutte le applicazioni che eseguono la messaggistica JMS con il fornitore di messaggistica IBM MQ . L'adattatore di risorse IBM MQ viene di solito aggiornato automaticamente quando si applicano i fix pack WebSphere Application Server , ma se l'adattatore di risorse è stato precedentemente aggiornato manualmente, è necessario aggiornare manualmente la propria configurazione per garantire che la manutenzione venga applicata correttamente.

Attività correlate
Scrittura di applicazioni IBM MQ classes for JMS
Riferimenti correlati
runmqsc

Configurazione di factory di connessione e destinazioni in un namespace JNDI

Le applicazioni JMS accedono agli oggetti gestiti nel servizio di denominazione e di directory tramite JNDI (Java Naming and Directory Interface). Gli oggetti gestiti JMS sono memorizzati in un'ubicazione all'interno del servizio di denominazione e di directory a cui si fa riferimento come spazio dei nomi JNDI. Un'applicazione JMS può ricercare gli oggetti gestiti per connettersi a IBM MQ e accedere alle destinazioni per l'invio o la ricezione di messaggi.

Informazioni su questa attività

Le applicazioni JMS cercano i nomi degli oggetti JMS nel servizio di denominazione e di directory utilizzando i contesti:

Contesto iniziale
Il contesto iniziale definisce la radice dello spazio nomi JNDI. Per ogni ubicazione nel servizio di denominazione e di directory, è necessario specificare un contesto iniziale per fornire un punto di partenza da cui un'applicazione JMS può risolvere i nomi degli oggetti gestiti in tale posizione del servizio di denominazione e di directory.

Contesti secondari
Un contesto può avere uno o più contesti secondari. Un contesto secondario è una suddivisione di uno spazio nomi JNDI e può contenere oggetti gestiti come factory di connessione e destinazioni, nonché altri contesti secondari. Un contesto secondario non è proprio un oggetto; è semplicemente un'estensione della convenzione di denominazione per gli oggetti nel contesto secondario.

È possibile creare contesti utilizzando IBM MQ Explorer o lo Strumento di amministrazione IBM MQ JMS .

Prima che un'applicazione IBM MQ classes for JMS possa recuperare gli oggetti gestiti da uno spazio nomi JNDI, è necessario prima creare gli oggetti gestiti utilizzando IBM MQ Explorer o lo strumento di amministrazione IBM MQ JMS . È possibile creare e configurare i seguenti tipi di oggetto JMS :

Factory di connessione
Un oggetto factory di connessione JMS definisce una serie di proprietà di configurazione standard per connessioni. Un'applicazione JMS utilizza una factory di connessione per creare una connessione a IBM MQ. È possibile creare una factory di connessione specifica per uno dei due domini di messaggistica, il dominio di messaggistica point-to-point e il dominio di messaggistica di pubblicazione / sottoscrizione. In alternativa, da JMS 1.1, è possibile creare factory di connessione indipendenti dal dominio che possono essere utilizzati sia per la messaggistica point-to-point che per la messaggistica di pubblicazione / sottoscrizione.

Destination
Una destinazione JMS è un oggetto che rappresenta la destinazione dei messaggi prodotti dal client e l'origine dei messaggi utilizzati da un'applicazione JMS . L'applicazione JMS può utilizzare un singolo oggetto di destinazione per inserire e ricevere messaggi oppure l'applicazione può utilizzare oggetti di destinazione separati. Esistono due tipi di oggetto di destinazione:

- Destinazione coda JMS utilizzata nella messaggistica point - to - point
- Destinazione argomento JMS utilizzata nella messaggistica di pubblicazione / sottoscrizione

Il seguente diagramma mostra un esempio di oggetti JMS creati in uno spazio dei nomi JNDI IBM MQ .

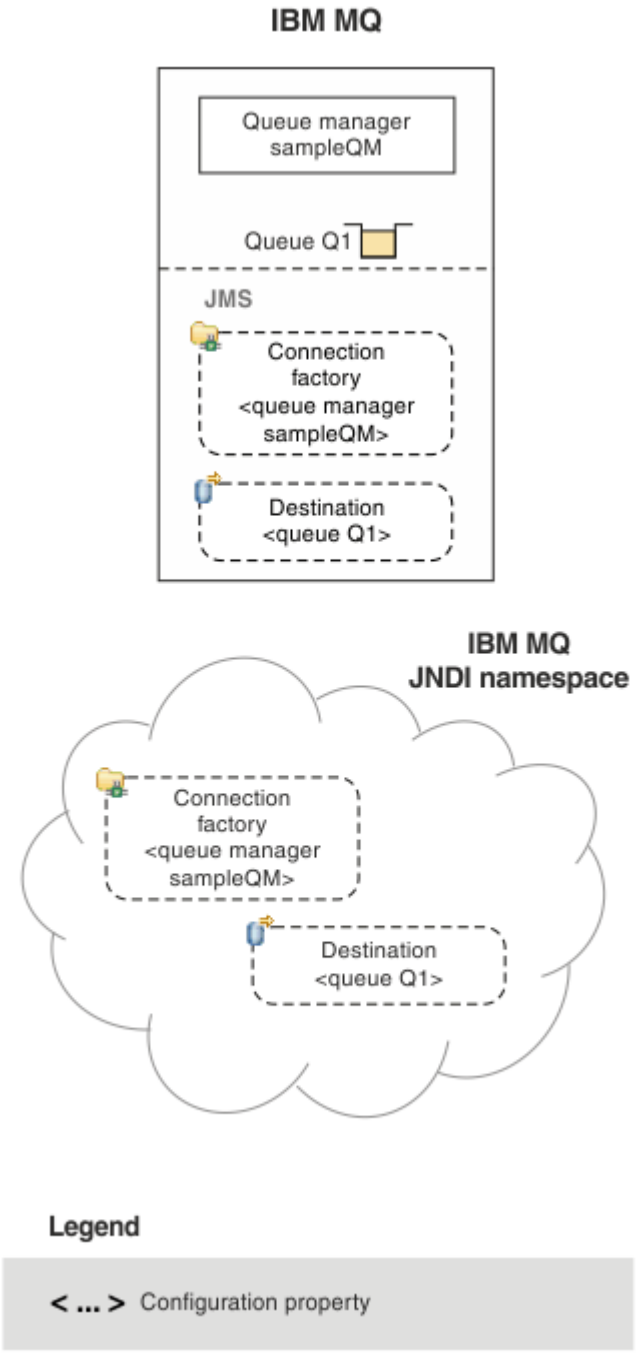


Figura 89. JMS oggetti creati in IBM MQ

Se si utilizza la messaggistica JMS tra WebSphere Application Server e IBM MQ, è necessario creare gli oggetti corrispondenti in WebSphere Application Server da utilizzare per comunicare con IBM MQ. Quando si crea uno di questi oggetti in WebSphere Application Server, viene memorizzato nello spazio dei nomi JNDI WebSphere Application Server come mostrato nel seguente diagramma.

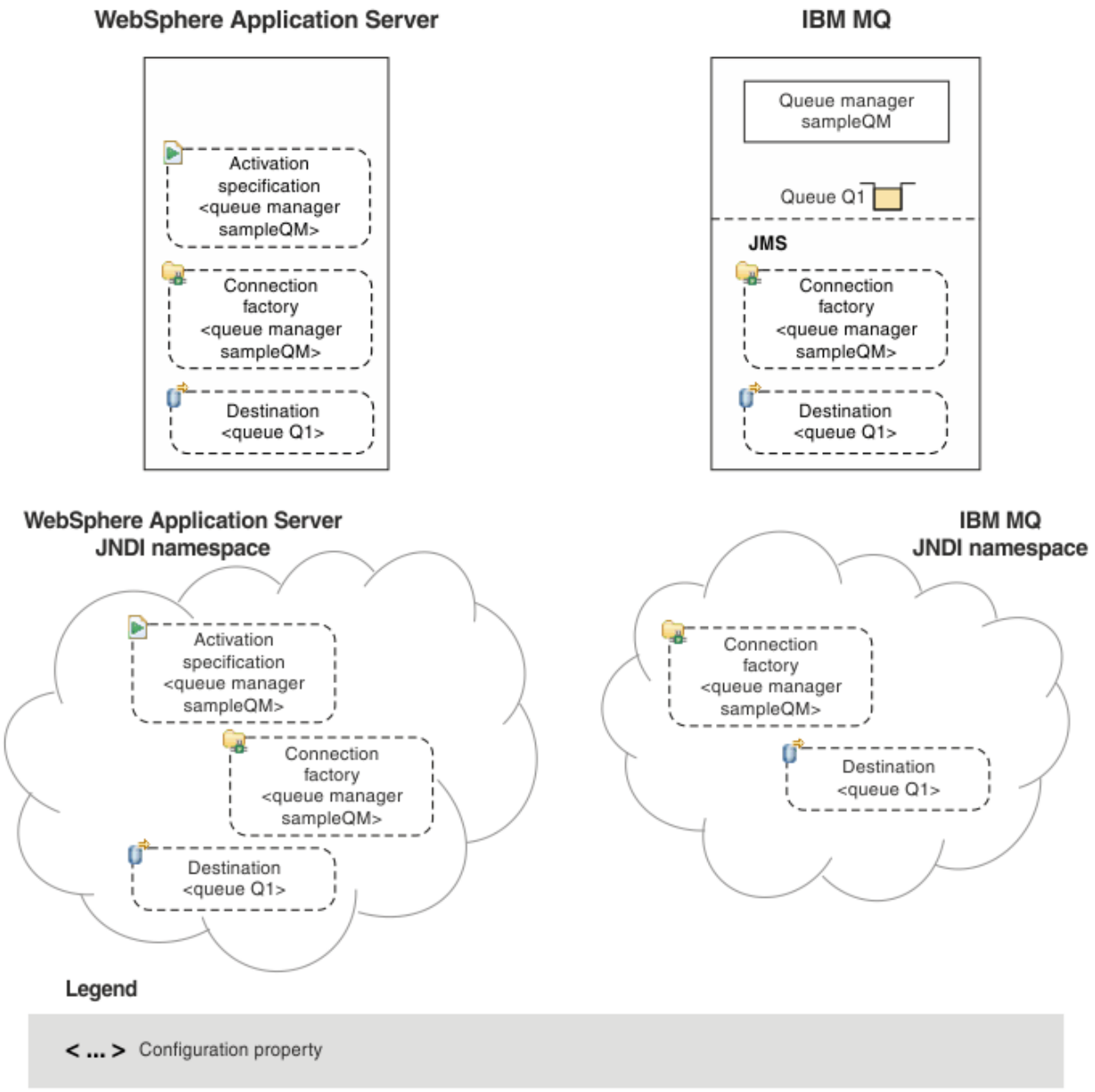


Figura 90. Oggetti creati in WebSphere Application Servere oggetti corrispondenti in IBM MQ

Se l'applicazione utilizza un MDB (message - driven bean), il factory di connessione viene utilizzato solo per i messaggi in uscita e i messaggi in entrata vengono ricevuti da una specifica di attivazione. Le specifiche di attivazione fanno parte dello standard Java EE Connector Architecture 1.5 (JCA 1.5). JCA 1.5 fornisce un modo standard per integrare i provider JMS , come IBM MQ, con i server delle applicazioni Java EE come WebSphere Application Server. Una specifica di attivazione JMS può essere associata a uno o più MDB (message driven bean) e fornisce la configurazione necessaria affinché questi MDB siano in ascolto dei messaggi che arrivano a una destinazione.

È possibile utilizzare la console di gestione WebSphere Application Server o i comandi di script wsadmin per creare e configurare le risorse JMS necessarie.

Procedura

- Per configurare gli oggetti JMS per IBM MQ utilizzando IBM MQ Explorer, consultare “Configurazione di oggetti JMS utilizzando IBM MQ Explorer” a pagina 636.

- Per configurare gli oggetti JMS per IBM MQ utilizzando lo strumento di amministrazione IBM MQ JMS , consultare “Configurazione di oggetti JMS utilizzando lo strumento di gestione” a pagina 637.
- Per configurare gli oggetti JMS per WebSphere Application Server, consultare “Configurazione di risorse JMS in WebSphere Application Server” a pagina 646.

Risultati

Un'applicazione IBM MQ classes for JMS può richiamare gli oggetti gestiti dallo spazio nomi JNDI e, se necessario, impostare o modificare una o più proprietà utilizzando le estensioni IBM JMS o le estensioni IBM MQ JMS .

Attività correlate

Utilizzo di JNDI per richiamare gli oggetti gestiti in una applicazione JMS

Creazione e configurazione di factory di connessione e destinazioni in una applicazione IBM MQ classes for JMS

Configurazione di oggetti JMS utilizzando IBM MQ Explorer

Utilizzare la GUI (graphical user interface) IBM MQ Explorer per creare oggetti JMS da oggetti IBM MQ e oggetti IBM MQ da oggetti JMS , nonché per la gestione e il monitoraggio di altri oggetti IBM MQ .

Informazioni su questa attività

IBM MQ Explorer è la GUI (graphical user interface) in cui è possibile amministrare e controllare gli oggetti IBM MQ, siano essi ospitati dal computer locale o su un sistema remoto. IBM MQ Explorer viene eseguito su Windows e Linux x86-64. È possibile collegarlo in remoto ai gestori code in esecuzione su qualsiasi piattaforma supportata, incluso z/OS, consentendo la visualizzazione, esplorazione e modifica del backbone di messaggistica dalla console.

In IBM MQ Explorer, tutte le factory di connessione vengono memorizzate nelle cartelle Factory di connessione nel contesto appropriato e nei contesti secondari.

È possibile eseguire i seguenti tipi di attività con IBM MQ Explorer, contestualmente da un oggetto esistente in IBM MQ Explorero dall'interno di una procedura guidata di creazione di un nuovo oggetto:

- Creare un factory di connessione JMS da uno dei seguenti oggetti IBM MQ :
  - Un gestore code IBM MQ , sul computer locale o su un sistema remoto.
  - Un canale IBM MQ .
  - Un listener IBM MQ .
- Aggiungere un gestore code IBM MQ a IBM MQ Explorer utilizzando un factory di connessione JMS .
- Creare una coda JMS da una coda IBM MQ .
- Creare una coda IBM MQ da una coda JMS .
- Creare un argomento JMS da un argomento IBM MQ , che può essere un oggetto IBM MQ o un argomento dinamico.
- Creare un argomento IBM MQ da un argomento JMS .

Procedura

- Avviare IBM MQ Explorer, se non è già in esecuzione.

  Se IBM MQ Explorer è in esecuzione e visualizza la pagina di benvenuto, chiudere la pagina di benvenuto per avviare la gestione degli oggetti IBM MQ .
- Se non è già stato fatto, creare un contesto iniziale definendo la root dello spazio dei nomi JNDI in cui gli oggetti JMS sono memorizzati nel servizio di denominazione e di directory.

  Dopo aver aggiunto il contesto iniziale a IBM MQ Explorer, è possibile creare oggetti factory di connessione, oggetti destinazione e contesti secondari nello spazio nomi JNDI.

Il contesto iniziale viene visualizzato nella vista Navigator nella cartella Oggetti amministrati JMS . Tenere presente che, sebbene venga visualizzato il contenuto completo dello spazio dei nomi JNDI, in IBM MQ Explorer è possibile modificare solo gli oggetti IBM MQ classes for JMS memorizzati in tale spazio. Per ulteriori informazioni, fare riferimento a Aggiunta di un contesto iniziale.

- Creare e configurare i contesti secondari e gli oggetti amministrati JMS necessari.

  Per ulteriori informazioni, consultare Creazione e configurazione di oggetti amministrati JMS.
- Configurare IBM MQ.

  Per ulteriori informazioni, consultare Configurazione di IBM MQ utilizzando IBM MQ Explorer .

Concetti correlati

Introduzione a IBM MQ Explorer

Attività correlate

Creazione e configurazione di factory di connessione e destinazioni in una applicazione IBM MQ classes for JMS

Configurazione di oggetti JMS utilizzando lo strumento di gestione

È possibile utilizzare lo strumento di amministrazione IBM MQ JMS per definire le proprietà di otto tipi di oggetti IBM MQ classes for JMS e memorizzarli all'interno di uno spazio dei nomi JNDI. Le applicazioni possono quindi utilizzare JNDI per richiamare questi oggetti gestiti dallo spazio dei nomi.

Informazioni su questa attività

La seguente tabella mostra gli otto tipi di oggetti gestiti che è possibile creare, configurare e manipolare utilizzando i verbi. La colonna Parola chiave mostra le stringhe che è possibile sostituire per *TYPE* nei comandi mostrati in Tabella 37 a pagina 637.

Tabella 37. I tipi di oggetto JMS gestiti dallo strumento di gestione

Tipo di oggetto	Parola chiave	Descrizione
MQConnectionFactory	CF	L'implementazione IBM MQ dell'interfaccia JMS ConnectionFactory . Questo rappresenta un oggetto factory per la creazione di connessioni in entrambi i domini point-to-point e di pubblicazione / sottoscrizione.
Factory di MQQueueConnection	QCF	L'implementazione IBM MQ dell'interfaccia factory JMS QueueConnection. Rappresenta un oggetto factory per la creazione di connessioni nel dominio point - to - point.
Factory MQTopicConnection	TCF	L'implementazione IBM MQ dell'interfaccia factory di JMS TopicConnection. Rappresenta un oggetto factory per la creazione di connessioni nel dominio di pubblicazione / sottoscrizione.
MQQUEUE	Q	L'implementazione IBM MQ dell'interfaccia della coda JMS . Rappresenta una destinazione per i messaggi nel dominio point - to - point.
MQArgomento	T	L'implementazione IBM MQ dell'interfaccia dell'argomento JMS . Rappresenta una destinazione per i messaggi nel dominio di pubblicazione / sottoscrizione.

Tabella 37. I tipi di oggetto JMS gestiti dallo strumento di gestione (Continua)		
Tipo di oggetto	**Parola chiave**	**Descrizione**
MQXAConnectionFactory “1” a pagina 638	XACF	L'implementazione IBM MQ dell'interfaccia JMS XAConnectionFactory . Rappresenta un oggetto factory per la creazione di connessioni nei domini point-to-point e di pubblicazione / sottoscrizione e dove le connessioni utilizzano le versioni XA delle classi JMS .
MQXAQueueConnectionFactory “1” a pagina 638	XAQCF	L'implementazione IBM MQ dell'interfaccia factory JMS XAQueueConnection. Ciò rappresenta un oggetto factory per creare connessioni nel dominio point - to - point che utilizzano le versioni XA delle classi JMS .
MQXATopicConnectionFactory “1” a pagina 638	XATCF	L'implementazione IBM MQ dell'interfaccia factory JMS XATopicConnection. Rappresenta un oggetto factory per la creazione di connessioni nel dominio di pubblicazione / sottoscrizione che utilizzano le versioni XA delle classi JMS .

Nota:

1. Queste classi vengono fornite per essere utilizzate dai fornitori dei server delle applicazioni. È improbabile che siano direttamente utili per i programmatori di applicazioni.

Per ulteriori informazioni su come configurare questi oggetti, consultare “Configurazione di oggetti JMS” a pagina 646.

I valori e i tipi di proprietà necessari per utilizzare questo strumento sono elencati in Proprietà degli oggetti IBM MQ classes for JMS.

È anche possibile utilizzare lo strumento per manipolare i contesti secondari dello spazio nomi della directory all'interno di JNDI come descritto in “Configurazione dei contesti secondari” a pagina 643.

È inoltre possibile creare e configurare gli oggetti gestiti JMS con IBM MQ Explorer.

Attività correlate

Creazione e configurazione di factory di connessione e destinazioni in una applicazione IBM MQ classes for JMS

Utilizzo di JNDI per richiamare gli oggetti gestiti in una applicazione JMS

Configurazione dello strumento di amministrazione JMS

Lo strumento di amministrazione IBM MQ JMS utilizza un file di configurazione per impostare i valori di alcune proprietà. Viene fornito un file di configurazione di esempio, che è possibile modificare per adattarlo al sistema.

Informazioni su questa attività

Il file di configurazione è un file di testo semplice costituito da una serie di coppie chiave - valore, separate dal segno uguale (=). Configurare lo strumento di amministrazione impostando i valori per le tre proprietà definite nel file di configurazione. Il seguente esempio mostra queste tre proprietà:

```
#Set the service provider
INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
```

```
#Set the initial context
PROVIDER_URL=ldap://polaris/o=ibm_us,c=us
#Set the authentication type
SECURITY_AUTHENTICATION=none
```

In questo esempio, un segno cancelletto (#) nella prima colonna della riga indica un commento o una riga non utilizzata.

Un file di configurazione di esempio, utilizzato come file di configurazione predefinito, viene fornito con IBM MQ. Il file di esempio è denominato `JMSAdmin.config`e si trova nella directory *MQ_JAVA_INSTALL_PATH*`/bin` . È possibile modificare questo file di esempio per definire le impostazioni necessarie per il proprio sistema oppure creare il proprio file di configurazione.

Quando si avvia lo strumento di gestione, è possibile specificare il file di configurazione da utilizzare utilizzando il parametro della riga comandi `-cfg` , come descritto in “Avvio dello strumento di amministrazione” a pagina 640. Se non si specifica un nome file di configurazione quando si richiama lo strumento, lo strumento tenta di caricare il file di configurazione predefinito (`JMSAdmin.config`). Ricerca questo file prima nella directory corrente e poi nella directory *MQ_JAVA_INSTALL_PATH*`/bin` , dove *MQ_JAVA_INSTALL_PATH* è il percorso per l'installazione di IBM MQ classes for JMS .

I nomi degli oggetti JMS memorizzati in un ambiente LDAP devono essere conformi alle convenzioni di denominazione LDAP. Una di queste convenzioni è che i nomi oggetto e contesto devono includere un prefisso, come `cn=` (nome comune) o `ou=` (unità organizzativa). Lo strumento di amministrazione semplifica l'utilizzo dei provider di servizi LDAP consentendo di fare riferimento a nomi di oggetti e di contesto senza un prefisso. Se non si fornisce un prefisso, lo strumento aggiunge automaticamente un prefisso predefinito al nome fornito. Per LDAP, è `cn=`. Se necessario, è possibile modificare il prefisso predefinito impostando la proprietà **NAME_PREFIX** nel file di configurazione.

Nota: Potrebbe essere necessario configurare il server LDAP per memorizzare gli oggetti Java . Per ulteriori informazioni, consultare la documentazione per il server LDAP.

Procedura

1. Definire il provider di servizi utilizzato dallo strumento configurando la proprietà **INITIAL_CONTEXT_FACTORY** .

   I valori supportati per questa proprietà sono i seguenti:

   - com.sun.jndi.ldap.LdapCtxFactory (per LDAP)
   - com.sun.jndi.fscontext.RefFSContextFactory (per il contesto del file system)
   - z/OS com.ibm.jndi.LDAPCtxFactory è supportato solo su z/OS e fornisce l'accesso a un server LDAP. Tuttavia, questa classe non è compatibile con com.sun.jndi.ldap.LdapCtxFactory, poiché gli oggetti creati utilizzando un factory InitialContextnon possono essere letti o modificati utilizzando l'altro factory.

   È anche possibile utilizzare lo strumento di gestione per collegarsi ad altri contesti JNDI utilizzando tre parametri definiti nel file di configurazione JMSAdmin. Per utilizzare un factory InitialContextdifferente:

   a) Impostare la proprietà **INITIAL_CONTEXT_FACTORY** sul nome classe richiesto.

   b) Definire il funzionamento del factory InitialContextutilizzando le proprietà **USE_INITIAL_DIR_CONTEXT**, **NAME_PREFIX** e **NAME_READABILITY_MARKER** .

      Le impostazioni per queste proprietà sono descritte nei commenti del file di configurazione di esempio.

   Non è necessario definire le proprietà **USE_INITIAL_DIR_CONTEXT**, **NAME_PREFIX** e **NAME_READABILITY_MARKER** se si utilizza uno dei valori **INITIAL_CONTEXT_FACTORY** supportati. Tuttavia, è possibile assegnare dei valori a queste proprietà se si desidera sovrascrivere i valori predefiniti del sistema. Ad esempio, se gli oggetti sono archiviati in un ambiente LDAP, è possibile modificare il prefisso predefinito che lo strumento aggiunge ai nomi oggetto e contesto impostando la proprietà **NAME_PREFIX** sul prefisso richiesto.

Se si omettono una o più delle tre proprietà InitialContextFactory, lo strumento di amministrazione fornisce valori predefiniti appropriati in base ai valori delle altre proprietà.

2. Definire l'URL del contesto iniziale della sessione configurando la proprietà **PROVIDER_URL** .

   Questo URL è la root di tutte le operazioni JNDI eseguite dallo strumento. Sono supportate due forme di questa proprietà:

   - ldap://nomehost/nomecontesto
   - file: [unità:] /nomepercorso

   Il formato dell'URL LDAP può variare, a seconda del provider LDAP. Per ulteriori informazioni, consultare la documentazione LDAP.

3. Definire se JNDI trasmette le credenziali di sicurezza al provider di servizi configurando la proprietà **SECURITY_AUTHENTICATION** .

   Questa proprietà viene utilizzata solo quando viene utilizzato un fornitore di servizi LDAP e può assumere uno dei tre seguenti valori:

   none (autenticazione anonima)
   Se si imposta questo parametro su none, JNDI non passa alcuna credenziale di sicurezza al provider di servizi e viene eseguita l' *autenticazione anonima* .

   semplice (autenticazione semplice)
   Se si imposta il parametro su semplice, le credenziali di sicurezza vengono trasmesse tramite JNDI al fornitore del servizio sottostante. Queste credenziali di sicurezza sono nel formato di un DN (distinguished name) utente e parola d'ordine.

   CRAM-MD5 (meccanismo di autenticazioneCRAM-MD5)
   Se si imposta il parametro su CRAM-MD5, le credenziali di sicurezza vengono trasmesse tramite JNDI al provider di servizi sottostante. Queste credenziali di sicurezza sono nel formato di un DN (distinguished name) utente e parola d'ordine.

   Se non si fornisce un valore valido per la proprietà **SECURITY_AUTHENTICATION** , la proprietà assume il valore predefinito none.

   Se le credenziali di sicurezza sono richieste, vengono richieste quando lo strumento viene inizializzato. È possibile evitare questa situazione impostando le proprietà **PROVIDER_USERDN** e **PROVIDER_PASSWORD** nel file di configurazione JMSAdmin.

   Nota: Se non si utilizzano queste proprietà, il testo immesso, *inclusa la password*, viene ripetuto sullo schermo. Ciò potrebbe avere implicazioni sulla sicurezza.

   Lo strumento non esegue l'autenticazione; l'attività di autenticazione è delegata al server LDAP. L'amministratore del server LDAP deve impostare e gestire i privilegi di accesso a parti differenti della directory. Per ulteriori informazioni, consultare la documentazione LDAP. Se l'autenticazione ha esito negativo, lo strumento visualizza un messaggio di errore appropriato e termina.

   Informazioni più dettagliate sulla sicurezza e JNDI sono disponibili nella documentazione sul sito Web Oracle Java (Oracle Technology Network for Java Developers).

Avvio dello strumento di amministrazione

Lo strumento di amministrazione dispone di una CLI (command - line interface) che è possibile utilizzare in modo interattivo o per avviare un processo batch.

Informazioni su questa attività

La modalità interattiva fornisce un prompt dei comandi in cui è possibile immettere i comandi di gestione. In modalità batch, il comando per avviare lo strumento include il nome di un file contenente uno script di comandi di amministrazione.

Procedura

Modalità interattiva

- Per avviare lo strumento in modalità interattiva, immettere il seguente comando:

```
JMSAdmin [-t] [-v] [-cfg config_filename]
```

dove:

-t
Abilita traccia (il valore predefinito è traccia disattivata)

Il file di traccia viene creato in `"%MQ_JAVA_DATA_PATH%"\errors` (Windows) o `/var/mqm/trace` (UNIX). Il nome del file di traccia è nel formato:

`mqjms_`*`PID`*`.trc`

dove *PID* è l'ID processo della JVM.

-v
Produce output dettagliato (il valore predefinito è output conciso)

-cfg nomefile_config
Denomina un file di configurazione alternativo. Se questo parametro viene omesso, viene utilizzato il file di configurazione predefinito, `JMSAdmin.config`. Per ulteriori informazioni sul file di configurazione, consultare “Configurazione dello strumento di amministrazione JMS” a pagina 638.

Viene visualizzato un prompt dei comandi, che indica che lo strumento è pronto ad accettare i comandi di gestione. Questa richiesta inizialmente viene visualizzata come:

```
InitCtx>
```

che indica che il contesto corrente (ossia, il contesto JNDI a cui fanno riferimento tutte le operazioni di denominazione e di directory) è il contesto iniziale definito nel parametro di configurazione **PROVIDER_URL** . Per maggiori informazioni su questo parametro, fare riferimento a “Configurazione dello strumento di amministrazione JMS” a pagina 638.

Mentre si attraversa lo spazio dei nomi della directory, il prompt cambia per riflettere questo, in modo che il prompt visualizzi sempre il contesto corrente.

Modalità batch

- Per avviare lo strumento in modalit ... batch, immettere il seguente comando:

```
JMSAdmin test.scp
```

dove *test.scp* è un file script che contiene i comandi di gestione. Per ulteriori informazioni, consultare “Utilizzo dei comandi di gestione” a pagina 641. L'ultimo comando nel file deve essere il comando `END` .

Utilizzo dei comandi di gestione

Lo strumento di amministrazione accetta comandi costituiti da un verbo di amministrazione e dai relativi parametri appropriati.

Informazioni su questa attività

La seguente tabella elenca i verbi di amministrazione che è possibile utilizzare quando si immettono comandi con lo strumento di amministrazione.

Tabella 38. Verbi di amministrazione

Verbo	**Forma breve**	**Descrizione**
MODIFICA	Alt	Modificare almeno una delle proprietà di un oggetto gestito

Tabella 38. Verbi di amministrazione (Continua)		
Verbo	**Forma breve**	**Descrizione**
Definisci	DEF	Creare e memorizzare un oggetto gestito o creare un contesto secondario
VISUALIZZA	DIS	Visualizza le proprietà di uno o più oggetti gestiti memorizzati o il contenuto del contesto corrente
ELIMINA	DEL	Rimuovere uno o più oggetti gestiti dallo spazio dei nomi o rimuovere un contesto secondario vuoto
CHANGE	CHG	Modificare il contesto corrente, consentendo all'utente di attraversare lo spazio dei nomi della directory in un punto qualsiasi al di sotto del contesto iniziale (autorizzazione di sicurezza in sospeso)
Copia	CP	Creare una copia di un oggetto gestito memorizzato, memorizzandolo con un nome alternativo
SPOSTA	mV	Modificare il nome con cui è memorizzato un oggetto gestito
FINE		Chiudere lo Strumento di amministrazione

Procedura

- Se lo strumento di amministrazione non è già stato avviato, avviarlo come descritto in "Avvio dello strumento di amministrazione" a pagina 640.

  Viene visualizzato il prompt dei comandi, che indica che lo strumento è pronto ad accettare i comandi di gestione. Questa richiesta inizialmente viene visualizzata come:

  ```
  InitCtx>
  ```

  Per modificare il contesto corrente, utilizzare il comando CHANGE come descritto in "Configurazione dei contesti secondari" a pagina 643.
- Immettere i comandi nel seguente formato:

  ```
  verb [param]*
  ```

  dove **verb** è uno dei verbi di amministrazione elencati in Tabella 38 a pagina 641. Tutti i comandi validi contengono un verbo, che viene visualizzato all'inizio del comando in formato standard o breve. I nomi dei verbi non sono sensibili al maiuscolo / minuscolo.
- Per terminare un comando, premere Invio, a meno che non si desideri immettere più comandi insieme, nel qual caso immettere il segno più (+) direttamente prima di premere Invio.

  In genere, per terminare i comandi, premere Invio. Tuttavia, è possibile sovrascriverlo immettendo il segno più (+) direttamente prima di premere Invio. Ciò consente di immettere comandi a più righe, come mostrato nel seguente esempio:

  ```
  DEFINE Q(BookingsInputQueue) +
  QMGR(QM.POLARIS.TEST) +
  QUEUE(BOOKINGS.INPUT.QUEUE) +
  PORT(1415) +
  CCSID(437)
  ```
- Per chiudere lo strumento di amministrazione, utilizzare il comando **END** .

  Questo verbo non può prendere alcun parametro.

Configurazione dei contesti secondari

È possibile utilizzare i verbi **CHANGE**, **DEFINE**, **DISPLAY** e **DELETE** per configurare i contesti secondari dello spazio dei nomi della directory.

Informazioni su questa attività

L'uso di questi verbi è descritto nella tabella seguente.

Tabella 39. Sintassi e descrizione dei comandi utilizzati per manipolare i contesti secondari

Sintassi dei comandi	Descrizione
DEFINE CTX (ctxName)	Tenta di creare un contesto secondario del contesto corrente, con il nome ctxName. Non riesce se si verifica una violazione della sicurezza, se il contesto secondario esiste già o se il nome fornito non è valido.
VISUALIZZA CTX	Visualizza il contenuto del contesto corrente. Gli oggetti gestiti sono annotati con a, i contesti secondari con `[D]`. Viene visualizzato anche il tipo Java di ciascun oggetto.
DELETE CTX (ctxName)	Tenta di eliminare il contesto child del contesto corrente con il nome ctxName. Non riesce se il contesto non viene trovato, non è vuoto o se si verifica una violazione della sicurezza.
MODIFICA CTX (ctxName)	Modifica il contesto corrente, in modo che ora faccia riferimento al contesto child con il nome ctxName. È possibile fornire uno dei due valori speciali di ctxName : **= ATTIVO** passa al parent del contesto corrente **= INIT** passa direttamente al contesto iniziale Ha esito negativo se il contesto specificato non esiste o se si verifica una violazione della sicurezza.

I nomi degli oggetti JMS memorizzati in un ambiente LDAP devono essere conformi alle convenzioni di denominazione LDAP. Una di queste convenzioni è che i nomi oggetto e contesto devono includere un prefisso, come `cn=` (nome comune) o `ou=` (unità organizzativa). Lo strumento di amministrazione semplifica l'utilizzo dei provider di servizi LDAP consentendo di fare riferimento a nomi di oggetti e di contesto senza un prefisso. Se non si fornisce un prefisso, lo strumento aggiunge automaticamente un prefisso predefinito al nome fornito. Per LDAP, è `cn=`. Se necessario, è possibile modificare il prefisso predefinito impostando la proprietà **NAME_PREFIX** nel file di configurazione. Per ulteriori informazioni, consultare “Configurazione dello strumento di amministrazione JMS” a pagina 638.

Nota: Potrebbe essere necessario configurare il server LDAP per memorizzare gli oggetti Java . Per ulteriori informazioni, consultare la documentazione per il server LDAP.

Creazione di oggetti JMS

Per creare oggetti di destinazione e factory di connessione JMS e memorizzarli in un namespace JNDI, utilizzare il comando `DEFINE` . Per memorizzare gli oggetti in un ambiente LDAP, è necessario fornire nomi conformi a determinate convenzioni. Lo strumento di amministrazione consente di rispettare le convenzioni di denominazione LDAP aggiungendo un prefisso predefinito ai nomi oggetto.

Informazioni su questa attività

Il comando DEFINE crea un oggetto gestito con il tipo, il nome e le proprietà specificati. Il nuovo oggetto viene memorizzato nel contesto corrente.

I nomi degli oggetti JMS memorizzati in un ambiente LDAP devono essere conformi alle convenzioni di denominazione LDAP. Una di queste convenzioni è che i nomi oggetto e contesto devono includere un prefisso, come cn= (nome comune) o ou= (unità organizzativa). Lo strumento di amministrazione semplifica l'utilizzo dei provider di servizi LDAP consentendo di fare riferimento a nomi di oggetti e di contesto senza un prefisso. Se non si fornisce un prefisso, lo strumento aggiunge automaticamente un prefisso predefinito al nome fornito. Per LDAP, è cn=. Se necessario, è possibile modificare il prefisso predefinito impostando la proprietà **NAME_PREFIX** nel file di configurazione. Per ulteriori informazioni, consultare "Configurazione dello strumento di amministrazione JMS" a pagina 638.

Nota: Potrebbe essere necessario configurare il server LDAP per memorizzare gli oggetti Java . Per ulteriori informazioni, consultare la documentazione per il server LDAP.

Procedura

1. Se lo strumento di amministrazione non è già stato avviato, avviarlo come descritto in "Avvio dello strumento di amministrazione" a pagina 640.

   Viene visualizzato il prompt dei comandi, che indica che lo strumento è pronto ad accettare i comandi di gestione.
2. Assicurarsi che il prompt dei comandi mostri il contesto in cui si desidera creare il nuovo oggetto.

   Quando si avvia lo strumento di gestione, il prompt inizialmente viene visualizzato come:

   ```
   InitCtx>
   ```

   Per modificare il contesto corrente, utilizzare il comando CHANGE come descritto in "Configurazione dei contesti secondari" a pagina 643.
3. Per creare una factory di connessione, una destinazione coda o una destinazione argomento, utilizzare la seguente sintassi del comando:

   ```
   DEFINE TYPE (name) [property]*
   ```

   Vale a dire, immettere il comando DEFINE , seguito da un *TYPE* (name) riferimento oggetto gestito, seguito da zero o più *proprietà* (consultare Proprietà di oggetti IBM MQ classes for JMS).
4. Per creare una factory di connessione, una destinazione coda o una destinazione argomento, utilizzare la seguente sintassi del comando:

   ```
   DEFINE TYPE (name) [property]*
   ```
5. Per visualizzare l'oggetto appena creato, utilizzare il comando DISPLAY con la seguente sintassi del comando:

   ```
   DISPLAY TYPE (name)
   ```

Esempio

Il seguente esempio mostra una coda denominata testQueue creata nel contesto iniziale utilizzando il comando DEFINE . Poiché questo oggetto viene memorizzato in un ambiente LDAP, anche se il nome oggetto testQueue non viene immesso con un prefisso, lo strumento ne aggiunge automaticamente uno per garantire la conformità con la convenzione di denominazione LDAP. L'inoltro del comando DISPLAY Q(testQueue) comporta anche l'aggiunta di questo prefisso.

```
InitCtx> DEFINE Q(testQueue)
InitCtx> DISPLAY CTX
Contents of InitCtx
a cn=testQueue       com.ibm.mq.jms.MQQueue
```

```
1 Object(s)
0 Context(s)
1 Binding(s), 1 Administered
```

Condizioni di errore di esempio che creano un oggetto JMS

Quando si crea un oggetto, possono verificarsi diverse condizioni di errore comuni.

Di seguito sono riportati esempi di queste condizioni di errore:

CipherSpec associato a CipherSuite

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) SSLCIPHERSUITE(RC4_MD5_US)
WARNING: Converting CipherSpec RC4_MD5_US to
CipherSuite SSL_RSA_WITH_RC4_128_MD5
```

Proprietà non valida per l'oggetto

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) PRIORITY(4)
Unable to create a valid object, please check the parameters supplied
Invalid property for a QCF: PRI
```

Tipo non valido per il valore della proprietà

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) CCSID(english)
Unable to create a valid object, please check the parameters supplied
Invalid value for CCS property: English
```

Conflitto di proprietà - il client/bindings

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) HOSTNAME(polaris.hursley.ibm.com)
Unable to create a valid object, please check the parameters supplied
Invalid property in this context: Client-bindings attribute clash
```

Conflitto di proprietà - Inizializzazione uscita

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) SECEXITINIT(initStr)
Unable to create a valid object, please check the parameters supplied
Invalid property in this context: ExitInit string supplied
without Exit string
```

Il valore della proprietà non è compreso nell'intervallo valido

```
InitCtx/cn=Trash> DEFINE Q(testQ) PRIORITY(12)
Unable to create a valid object, please check the parameters supplied
Invalid value for PRI property: 12
```

Proprietà sconosciuta

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) PIZZA(ham and mushroom)
Unable to create a valid object, please check the parameters supplied
Unknown property: PIZZA
```

Di seguito sono riportati esempi di condizioni di errore che potrebbero verificarsi su Windows quando si ricercano oggetti gestiti da JNDI da un'applicazione JMS .

1. Se si utilizza il provider JNDI WebSphere , com.ibm.websphere.naming.WsnInitialContextFactory, è necessario utilizzare una barra (/) per accedere agli oggetti gestiti definiti nei contesti secondari; ad esempio, jms /MyQueueName. Se si utilizza una barra rovesciata (\), viene generata un'eccezione InvalidName.

2. Se si utilizza il provider JNDI Oracle , com.sun.jndi.fscontext.RefFSContextFactory, è necessario utilizzare una barra rovesciata (\) per accedere agli oggetti gestiti definiti nei contesti secondari; ad esempio, ctx1\\fred. Se si utilizza una barra (/), viene generata unaFoundException NameNot.

Configurazione di oggetti JMS

È possibile utilizzare i comandi ALTER, DEFINE, DISPLAY, DELETE, COPYe MOVE per manipolare gli oggetti amministrati nello spazio dei nomi della directory.

Informazioni su questa attività

Tabella 40 a pagina 646 riepiloga l'utilizzo di questi verbi. Sostituire *TYPE* con la parola chiave che rappresenta l'oggetto gestito richiesto, come descritto in "Configurazione di oggetti JMS utilizzando lo strumento di gestione" a pagina 637.

Tabella 40. Sintassi e descrizione dei comandi utilizzati per manipolare gli oggetti gestiti

Sintassi dei comandi	**Descrizione**
ALTER *TYPE* (nome) [proprietà] *	Tenta di aggiornare le proprietà dell'oggetto gestito con quelle fornite. Ha esito negativo se si verifica una violazione della sicurezza, se non è possibile trovare l'oggetto specificato o se le nuove proprietà fornite non sono valide.
DEFINE *TYPE* (nome) [proprietà] *	Tenta di creare un oggetto gestito di tipo *TYPE* con le proprietà fornite e lo memorizza con il nome name nel contesto corrente. Non riesce se si verifica una violazione della sicurezza, se il nome fornito non è valido o se esiste un oggetto con tale nome o se le proprietà fornite non sono valide.
DISPLAY *TYPE* (nome)	Visualizza le proprietà dell'oggetto amministrato di tipo *TYPE* , associato al nome name nel contesto corrente. Non riesce se l'oggetto non esiste o se si verifica una violazione della sicurezza.
DELETE *TYPE* (nome)	Tenta di rimuovere l'oggetto gestito di tipo *TYPE* , con nome name, dal contesto corrente. Non riesce se l'oggetto non esiste o se si verifica una violazione della sicurezza.
COPY *TYPE* (nameA) *TYPE* (nameB)	Crea una copia dell'oggetto gestito di tipo *TYPE* , con il nome nameA, denominando la copia nameB. Tutto ciò si verifica nell'ambito del contesto corrente. Non riesce se l'oggetto da copiare non esiste, se esiste un oggetto denominato nameB o se si verifica una violazione della sicurezza.
MOVE *TYPE* (nameA) *TYPE* (nameB)	Sposta (ridenomina) l'oggetto gestito di tipo *TYPE* , con il nome nameA, in nameB. Tutto ciò si verifica nell'ambito del contesto corrente. Non riesce se l'oggetto da spostare non esiste, se esiste un oggetto con nome nameB o se si verifica una violazione della sicurezza.

Configurazione di risorse JMS in WebSphere Application Server

Per configurare le risorse JMS in WebSphere Application Server, è possibile utilizzare la console di gestione o i comandi wsadmin.

Informazioni su questa attività

Le applicazioni Java Message Service (JMS) generalmente si basano su oggetti configurati esternamente che descrivono il modo in cui l'applicazione si connette al provider JMS e alle destinazioni a cui accede.

Le applicazioni JMS utilizzano Java Naming Directory Interface (JNDI) per accedere ai seguenti tipi di oggetto al runtime:

- Specifiche di attivazione (utilizzate dai server delle applicazioni Java EE)
- Le factory di connessione unificate (con JMS 1.1, le factory di connessione indipendenti dal dominio (unificate) sono preferite alle factory di connessione code specifiche del dominio e alle factory di connessione argomenti)
- Factory di connessione argomenti (utilizzati dalle applicazioni JMS 1.0)
- Factory di connessione code (utilizzate da applicazioni JMS 1.0)
- Code
- Argomenti

Tramite il provider di messaggistica IBM MQ in WebSphere Application Server, le applicazioni di messaggistica Java Message Service (JMS) possono utilizzare il proprio sistema IBM MQ come provider esterno di risorse di messaggistica JMS . Per abilitare questo approccio, si configura il fornitore di messaggistica IBM MQ in WebSphere Application Server per definire le risorse JMS per la connessione a qualsiasi gestore code sulla rete IBM MQ .

È possibile utilizzare WebSphere Application Server per configurare le risorse IBM MQ per le applicazioni (ad esempio factory di connessione code) e per gestire i messaggi e le sottoscrizioni associate alle destinazioni JMS . La sicurezza viene gestita tramite IBM MQ.

Attività correlate

Utilizzo congiunto di IBM MQ e WebSphere Application Server

WebSphere Application Server argomenti

Interoperabilità utilizzando il provider di messaggistica IBM MQ

Gestione della messaggistica con il provider di messaggistica IBM MQ

Associazione dei nomi del pannello della console di gestione ai nomi di comandi e ai nomi IBM MQ

Configurazione delle risorse JMS utilizzando la console di gestione

È possibile utilizzare la console di gestione WebSphere Application Server per configurare le specifiche di attivazione, le factory di connessione e le destinazioni per il provider IBM MQ JMS .

Informazioni su questa attività

È possibile utilizzare la console di amministrazione WebSphere Application Server per creare, visualizzare o modificare una delle seguenti risorse:

- Specifiche di attivazione
- Factory di connessione indipendenti dal dominio (JMS 1.1 o versioni successive)
- Factory di connessione code
- Factory di connessione argomenti
- Code
- Argomenti

La seguente procedura fornisce una panoramica dei modi in cui è possibile utilizzare la console di gestione per configurare le risorse JMS da utilizzare con il provider di messaggistica IBM MQ . Ogni passo include il nome dell'argomento nella documentazione del prodotto WebSphere Application Server a cui è possibile fare riferimento per ulteriori informazioni. Consultare *Collegamenti correlati* per i link a questi argomenti nella documentazione del prodotto WebSphere Application Server .

In una cella WebSphere Application Server a versione mista, è possibile gestire le risorse IBM MQ sui nodi di tutte le versioni. Tuttavia, alcune proprietà non sono disponibili su tutte le versioni. In questa situazione, nella console di gestione vengono visualizzate solo le proprietà di quel particolare nodo.

Procedura

Per creare o configurare una specifica di attivazione da utilizzare con il fornitore di messaggistica IBM MQ :

- Per creare una specifica di attivazione, utilizzare la procedura guidata Crea risorsa IBM MQ JMS .

  È possibile utilizzare la procedura guidata per specificare tutti i dettagli per la specifica di attivazione oppure è possibile scegliere di specificare i dettagli di connessione per IBM MQ utilizzando una CCDT (client channel definition table). Quando si specificano i dettagli della connessione utilizzando la procedura guidata, è possibile scegliere di immettere le informazioni sull'host e sulla porta separatamente oppure, se si utilizza un gestore code a più istanze, immettere le informazioni sull'host e sulla porta sotto forma di un elenco di nomi di connessione. Per ulteriori informazioni, consultare *Creazione di una specifica di attivazione per il provider di messaggistica IBM MQ*.
- Per visualizzare o modificare le proprietà di configurazione di una specifica di attivazione, utilizzare il pannello delle impostazioni della factory di connessione del provider di messaggistica IBM MQ della console di gestione.

  Queste proprietà di configurazione controllano il modo in cui vengono create le connessioni alle code e agli argomenti associati. Per ulteriori informazioni, fare riferimento a *Configurazione di una specifica di attivazione per il provider di messaggistica IBM MQ*.

Per creare o configurare una factory di connessione unificata, una factory di connessione code o una factory di connessione argomenti da utilizzare con il fornitore di messaggistica IBM MQ :

- Per creare una factory di connessione, selezionare il tipo di factory di connessione che si desidera creare, quindi utilizzare la procedura guidata Crea risorsa IBM MQ JMS per specificare i dettagli.
  - Se l'applicazione JMS è progettata per utilizzare solo la messaggistica point - to - point, creare una factory di connessione specifica del dominio per il dominio di messaggistica point - to - point che può essere utilizzato per creare connessioni specifiche per la messaggistica point - to - point.
  - Se l'applicazione JMS è progettata solo per utilizzare la messaggistica di pubblicazione / sottoscrizione, creare una factory di connessione specifica del dominio per il dominio di messaggistica di pubblicazione / sottoscrizione che può essere utilizzato per la creazione di connessioni specifiche per la messaggistica di pubblicazione / sottoscrizione.
  - Per JMS 1.1 o versioni successive, creare un factory di connessione indipendente dal dominio che può essere utilizzato sia per la messaggistica point-to-point che per la messaggistica di pubblicazione / sottoscrizione, consentendo all'applicazione di eseguire entrambe le operazioni point-to-point e di pubblicazione / sottoscrizione nella stessa transazione.

  È possibile scegliere se utilizzare la procedura guidata per specificare tutti i dettagli per la factory di connessione oppure è possibile scegliere di specificare i dettagli di connessione per IBM MQ utilizzando una CCDT (client channel definition table). Quando si specificano i dettagli della connessione utilizzando la procedura guidata, è possibile scegliere di immettere le informazioni sull'host e sulla porta separatamente oppure, se si utilizza un gestore code a più istanze, immettere le informazioni sull'host e sulla porta sotto forma di un elenco di nomi di connessione. Per ulteriori informazioni, consultare *Creazione di una factory di connessione per il provider dei messaggi IBM MQ*.

Per visualizzare o modificare le proprietà di configurazione di un factory di connessione:

- Utilizzare il pannello delle impostazioni della produzione connessioni della console di gestione per il tipo di produzione connessioni che si desidera configurare.

  Le proprietà di configurazione controllano il modo in cui vengono create le connessioni alle code e agli argomenti associati. Per ulteriori informazioni, consultare *Configurazione di una factory di raccolta per il provider di messaggistica IBM MQ*, *Configurazione di una factory di raccolta code per il provider di messaggistica IBM MQ*o *Configurazione di una factory di raccolta argomenti per il provider di messaggistica IBM MQ*.

Per configurare una destinazione coda JMS per la messaggistica point - to - point con il fornitore di messaggistica IBM MQ :

- Utilizzare il pannello delle impostazioni della coda del provider di messaggistica IBM MQ della console di gestione per definire i seguenti tipi di proprietà:
  - Proprietà generali, incluse le proprietà di gestione e delle code IBM MQ .

- Proprietà di connessione che specifica come connettersi al gestore code su cui è presente la coda.
- Proprietà avanzate che controllano il funzionamento delle connessioni effettuate alle destinazioni dei provider dei messaggi IBM MQ .
- Qualsiasi proprietà personalizzata per la destinazione della coda.

Per ulteriori informazioni, consultare *Configurazione di una coda per il provider di messaggistica IBM MQ*.

Per creare o configurare una destinazione argomenti JMS per la messaggistica di pubblicazione / sottoscrizione con il provider di messaggistica IBM MQ :

- Utilizzare il pannello di impostazioni dell'argomento del fornitore di messaggistica IBM MQ per definire i tipi di proprietà seguenti:
  - Proprietà generali, incluse le proprietà di amministrazione e IBM MQ .
  - Proprietà avanzate che controllano il funzionamento delle connessioni effettuate alle destinazioni dei provider dei messaggi IBM MQ .
  - Qualsiasi proprietà personalizzata per la destinazione della coda.

  Per ulteriori informazioni, consultare *Configurazione di un argomento per il provider di messaggistica IBM MQ*.

Concetti correlati

“Gestori code a più istanze” a pagina 475
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.

Attività correlate

“Configurazione di un formato binario CCDT” a pagina 42
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 Multiplatforms, una CCDT binaria contenente le impostazioni predefinite viene creata automaticamente quando viene creato il gestore code. Utilizzare il comando **runmqsc** per aggiornare una CCDT binaria.

“Configurazione della messaggistica di pubblicazione/sottoscrizione” a pagina 396
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.

WebSphere Application Server argomenti

Specifiche di attivazione del fornitore di messaggistica IBM MQ

Creazione di una specifica di attivazione per il provider di messaggistica IBM MQ

Configurazione di una specifica di attivazione per il provider di messaggistica IBM MQ

Creazione di una factory di connessione per il provider dei messaggi IBM MQ

Configurazione di una factory di connessione unificata per il provider di messaggistica IBM MQ

Configurazione di una factory di connessione code per il provider di messaggistica IBM MQ

Configurazione di una factory di connessione argomenti per il provider dei messaggi IBM MQ

Configurazione di una coda per il provider di messaggistica IBM MQ

Configurazione di un argomento per il provider di messaggistica IBM MQ

Configurazione delle risorse JMS utilizzando i comandi di script wsadmin

È possibile utilizzare i comandi di script WebSphere Application Server wsadmin per creare, modificare, eliminare o visualizzare informazioni sulle specifiche di attivazione JMS , sulle factory di connessione, sulle code e sugli argomenti. È inoltre possibile visualizzare e gestire le impostazioni per l'adattatore risorse IBM MQ .

Informazioni su questa attività

I seguenti passi forniscono una panoramica dei modi in cui è possibile utilizzare comandi WebSphere Application Server wsadmin per configurare le risorse JMS da utilizzare con il provider di messaggistica IBM MQ . Per ulteriori informazioni su come utilizzare questi comandi, consultare *Link correlati* per i link alla documentazione del prodotto WebSphere Application Server .

Per eseguire un comando, utilizzare l'oggetto AdminTask del client di script wsadmin.

Dopo aver utilizzato un comando per creare un nuovo oggetto o apportare modifiche, salvare le proprie modifiche alla configurazione principale. Ad esempio, utilizza il seguente comando:

```
AdminConfig.save()
```

Per visualizzare un elenco dei comandi di gestione del provider dei messaggi IBM MQ disponibili e una breve descrizione di ciascun comando, immettere il seguente comando dal prompt wsadmin:

```
print AdminTask.help('WMQAdminCommands')
```

Per visualizzare la guida di panoramica su un determinato comando, immettere il seguente comando nel prompt wsadmin:

```
print AdminTask.help('command_name')
```

Procedura

Per elencare tutte le risorse del provider dei messaggi IBM MQ definite nell'ambito in cui viene eseguito un comando, utilizzare i seguenti comandi.

- Per elencare le specifiche di attivazione, utilizzare il comando **listWMQActivationSpecs** .
- Per elencare le produzioni connessioni, utilizzare il comando **listWMQConnectionFactories** .
- Per elencare le destinazioni di tipo coda, utilizzare il comando **listWMQQueues** .
- Per elencare le destinazioni del tipo di argomento, utilizzare il comando **listWMQTopics** .

Per creare una risorsa JMS per il fornitore di messaggistica IBM MQ in un ambito specifico, utilizzare i seguenti comandi.

- Per creare una specifica di attivazione, utilizzare il comando **createWMQActivationSpec** .

  È possibile creare una specifica di attivazione specificando tutti i parametri da utilizzare per stabilire una connessione oppure è possibile creare la specifica di attivazione in modo che utilizzi una CCDT (client channel definition table) per individuare il gestore code a cui connettersi.
- Per creare una factory di connessione, utilizzare il comando **createWMQConnectionFactory** , utilizzando il parametro **-type** per specificare il tipo di factory di connessione che si desidera creare:
  - Se l'applicazione JMS è progettata per utilizzare solo la messaggistica point - to - point, creare una factory di connessione specifica del dominio per il dominio di messaggistica point - to - point che può essere utilizzato per creare connessioni specifiche per la messaggistica point - to - point.
  - Se l'applicazione JMS è progettata solo per utilizzare la messaggistica di pubblicazione / sottoscrizione, creare una factory di connessione specifica del dominio per il dominio di messaggistica di pubblicazione / sottoscrizione che può essere utilizzato per la creazione di connessioni specifiche per la messaggistica di pubblicazione / sottoscrizione.
  - Per JMS 1.1 o versioni successive, creare un factory di connessione indipendente dal dominio che può essere utilizzato sia per la messaggistica point-to-point che per la messaggistica di pubblicazione / sottoscrizione, consentendo all'applicazione di eseguire entrambe le operazioni point-to-point e di pubblicazione / sottoscrizione nella stessa transazione.

  Il tipo predefinito è factory di connessione indipendente dal dominio.
- Per creare una destinazione di tipo coda, utilizzare il comando **createWMQQueue** .

- Per creare una destinazione del tipo di argomento, utilizzare il comando **createWMQTopic** .

Per modificare una risorsa JMS per il fornitore di messaggistica IBM MQ in un ambito specifico, utilizzare i seguenti comandi.

- Per modificare una specifica di attivazione, utilizzare il comando **modifyWMQActivationSpec** .

  Non è possibile modificare il tipo di una specifica di attivazione. Ad esempio, non è possibile creare una specifica di attivazione in cui si immettono tutte le informazioni di configurazione manualmente e quindi modificarle per utilizzare una CCDT.
- Per modificare una factory di connessione, utilizzare il comando **modifyWMQConnectionFactory** .
- Per modificare una destinazione del tipo di coda, utilizzare il comando **modifyWMQQueue** .
- Per modificare una destinazione del tipo di argomento, utilizzare il comando **modifyWMQTopic** .

Per cancellare una risorsa JMS per il fornitore di messaggistica IBM MQ in un ambito specifico, utilizzare i seguenti comandi.

- Per cancellare una specifica di attivazione, utilizzare il comando **deleteWMQActivationSpec** .
- Per eliminare una factory di connessione, utilizzare il comando **deleteWMQConnectionFactory** .
- Per eliminare una destinazione di tipo coda, utilizzare il comando **deleteWMQQueue** .
- Per cancellare una destinazione di tipo argomento, utilizzare il comando **deleteWMQTopic** .

Per visualizzare informazioni su una specifica risorsa del fornitore di messaggistica IBM MQ , utilizzare i seguenti comandi.

- Per visualizzare tutti i parametri e i relativi valori associati a una particolare specifica di attivazione, utilizzare il comando **showWMQActivationSpec** .
- Per visualizzare tutti i parametri ed i relativi valori associati ad un determinato factory di connessione, utilizzare il comando **showWMQConnectionFactory** .
- Per visualizzare tutti i parametri e i relativi valori associati a una particolare destinazione del tipo di coda, utilizzare il comando **showWMQQueue** .
- Per visualizzare tutti i parametri e i relativi valori associati a una destinazione di tipo argomento, utilizzare il comando **deleteWMQTopic** .

Per gestire le impostazioni per l'adattatore di risorse IBM MQ o per il provider di messaggistica IBM MQ , utilizzare i seguenti comandi.

- Per gestire le impostazioni dell'adattatore di risorse IBM MQ installato in un particolare ambito, utilizzare il comando **manageWMQ** .
- Per visualizzare tutti i parametri e i relativi valori che possono essere impostati dal comando **manageWMQ** , utilizzare il comando **showWMQ** . Queste impostazioni sono correlate all'adattatore di risorse IBM MQ o al fornitore di messaggistica IBM MQ . Il comando **showWMQ** mostra anche le proprietà personalizzate impostate sull'adattatore di risorse IBM MQ .

Concetti correlati

“Gestori code a più istanze” a pagina 475
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.

Attività correlate

“Configurazione di un formato binario CCDT” a pagina 42
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 Multiplatforms, una CCDT binaria contenente le impostazioni predefinite viene creata automaticamente quando viene creato il gestore code. Utilizzare il comando **runmqsc** per aggiornare una CCDT binaria.

“Configurazione della messaggistica di pubblicazione/sottoscrizione” a pagina 396
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.

WebSphere Application Server argomenti
createWMQActivationSpec comando
createWMQConnectionFactory comando
createWMQQueue comando
createWMQTopic comando
deleteWMQActivationSpec comando
deleteWMQConnectionFactory comando
deleteWMQQueue comando
deleteWMQTopic comando
listWMQActivationSpecs comando
listWMQConnectionFactories comando
listWMQQueues comando
listWMQTopics comando
modifyWMQActivationSpec comando
modifyWMQConnectionFactory comando
modifyWMQQueue comando
modifyWMQTopic comando
showWMQActivationSpec comando
showWMQConnectionFactory comando
showWMQQueue comando
showWMQTopic comando
showWMQ comando
manageWMQ comando

Utilizzo delle sottoscrizioni condivise JMS 2.0

In WebSphere Application Server traditional 9.0, puoi configurare e utilizzare le sottoscrizioni condivise JMS 2.0 con IBM MQ 9.0.

Informazioni su questa attività

La specificazione JMS 2.0 ha introdotto il concetto di sottoscrizioni condivise, che consente a una singola sottoscrizione di essere aperta da uno o più consumer. I messaggi sono condivisi tra tutti questi consumatori. Non vi è alcuna limitazione quando questi consumer sono così lunghi che si connettono allo stesso gestore code.

Le sottoscrizioni condivise possono essere durevoli o non durevoli, con la stessa semantica di quelle a cui ora si fa riferimento come sottoscrizioni non condivise.

Per consentire a un utente di identificare quale sottoscrizione utilizzare, è necessario fornire un nome sottoscrizione. È simile alle sottoscrizioni durevoli non condivise, ma è richiesto un nome di sottoscrizione in tutti i casi in cui è richiesta una sottoscrizione condivisa. Un clientID, tuttavia, non è richiesto nel caso di una sottoscrizione condivisa durevole; può essere fornito ma non è obbligatorio.

Mentre le sottoscrizioni condivise possono essere considerate come un meccanismo di bilanciamento del carico, né in IBM MQ né nella specifica JMS 2.0 vi è alcun impegno su come i messaggi vengono distribuiti tra i consumatori.

In WebSphere Application Server traditional 9.0 è preinstallato un adattatore di risorse IBM MQ 9.0 .

La seguente procedura mostra come configurare una specifica di attivazione per utilizzare una sottoscrizione condivisa durevole o non durevole utilizzando la console di gestione WebSphere Application Server traditional .

Procedura

Creare prima gli oggetti in JNDI.

1. Creare una destinazione argomenti in JNDI come di consueto (consultare "Configurazione delle risorse JMS utilizzando la console di gestione" a pagina 647).
2. Creare la specifica di attivazione (consultare "Configurazione delle risorse JMS utilizzando la console di gestione" a pagina 647).

   È possibile creare la specifica di attivazione con esattamente le proprietà necessarie. Se si desidera utilizzare una sottoscrizione durevole, è possibile selezionarla al momento della creazione e specificare un nome. Se si desidera utilizzare una sottoscrizione non durevole, non è possibile specificare un nome a questo punto. Invece, è necessario creare una proprietà personalizzata per il nome della sottoscrizione.

Aggiornare la specifica di attivazione creata con le proprietà personalizzate richieste. Potrebbero essere necessarie due proprietà personalizzate:

- In tutti i casi, è necessario creare una proprietà personalizzata per specificare che questa specifica di attivazione deve utilizzare una sottoscrizione condivisa.
- Se la sottoscrizione è stata creata come non durevole, la proprietà del nome della sottoscrizione deve essere impostata come proprietà personalizzata.

La seguente tabella mostra il valore valido che è possibile specificare per ciascuna proprietà personalizzata:

Nome proprietà	Tipo	Valori validi
sharedSubscription	Stringa	true, false
subscriptionName	Stringa	Stringa java di lunghezza diversa da zero

3. Selezionare la specifica di attivazione dall'elenco visualizzato nel modulo **Raccolta specifica di attivazione** .

   I dettagli per la specifica di attivazione vengono visualizzati nel modulo **Impostazioni della specifica di attivazione del fornitore di messaggistica IBM MQ** .
4. Nel modulo **IBM MQ** , fare clic su **Proprietà personalizzate**.

   Viene visualizzato il modulo **Proprietà personalizzate** .
5. Se si utilizza una sottoscrizione non durevole, creare la proprietà personalizzata subscriptionName .

   Sul pannello **Proprietà personalizzate** della specifica di attivazione, fare clic su **Nuovo**, quindi immettere i seguenti dettagli:

   Nome

   Il nome della proprietà personalizzata, che in questo caso è `subscriptionName`.

   Valore

   Il valore della proprietà personalizzata. È possibile utilizzare i nomi JNDI nel campo **Valore** , ad esempio `WASSharedSub0ne`.

   Tipo

   Il tipo di proprietà personalizzata. Selezionare il tipo di proprietà personalizzata dall'elenco, che in questo caso deve essere `java.lang.String`.
6. Per una sottoscrizione durevole e non durevole condivisa, creare la proprietà personalizzata sharedSubscription .

   Sul pannello **Proprietà personalizzate** della specifica di attivazione, fare clic su **Nuovo**, quindi immettere i seguenti dettagli:

   Nome

   Il nome della proprietà personalizzata, che in questo caso è `sharedSubscription`.

Valore

Il valore della proprietà personalizzata. Per specificare che la specifica di attivazione utilizza una sottoscrizione condivisa, impostare il valore su `true`. Se in seguito si desidera interrompere l'utilizzo di una sottoscrizione condivisa per questa specifica di attivazione, è possibile farlo impostando il valore di questa proprietà personalizzata su `false`.

Tipo

Il tipo di proprietà personalizzata. Selezionare il tipo di proprietà personalizzata dall'elenco, che in questo caso deve essere `java.lang.String`.

7. Quando le proprietà sono impostate, riavviare il server di applicazioni.

   I bean basati sui messaggi (MDB) per le specifiche di attivazione vengono guidati quando arrivano i messaggi, ma solo gli MDB condividono i messaggi inviati.

Concetti correlati

Sottoscrizioni clonate e condivise

Durata sottoscrizione

Attività correlate

Configurazione dell'adattatore di risorse per la comunicazione in entrata

Informazioni correlate per WebSphere Application Server traditional 9.0

Configurazione di un argomento per il provider di messaggistica IBM MQ

Specifiche di attivazione del fornitore di messaggistica IBM MQ

Creazione di una specifica di attivazione per il provider di messaggistica IBM MQ

Configurazione di una specifica di attivazione per il provider di messaggistica IBM MQ

Configurazione delle proprietà personalizzate per le risorse del IBM MQ provider di messaggistica JMS

Utilizzo delle proprietà JMS 2.0 ConnectionFactory e Destination Lookup

In WebSphere Application Server traditional 9.0, le proprietà ConnectionFactoryLookup e DestinationLookup di una specifica di attivazione possono essere fornite con un nome JNDI di un oggetto gestito da utilizzare come preferenza rispetto alle altre proprietà della specifica di attivazione.

Informazioni su questa attività

La specifica JMS 2.0 specifica due proprietà aggiuntive sulla specifica di attivazione utilizzata per guidare MDB (message - driven bean). In precedenza, ogni fornitore doveva specificare le proprietà personalizzate nella specifica di attivazione per fornire i dettagli richiesti per la connessione a un sistema di messaggistica e per definire la destinazione da cui ottenere i messaggi.

Le proprietà connectionFactoryLookup e destinationLookup ora standard possono essere utilizzate per fornire un JNDI nome dell'oggetto pertinente da cercare e utilizzare. All'interno di WebSphere Application Server traditional 9.0 un adattatore risorse IBM MQ 9.0 è preinstallato.

La seguente procedura mostra come personalizzare e utilizzare queste due proprietà utilizzando la console di gestione WebSphere Application Server traditional .

Procedura

Creare prima gli oggetti in JNDI.

1. Creare ConnectionFactory in JNDI come di consueto (consultare “Configurazione delle risorse JMS utilizzando la console di gestione” a pagina 647).
2. Creare la destinazione in JNDI come normale (consultare “Configurazione delle risorse JMS utilizzando la console di gestione” a pagina 647).

   L'oggetto Destinazione deve avere i valori corretti.
3. Creare la specifica di attivazione utilizzando i valori necessari (consultare “Configurazione delle risorse JMS utilizzando la console di gestione” a pagina 647).

È possibile creare la specifica di attivazione con esattamente le proprietà necessarie. Tuttavia, è necessario tenere presente le seguenti considerazioni:

- Se si desidera che l'adattatore di risorse IBM MQ utilizzi le proprietà di ricerca della destinazione e della factory di connessione Java EE , è meno rilevante quali proprietà vengono utilizzate quando si crea la specifica di attivazione (consultare ActivationSpec ConnectionFactoryLookup e DestinationLookup properties).
- Tuttavia, qualsiasi proprietà che non sia già definita sul factory di connessione o sulla destinazione deve essere ancora specificata sulla specifica di attivazione. Pertanto, è necessario definire le proprietà del consumer della connessione e le proprietà aggiuntive e le informazioni di autenticazione utilizzate quando viene effettivamente creata una connessione.
- Delle proprietà definite sul factory di connessione, la proprietà ClientID ha un'elaborazione speciale. Ciò si verifica perché uno scenario comune utilizza un singolo factory di connessione con più specifiche di attivazione. Ciò semplifica la gestione, tuttavia la specifica JMS richiede ID client univoci, pertanto la specifica di attivazione deve avere la possibilità di sovrascrivere qualsiasi valore impostato in ConnectionFactory. Se non viene impostato alcun ClientID sulla specifica di attivazione, viene utilizzato qualsiasi valore sul factory di connessione.

Aggiornare la specifica di attivazione creata con le due nuove proprietà personalizzate utilizzando la console di gestione WebSphere Application Server come descritto nel passo “4” a pagina 655oppure utilizzare le annotazioni come descritto nel passo “5” a pagina 655.

4. Aggiornare la specifica di attivazione nella console di gestione WebSphere Application Server .

   Queste due proprietà devono essere impostate nel pannello delle proprietà personalizzate della specifica di attivazione. Queste proprietà non sono presenti nei pannelli principali della specifica di attivazione o nella procedura guidata di creazione della specifica di attivazione.

   a) Selezionare la specifica di attivazione dall'elenco visualizzato nel modulo **Raccolta specifica di attivazione** .

      I dettagli per la specifica di attivazione vengono visualizzati nel modulo **Impostazioni della specifica di attivazione del fornitore di messaggistica IBM MQ** .

   b) Nel modulo **IBM MQ** , fare clic su **Proprietà personalizzate**.

      Viene visualizzato il modulo **Proprietà personalizzate** .

   c) Nel modulo **Proprietà personalizzate** , creare due nuove proprietà personalizzate, di tipo java.lang.String.

      In ogni caso, fare clic su **Nuovo** , quindi immettere i dettagli seguenti per la proprietà personalizzata:

      Nome

      Il nome della proprietà personalizzata, `connectionFactoryLookup` o `destinationLookup`.

      Valore

      Il valore della proprietà personalizzata. È possibile utilizzare i nomi JNDI nel campo **Valore** , ad esempio `QuoteCF` e `QuoteQ`.

      Tipo

      Il tipo di proprietà personalizzata. Selezionare il tipo di proprietà personalizzata dall'elenco, che in questo caso deve essere `java.lang.String`.

   L'MDB distribuito utilizzerà questi valori per creare la factory di connessione e la destinazione. Quando si distribuisce l'MDB, non è necessario impostare la configurazione del valore JNDI .

5. Utilizzare le annotazioni invece della specifica di attivazione.

   È possibile utilizzare le annotazioni nel codice MDB per specificare anche i valori. Ad esempio, utilizzando JNDI names `QuoteCF` e `QuoteQ`, il codice è simile al seguente:

```
@MessageDriven(activationConfig = {
        @ActivationConfigProperty(propertyName =  "destinationType" , propertyValue =
"javax.jms.Topic" ),
        @ActivationConfigProperty(propertyName =  "destinationLookup" , propertyValue =
"QuoteQ" ),
```

```
        @ActivationConfigProperty(propertyName =  "connectionFactoryLookup" , propertyValue
=  "QuoteCF" )}, mappedName =  "LookupMDB" )
        @TransactionAttribute(TransactionAttributeType.REQUIRED)
        @TransactionManagement(TransactionManagementType.CONTAINER)
        publicclass LookupMDB implements MessageListener {
```

Attività correlate

Configurazione dell'adattatore di risorse per la comunicazione in entrata

Informazioni correlate per WebSphere Application Server traditional 9.0

Configurazione di una factory di connessione unificata per il provider di messaggistica IBM MQ

Configurazione di un argomento per il provider di messaggistica IBM MQ

Specifiche di attivazione del fornitore di messaggistica IBM MQ

Creazione di una specifica di attivazione per il provider di messaggistica IBM MQ

Configurazione di una specifica di attivazione per il provider di messaggistica IBM MQ

Configurazione delle proprietà personalizzate per le risorse del IBM MQ provider di messaggistica JMS

Configurazione del server delle applicazioni per utilizzare il livello di manutenzione dell'adattatore di risorse più recente

Per garantire che l'adattatore di risorse IBM MQ venga aggiornato automaticamente all'ultimo livello di manutenzione disponibile quando si applicano i fix pack WebSphere Application Server , è possibile configurare tutti i server nel proprio ambiente per utilizzare la versione più recente dell'adattatore di risorse contenuto nel fix pack WebSphere Application Server applicato all'installazione di ciascun nodo.

Prima di iniziare

Importante: Se si sta utilizzando WebSphere Application Server 8.5 o versioni precedenti su qualsiasi piattaforma, non installare l'adattatore di risorse IBM MQ 8.0 o versioni successive nel server delle applicazioni. L'adattatore di risorse IBM MQ 8.0 o successivo può essere distribuito solo in un server delle applicazioni che supporta JMS 2.0. Tuttavia, WebSphere Application Server 8.5 o versioni precedenti supporta solo JMS 1.1. Queste versioni di WebSphere Application Server vengono con l'adattatore di risorse IBM WebSphere MQ 7.0 , che può essere utilizzato per connettersi a un gestore code IBM MQ 8.0 utilizzando il trasporto BINDINGS o CLIENT.

Informazioni su questa attività

Utilizzare questa attività se una delle seguenti circostanze si applica alla configurazione e si desidera configurare tutti i server nel proprio ambiente per utilizzare la versione più recente dell'adattatore di risorse IBM MQ :

- I log JVM di qualsiasi server delle applicazioni nel proprio ambiente mostrano le seguenti informazioni sulla versione dell'adattatore di risorse IBM MQ dopo che è stato applicato WebSphere Application Server 7.0 Fix Pack 1 o successivo:

  ```
  WMSG1703I:RAR versione di implementazione 7.0.0.0-k700-L080820
  ```

- I log JVM di qualsiasi server delle applicazioni nel proprio ambiente contengono la seguente voce:

  ```
  WMSG1625E: Non è stato possibile rilevare
  il codice provider di messaggistica IBM MQ nel percorso specificato < null>
  ```

- Uno o più nodi sono stati precedentemente aggiornati manualmente per utilizzare un livello di manutenzione specifico dell'adattatore di risorse IBM MQ che è ora sostituito dalla versione più recente dell'adattatore di risorse contenuto nel livello di manutenzione WebSphere Application Server corrente.

La directory *profile_root* a cui fanno riferimento gli esempi è la directory home per il profilo WebSphere Application Server , ad esempio `C:\Program Files\IBM\WebSphere\AppServer1`.

Una volta eseguita la seguente procedura per tutte le celle e le installazioni di un singolo server nel proprio ambiente, i server ricevono automaticamente la manutenzione per l'adattatore di risorse IBM MQ quando viene applicato un nuovo fix pack WebSphere Application Server .

Procedura

1. Avviare il server delle applicazioni. Se il profilo fa parte di una configurazione di distribuzione di rete, avviare il gestore distribuzione e tutti gli agent del nodo. Se il profilo contiene un agent di gestione, avviare l'agent di gestione.
2. Verificare il livello di manutenzione dell'adattatore di risorse IBM MQ .
   a) Aprire una finestra del prompt dei comandi e passare alla directory *profile_root*\bin .

      Ad esempio, immettere `cd C:\Program Files\IBM\WebSphere\AppServer1\bin`.

   b) Avviare lo strumento wsadmin immettendo `wsadmin.bat -lang jython`, quindi, se richiesto, immettere il nome utente e la password.

   c) Immettere il comando riportato di seguito e premere due volte Invio:

```
wmqInfoMBeansUnsplit = AdminControl.queryNames("WebSphere:type=WMQInfo,*")
wmqInfoMBeansSplit = AdminUtilities.convertToList(wmqInfoMBeansUnsplit)
for wmqInfoMBean in wmqInfoMBeansSplit: print wmqInfoMBean; print AdminControl.invoke(wmqInfoMBean,
'getInfo', '')
```

      È possibile eseguire questo comando anche in Jacl. Per ulteriori informazioni su come effettuare questa operazione, consultare *Verifica che i server utilizzino il livello di manutenzione dell'adattatore di risorse IBM MQ disponibile più recente* nella documentazione del prodotto WebSphere Application Server .

   d) Individuare il messaggio `WMSG1703I` nell'emissione visualizzata dal comando e controllare il livello dell'adattatore risorse.

      Ad esempio, per WebSphere Application Server 7.0.1 Fix Pack 5 il messaggio deve essere:

      ```
      WMSG1703I: Versione implementazione RAR 7.0.1.3-k701-103-100812
      ```

      Questo messaggio indica che la versione è 7.0.1.3-k701-103-100812, che è il corretto livello dell'adattatore di risorse per questo fix pack. Tuttavia, se viene visualizzato il seguente messaggio, ciò significa che è necessario regolare l'adattatore di risorse al livello corretto di manutenzione per il Fix Pack 15.

      ```
      WMSG1703I: Versione implementazione RAR 7.0.0.0-k700-L080820
      ```

3. Copiare il seguente script Jython in un file denominato `convertWMQRA.py`, quindi salvarlo nella directory root del profilo, ad esempio `C:\Program Files\IBM\WebSphere\AppServer1\bin`.

```
ras = AdminUtilities.convertToList(AdminConfig.list('J2CResourceAdapter'))

for ra in ras :
  desc = AdminConfig.showAttribute(ra, "description")
  if (desc == "WAS 7.0 Built In IBM MQ Resource Adapter") or (desc == "WAS 7.0.0.1 Built In IBM MQ
Resource Adapter"):
    print "Updating archivePath and classpath of " + ra
    AdminConfig.modify(ra, [['archivePath', "${WAS_INSTALL_ROOT}/installedConnectors/wmq.jmsra.rar"]])
    AdminConfig.unsetAttributes(ra, ['classpath'])
    AdminConfig.modify(ra, [['classpath', "${WAS_INSTALL_ROOT}/installedConnectors/wmq.jmsra.rar"]])
    AdminConfig.save()
  #end if
#end for
```

   Suggerimento: Quando si salva il file, assicurarsi che sia salvato come file python piuttosto che come file di testo.

4. Utilizzare lo strumento wsadmin WebSphere Application Server per eseguire lo script Jython appena creato.

   Aprire un prompt dei comandi e passare alla directory `\bin` nella directory home per la directory WebSphere Application Server, ad esempio `C:\Program Files\IBM\WebSphere\AppServer1\bin` , quindi immettere il seguente comando e premere Invio:

   ```
   wsadmin -lang jython -f convertWMQRA.py
   ```

   Se richiesto, immettere il nome utente e la password.

Nota: Se si esegue lo script su un profilo che fa parte di una configurazione di distribuzione di rete, lo script aggiorna tutti i profili che devono essere aggiornati in tale configurazione. Una risincronizzazione completa potrebbe essere necessaria se si hanno incongruenze del file di configurazione preesistente.

5. Se si è in esecuzione in una configurazione di distribuzione di rete, assicurarsi che gli agent del nodo siano completamente risincronizzati. Per ulteriori informazioni, consultare la sezione Sincronizzazione dei nodi mediante lo strumento di script wsadmin o Aggiunta, gestione e rimozione di nodi.
6. Arrestare tutti i server nel profilo. Se il profilo fa parte di una configurazione di distribuzione di rete, arrestare anche tutti i membri del cluster nella configurazione, arrestare tutti gli agent del nodo nella configurazione e arrestare il gestore distribuzione. Se il profilo contiene un agent di gestione, arrestarlo.
7. Eseguire il comando **osgiCfgInit** dalla directory *profile_root*/bin .

   Il comando osgiCfgInit reimposta la cache delle classi utilizzata dall'ambiente di runtime OSGi. Se il profilo fa parte di una configurazione di distribuzione di rete, eseguire il comando **osgiCfgInit** dalla directory profile_root/bin di ogni profilo che è parte della configurazione.
8. Riavviare tutti i server nel profilo. Se il profilo fa parte di una configurazione di distribuzione di rete, riavviare anche tutti i membri del cluster nella configurazione, riavviare tutti gli agent del nodo nella configurazione e riavviare il gestore distribuzione. Se il profilo contiene un agent di gestione, riavviarlo.
9. Ripetere il passo 2 per controllare che l'adattatore risorse sia ora al livello corretto.

Operazioni successive

Se si continuano a riscontrare dei problemi dopo aver eseguito i passi descritti in questo argomento ed è stato precedentemente utilizzato il pulsante **Aggiorna adattatore risorse** nel pannello JMS Impostazioni provider nella console di gestione WebSphere Application Server per aggiornare l'adattatore risorse IBM MQ su qualsiasi nodo nel proprio ambiente, è possibile che si stia verificando il problema descritto in APAR PM10308.

Attività correlate

Utilizzo dell'adattatore di risorse IBM MQ

Informazioni correlate per WebSphere Application Server 8.5.5

Verifica che i server utilizzino il livello di manutenzione dell'adattatore di risorse IBM MQ più recente disponibile

Sincronizzazione dei nodi mediante lo strumento di script wsadmin

Aggiunta, gestione e rimozione di nodi

JMS Impostazioni provider

Configurazione della proprietà JMS PROVIDERVERSION

Il provider di messaggistica IBM MQ ha tre modalità operative: modalità normale, modalità normale con limitazioni e modalità di migrazione. È possibile impostare la proprietà JMS **PROVIDERVERSION** per selezionare quali di queste modalità un'applicazione JMS utilizza per pubblicare e sottoscrivere.

Informazioni su questa attività

La selezione della modalità operativa del provider di messaggistica IBM MQ può essere controllata principalmente impostando la proprietà della factory di connessione PROVIDERVERSION. La modalità di funzionamento può essere selezionata automaticamente anche se non è stata specificata una modalità.

La proprietà **PROVIDERVERSION** differenzia tra le tre modalità operative del provider di messaggistica IBM MQ :

Modalità normale del provider di messaggistica IBM MQ
La modalità normale utilizza tutte le funzioni di un gestore code IBM MQ per implementare JMS. Questa modalità è ottimizzata per utilizzare la API e la funzionalità JMS 2.0.

Modalità normale del provider di messaggistica IBM MQ con restrizioni
La modalità normale con limitazioni utilizza l'API JMS 2.0 , ma non le nuove funzioni, ossia le sottoscrizioni condivise, la consegna ritardata e l'invio asincrono.

Modalità di migrazione del provider di messaggistica IBM MQ
Con la modalità di migrazione, è possibile connettersi a un gestore code IBM MQ 8.0 o successivo, ma non viene utilizzata alcuna delle funzioni di un gestore code IBM WebSphere MQ 7.0 o successivo, come la lettura anticipata e lo streaming.

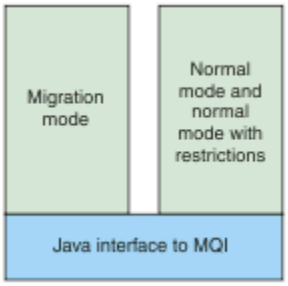


Figura 91. Modalità del provider di messaggistica

Procedura

Per configurare la proprietà **PROVIDERVERSION** per una specifica factory di connessione:

- Per configurare la proprietà **PROVIDERVERSION** utilizzando IBM MQ Explorer, fare riferimento a Configurazione di gestori code e oggetti.
- Per configurare la proprietà **PROVIDERVERSION** utilizzando lo strumento di gestione JMS , fare riferimento a Configurazione di gestori code e oggetti.
- Per configurare la proprietà **PROVIDERVERSION** in un'applicazione JMS utilizzando le estensioni IBM JMS o IBM MQ JMS , consultareCreazione e configurazione di factory di connessione e destinazioni in un'applicazione IBM MQ classes for JMS.

Per sovrascrivere le impostazioni della modalità del provider del factory di connessione per tutte le factory di connessione nella JVM:

- Per sovrascrivere le impostazioni della modalità del provider del factory di connessione, utilizzare la proprietà `com.ibm.msg.client.wmq.overrideProviderVersion`

  Se non è possibile modificare la factory di connessione che si sta utilizzando, è possibile utilizzare la proprietà `com.ibm.msg.client.wmq.overrideProviderVersion` per sovrascrivere qualsiasi impostazione sulla factory di connessione. Questa sovrascrittura si applica a tutte le factory di connessione della JVM, ma gli oggetti factory di connessione effettivi non vengono modificati.

Concetti correlati
Proprietà delle factory di connessione
Attività correlate
Risoluzione dei problemi relativi alla versione del provider JMS
Riferimenti correlati
PROVIDERVERSION
Dipendenze tra proprietà di oggetti IBM MQ classes for JMS

Modalità operative del provider di messaggistica IBM MQ

È possibile selezionare la modalità operativa del provider di messaggistica IBM MQ che un'applicazione JMS utilizza per pubblicare e sottoscrivere impostando la proprietà PROVIDERVERSION per la factory di connessione sul valore appropriato. In alcuni casi, la proprietà PROVIDERVERSION è impostata come non specificata, nel cui caso il client JMS utilizza un algoritmo per stabilire quale modalità di operazione utilizzare.

PROVIDERVERSION Valori proprietà

È possibile impostare la proprietà **PROVIDERVERSION** del factory di connessione su uno qualsiasi dei seguenti valori:

8 - Modalità normale
L'applicazione JMS utilizza la modalità normale. Questa modalit ... utilizza le funzioni di un gestore code IBM MQ per implementare JMS.

7 - Modalità normale con restrizioni
L'applicazione JMS utilizza la modalità normale con limitazioni. Questa modalità utilizza l'API JMS 2.0, ma non le nuove funzioni quali le sottoscrizioni condivise, il recapito ritardato o l'invio asincrono.

6 - modalità di migrazione
L'applicazione JMS utilizza la modalità di migrazione. In modalità migrazione, IBM MQ classes for JMS utilizza funzioni e algoritmi simili a quelli forniti con IBM WebSphere MQ 6.0.

non `specificato` (il valore predefinito)
Il client JMS utilizza un algoritmo per stabilire quale modalità di funzionamento viene utilizzata.

Il valore che si specifica per la proprietà **PROVIDERVERSION** deve essere una stringa. Se si specifica una delle opzioni 8, 7 o 6, è possibile farlo in uno qualsiasi dei seguenti formati:

- V.R.M.F
- V.R.M
- V.R
- V

dove V, R, M e F sono numeri interi maggiori o uguali a zero. Gli ulteriori valori R, M ed F sono facoltativi e sono disponibili per l'utilizzo qualora sia necessario un controllo più preciso. Ad esempio, se si desidera utilizzare un livello **PROVIDERVERSION** di 7, è possibile impostare **PROVIDERVERSION** = 7, `7.0`, `7.0.0` o `7.0.0.0`.

Tipi di oggetto factory di connessione

È possibile impostare la proprietà **PROVIDERVERSION** per i seguenti tipi di oggetto factory di connessione:

- MQConnectionFactory
- Factory di MQQueueConnection
- Factory MQTopicConnection
- MQXAConnectionFactory
- Factory MQXAQueueConnection
- Factory MQXAQueueConnection
- Factory MQXAQueueConnection
- Factory MQXATopicConnection

Per ulteriori informazioni su questi diversi tipi di factory di connessione, consultare “Configurazione di oggetti JMS utilizzando lo strumento di gestione” a pagina 637.

Concetti correlati
Provider di messaggistica IBM MQ

PROVIDERVERSION Modalità normale

La modalità normale utilizza tutte le funzioni di un gestore code IBM MQ per implementare JMS. Questa modalità è ottimizzata per utilizzare la API e la funzionalità JMS 2.0.

Il seguente diagramma di flusso mostra i controlli eseguiti dal client JMS per stabilire se è possibile creare una connessione in modalità normale.

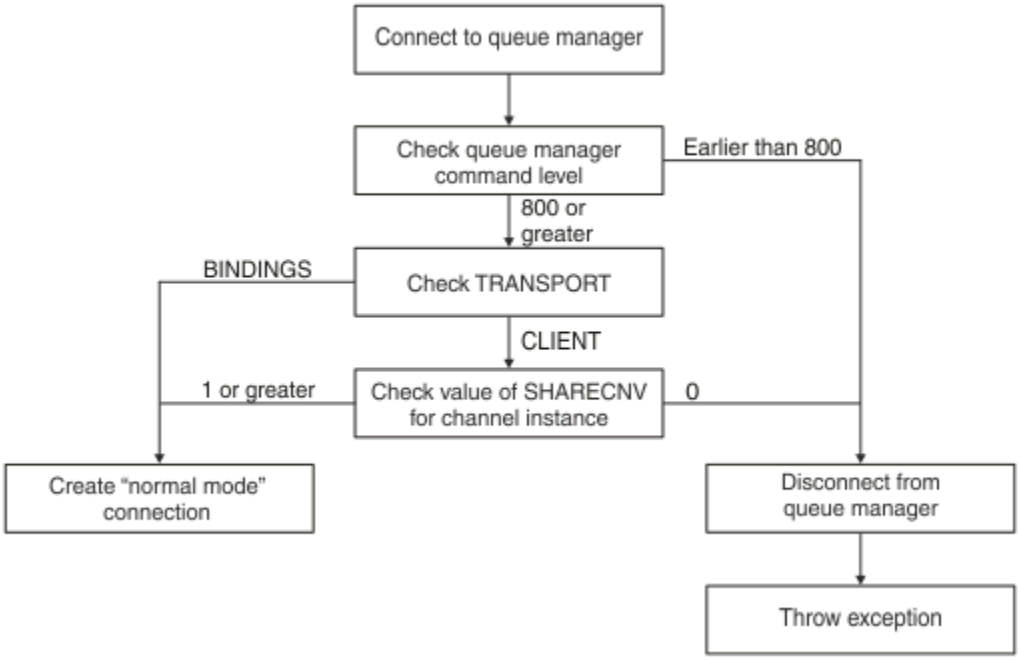


Figura 92. Modalità normale PROVIDERVERSION

Se il gestore code specificato nelle impostazioni del factory di connessione ha un livello di comando pari o superiore a 800 e la proprietà **TRANSPORT** del factory di connessione è impostata su BINDINGS, viene creata una connessione in modalità normale senza controllare ulteriori proprietà.

Se il gestore code specificato nelle impostazioni del factory di connessione ha un livello di comando di 800 o superiore e la proprietà **TRANSPORT** è impostata su CLIENT, viene controllata anche la proprietà **SHARECNV** sul canale di connessione del server. Questo controllo è necessario perché la modalità normale del provider di messaggistica di IBM MQ utilizza la funzione di condivisione delle conversazioni. Pertanto, affinché un tentativo di connessione in modalità normale abbia esito positivo, la proprietà **SHARECNV** , che controlla il numero di conversazioni che possono essere condivise, deve avere un valore pari o superiore a 1.

Se tutti i controlli mostrati nel diagramma di flusso hanno esito positivo, viene creata una connessione in modalità normale al gestore code e tutte le funzioni e l'API JMS 2.0 , ovvero l'invio asincrono, la consegna ritardata e la sottoscrizione condivisa, possono essere utilizzate.

Un tentativo di creare una connessione in modalità normale non è riuscito per uno dei seguenti motivi:

- Il gestore code specificato nelle impostazioni della factory di connessione ha un livello di comando precedente a 800. In questo caso, il metodo `createConnection` non riesce con un'eccezione `JMSFMQ0003`.
- La proprietà **SHARECNV** sul canale di connessione server è impostata su `0`. Se questa proprietà non ha un valore di 1 o superiore, il metodo `createConnection` non riesce con un'eccezione `JMSCC5007`.

Informazioni correlate

Dipendenze tra proprietà di oggetti IBM MQ classes for JMS
DEFINE CHANNEL (SHARECNV proprietà)
TRANSPORT

PROVIDERVERSION modalità normale con limitazioni

La modalità normale con limitazioni utilizza l'API JMS 2.0 , ma non le nuove funzioni IBM MQ 8.0 o successive come le sottoscrizioni condivise, la consegna ritardata o l'invio asincrono.

Il seguente diagramma di flusso mostra i controlli eseguiti dal client JMS per determinare se è possibile creare una modalità normale con restrizioni di connessione.

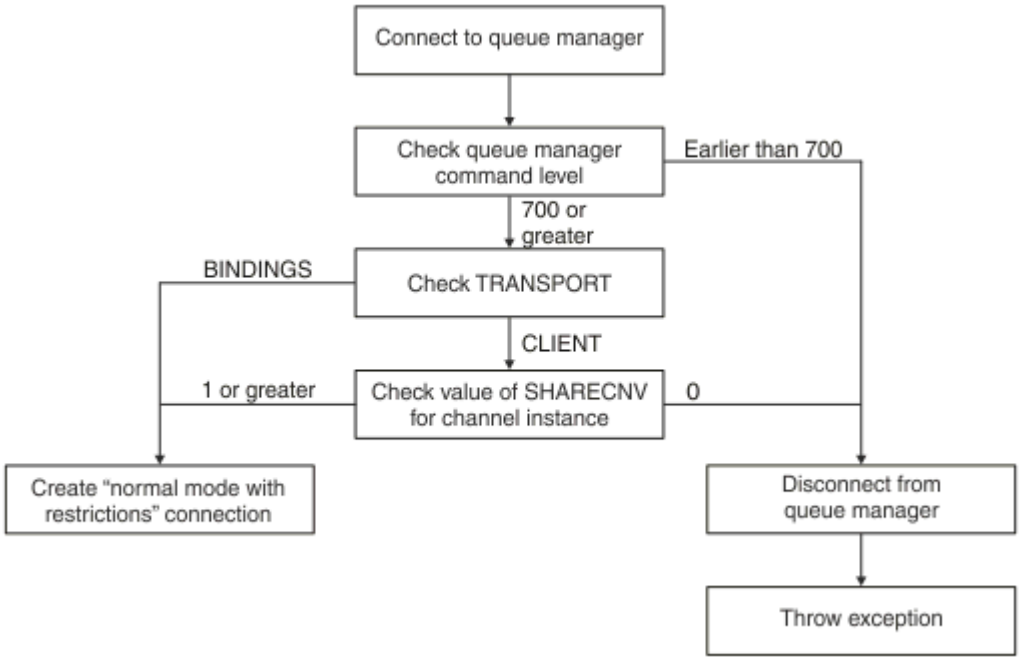


Figura 93. Modalità normale PROVIDERVERSION con restrizioni

Se il gestore code specificato nelle impostazioni della factory di connessione ha un livello di comando pari o superiore a 700 e la proprietà **TRANSPORT** della factory di connessione è impostata su BINDINGS, viene creata una connessione in modalità normale senza controllare ulteriori proprietà.

Se il gestore code specificato nelle impostazioni della factory di connessione ha un livello di comando di 700 o superiore e la proprietà **TRANSPORT** è impostata su CLIENT, viene controllata anche la proprietà **SHARECNV** sul canale di connessione del server. Questa verifica è necessaria perché la modalità normale del provider di messaggistica IBM MQ con limitazioni utilizza la funzionalità di condivisione delle conversazioni. Pertanto, per un normale tentativo di connessione in modalità normale con limitazioni, la proprietà **SHARECNV** , che controlla il numero di conversazioni che possono essere condivise, deve avere un valore pari o superiore a 1.

Se tutti i controlli mostrati nel diagramma di flusso hanno esito positivo, viene creata una modalità normale con restrizioni per la connessione al gestore code ed è quindi possibile utilizzare l'API JMS 2.0 , ma non le funzioni di invio asincrono, di consegna ritardata o di sottoscrizione condivisa.

Un tentativo di creare una modalità normale con restrizioni di connessione non riesce per uno dei seguenti motivi:

- Il gestore code specificato nelle impostazioni della factory di connessione ha un livello di comando precedente a 700. In questo caso, il metodo `createConnection` ha esito negativo con eccezione `JMSFCC5008`.
- La proprietà **SHARECNV** sul canale di connessione server è impostata su `0`. Se questa proprietà non ha un valore di `1` o superiore, il metodo `createConnection` non riesce con un'eccezione `JMSCC5007`.

Informazioni correlate

Dipendenze tra proprietà di oggetti IBM MQ classes for JMS
DEFINE CHANNEL (SHARECNV proprietà)
TRANSPORT

Modalità di migrazione PROVIDERVERSION

Per la modalità di migrazione, IBM MQ classes for JMS utilizza funzioni e algoritmi simili a quelli forniti con IBM WebSphere MQ 6.0, come la pubblicazione / sottoscrizione accodata, la selezione implementata sul lato client, i canali non multiplex e il polling utilizzato per implementare i listener.

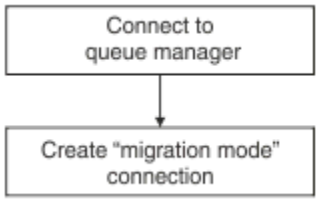


Figura 94. Modalità di migrazione PROVIDERVERSION

Se si desidera connettersi a WebSphere Message Broker 6.0 o a 6.1 utilizzando IBM MQ Enterprise Transport 6.0, è necessario utilizzare la modalità di migrazione.

È possibile connettersi a un gestore code IBM MQ 8.0 utilizzando la modalità di migrazione, ma nessuna delle nuove funzionalità di un gestore code IBM MQ classes for JMS viene utilizzata, ad esempio la lettura anticipata o lo streaming. Se un client IBM MQ 8.0 o successivo si connette a un gestore code IBM MQ 8.0 o successivo su una piattaforma distribuita, z/OS o un gestore code IBM MQ 8.0 o successivo su z/OS, la selezione del messaggio viene effettuata dal gestore code piuttosto che sul sistema client.

Se viene specificata la modalità di migrazione del fornitore di messaggistica IBM MQ e IBM MQ classes for JMS tenta di utilizzare una delle API JMS 2.0 , la chiamata del metodo API ha esito negativo con l'eccezione `JMSCC5007`.

Informazioni correlate

Dipendenze tra proprietà di oggetti IBM MQ classes for JMS

TRANSPORT

PROVIDERVERSION non specificato

Quando la proprietà **PROVIDERVERSION** di una factory di connessione non è specificata, il client JMS utilizza un algoritmo per determinare quale modalità operativa viene utilizzata per la connessione al gestore code. Una factory di connessione creata nello spazio nomi JNDI con una versione precedente di IBM MQ classes for JMS assume il valore non specificato quando la factory di connessione viene utilizzata con la nuova versione di IBM MQ classes for JMS.

Se la proprietà **PROVIDERVERSION** non è specificata, l'algoritmo viene utilizzato quando viene richiamato il metodo `createConnection` . L'algoritmo controlla un certo numero di proprietà della factory di connessione per stabilire se è richiesta la modalità normale del provider di messaggistica IBM MQ , la modalità normale con limitazioni o la modalità di migrazione del provider di messaggistica IBM MQ . La modalità normale viene sempre tentata prima e quindi la modalità normale con restrizioni. Se non è possibile effettuare nessuno di questi tipi di connessione, il client JMS si disconnette dal gestore code e si connette nuovamente con il gestore code per tentare una connessione in modalità di migrazione.

Controllo delle proprietà BROKERVER, BROKERQMGR, PSMODEe BROKERCONQ

La verifica dei valori delle proprietà inizia con la proprietà **BROKERVER** come mostrato nella Figura 1.

Se la proprietà **BROKERVER** è impostata su V1, la proprietà **TRANSPORT** viene selezionata successivamente come mostrato nella Figura 2. Tuttavia, se la proprietà **BROKERVER** è impostata su V2, il controllo aggiuntivo mostrato nella Figura 1 viene eseguito prima del controllo della proprietà **TRANSPORT** .

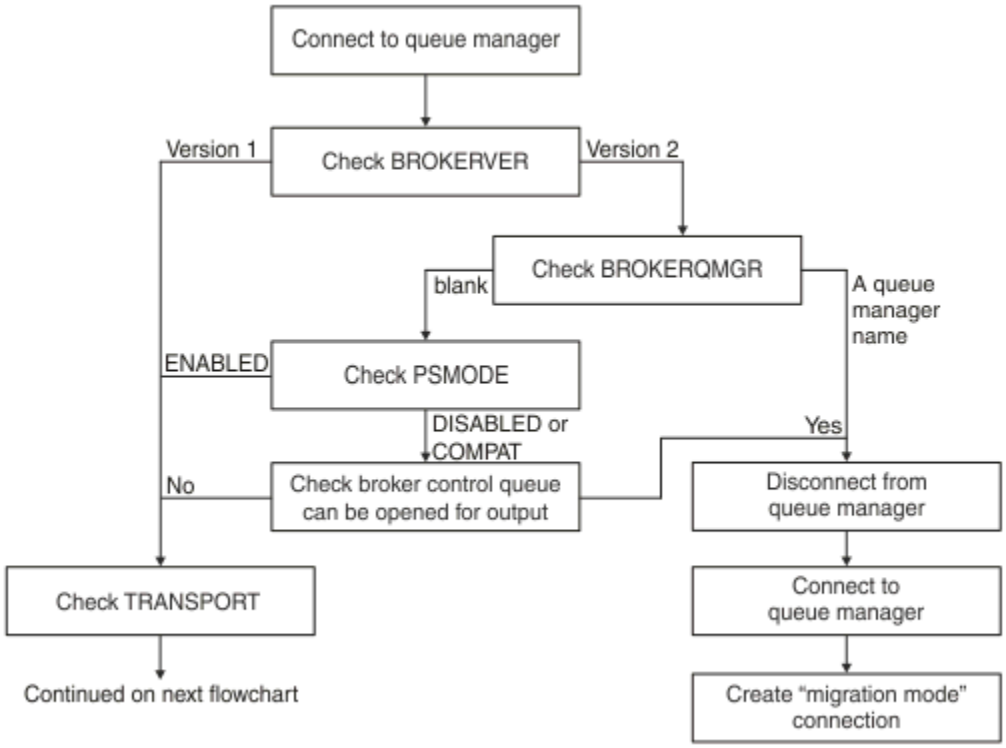


Figura 95. PROVIDERVERSION non specificato

Se la proprietà **BROKERVER** è impostata su V2, per rendere possibile una connessione in modalità normale, la proprietà **BROKERQMGR** deve essere `vuota`. Inoltre, l'attributo **PSMODE** sul gestore code deve essere impostato su ENABLED oppure la coda di controllo del broker specificata dalla proprietà **BROKERCONQ** non deve essere aperta per l'output.

Se i valori delle proprietà sono impostati come richiesto per una connessione in modalità normale, il controllo passa alla proprietà **TRANSPORT** come mostrato nella Figura 2.

Se i valori delle proprietà non sono impostati come richiesto per una connessione in modalità normale, il client JMS si disconnette dal gestore code, quindi si riconnette e crea una connessione in modalità di migrazione. Ciò si verifica nei seguenti casi:

- Se la proprietà **BROKERQMGR** è `vuota` e l'attributo **PSMODE** sul gestore code è impostato su `COMPAT` o `DISABLED` e la coda di controllo broker specificata dalla proprietà **BROKERCONQ** può essere aperta per l'output (ossia, `MQOPEN` per l'output riuscito).
- Se la proprietà **BROKERQMGR** specifica un nome coda.

Controllo della proprietà TRANSPORT e del livello di comando

La Figura 2 mostra i controlli effettuati per il livello di comando e la proprietà **TRANSPORT** del gestore code.

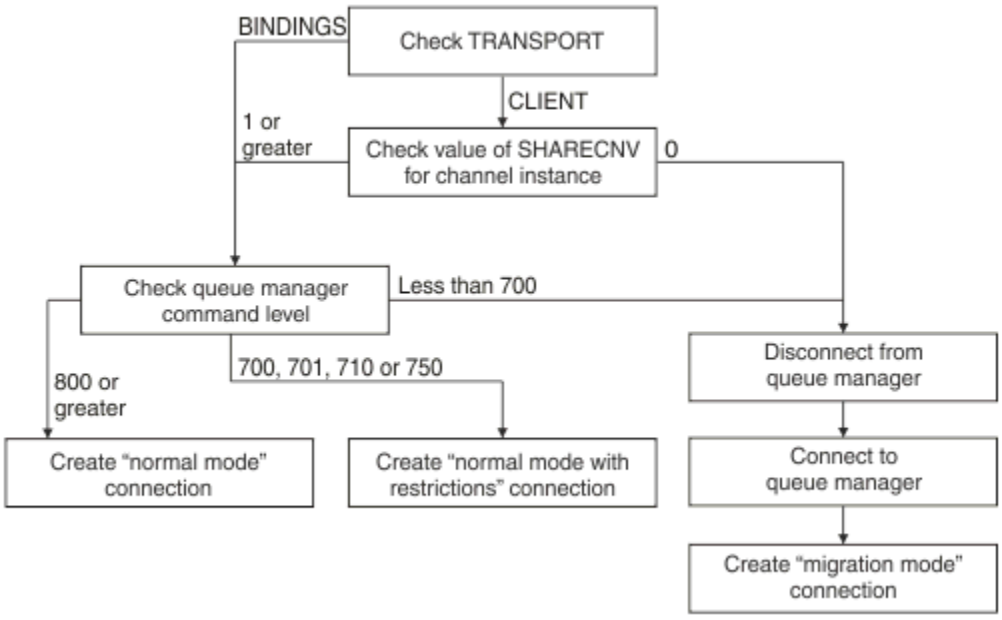


Figura 96. PROVIDERVERSION non specificato (continua)

Una connessione in modalità normale viene creata in uno dei seguenti casi:

- La proprietà **TRANSPORT** della factory di connessione è impostata su BINDINGS e il gestore code ha un livello di comando di 800 o superiore.
- La proprietà **TRANSPORT** è impostata su CLIENT, la proprietà **SHARECNV** sul canale di connessione server ha un valore pari o superiore a 1 e il gestore code ha un livello di comando pari o superiore a 800.

Se il livello di comando del gestore code è 710 o 750, viene creata una modalità normale con restrizioni di connessione al gestore code.

Una connessione in modalità di migrazione viene creata anche se la proprietà **TRANSPORT** è impostata su CLIENT e la proprietà **SHARECNV** sul canale di connessione del server ha il valore 0.

Informazioni correlate

Dipendenze tra proprietà di oggetti IBM MQ classes for JMS
ALTER QMGR (attributo PSMODE)
BROKERCONQ
BROKERQMGR
BROKERVER
DEFINE CHANNEL (SHARECNV proprietà)
TRANSPORT

Quando sovrascrivere l'impostazione predefinita PROVIDERVERSION

Se una factory di connessione creata nello spazio dei nomi JNDI con una versione precedente di IBM MQ classes for JMS viene utilizzata con la nuova versione di IBM MQ classes for JMS, la proprietà **PROVIDERVERSION** per la factory di connessione viene impostata sul valore predefinito non `specificato` e viene utilizzato un algoritmo per stabilire quale modalità di funzionamento del provider di messaggistica IBM MQ viene utilizzata. Tuttavia, ci sono due casi in cui è necessario sovrascrivere la selezione predefinita per la proprietà **PROVIDERVERSION** in modo che IBM MQ classes for JMS possa funzionare correttamente.

Nota: La modalità di migrazione descritta in questo argomento è per la migrazione da IBM WebSphere MQ 6.0 a IBM WebSphere MQ 7.0. Non si applica alla migrazione da release successive.

IBM WebSphere MQ 6.0, WebSphere Application Server 6.0.xe WebSphere Message Broker 6 non sono supportati e pertanto questo argomento è incluso solo a scopo di riferimento.

Quando la proprietà **PROVIDERVERSION** è impostata sul valore predefinito `non specificato`, viene utilizzato un algoritmo per determinare la modalità operativa da utilizzare, come descritto in "PROVIDERVERSION non specificato" a pagina 663. Tuttavia, non è possibile utilizzare questo algoritmo nei seguenti due scenari.

1. Se WebSphere Message Broker e WebSphere Event Broker si trovano in modalità di compatibilità, è necessario specificare un valore per la proprietà **PROVIDERVERSION** affinché WebSphere Message Broker e WebSphere Event Broker funzionino correttamente.
2. Se si utilizza WebSphere Application Server 6.0.1, WebSphere Application Server 6.0.2o WebSphere Application Server 6.1, i factory di connessione vengono definiti utilizzando la console di gestione WebSphere Application Server .

   In WebSphere Application Server, il valore predefinito della proprietà **BROKERVER** su un factory di connessione è V2. Il valore predefinito per la proprietà **BROKERVER** per i factory di connessione creati utilizzando lo JMS strumento di gestione **JMSAdmin** o IBM MQ Explorer è V1. Questa proprietà è ora `non specificata` in IBM MQ.

Se la proprietà **BROKERVER** è impostata su V2, perché è stata creata da WebSphere Application Server o perché la factory di connessione è stata utilizzata per la pubblicazione / sottoscrizione prima e ha un gestore code esistente che ha una proprietà **BROKERCONQ** definita (perché è stata utilizzata per la messaggistica di pubblicazione / sottoscrizione prima), viene utilizzata la modalità di migrazione del provider di messaggistica IBM MQ .

Tuttavia, se si desidera che l'applicazione utilizzi la comunicazione peer - to - peer e l'applicazione utilizza un gestore code esistente che è stato mai utilizzato per la pubblicazione / sottoscrizione e dispone di una factory di connessione con **BROKERVER** impostato su 2, che è l'impostazione predefinita se la factory di connessione è stata creata in WebSphere Application Server, viene utilizzata la modalità di migrazione del provider di messaggistica IBM MQ . L'uso della modalità di migrazione del fornitore di messaggistica IBM MQ in questo caso non è necessario; utilizzare invece la modalità normale del fornitore di messaggistica IBM MQ . Per aggirare questo problema, è possibile utilizzare uno dei seguenti metodi:

- Impostare **BROKERVER** su 1 o non specificato. L'opzione scelta dipende dall'applicazione.
- Impostare **PROVIDERVERSION** su 8o 7, che sono proprietà personalizzate in WebSphere Application Server 6.1.

  In alternativa, utilizzare la proprietà di configurazione del client o modificare il gestore code connesso in modo che non disponga della proprietà **BROKERCONQ** impostata o rendere la coda inutilizzabile.

Configurazione delle informazioni sulla versione del provider in WebSphere Application Server

Per configurare le informazioni sulla versione del fornitore in WebSphere Application Server, è possibile utilizzare la console di gestione o i comandi wsadmin.

Procedura

Per configurare le informazioni sulla versione del provider per un factory di connessione IBM MQ o per un oggetto della specifica di attivazione in WebSphere Application Server, consultare *Informazioni correlate* per i link a ulteriori informazioni nella documentazione del prodotto WebSphere Application Server .

Informazioni correlate per WebSphere Application Server 8.5.5

Impostazioni della factory di connessione del fornitore di messaggistica IBM MQ

`createWMQConnectionFactory` comando

Impostazioni della specifica di attivazione del fornitore di messaggistica IBM MQ

`createWMQActivationSpec` comando

Informazioni correlate per WebSphere Application Server 8.0.0

Impostazioni della factory di connessione del fornitore di messaggistica IBM MQ

createWMQConnectionFactory comando
Impostazioni della specifica di attivazione IBM MQ
createWMQActivationSpec comando
Informazioni correlate per WebSphere Application Server 7.0.0
Impostazioni della factory di connessione del fornitore di messaggistica IBM MQ
createWMQConnectionFactory comando
Impostazioni della specifica di attivazione IBM MQ
createWMQActivationSpec comando

Rimozione di sottoscrizioni durevoli WebSphere Application Server

Quando si utilizza il provider di messaggistica IBM MQ con WebSphere Application Server 7.0 e IBM MQ 8.0, le sottoscrizioni durevoli create dalle applicazioni MDB (message - driven bean) associate alle specifiche di attivazione non vengono rimosse. Le sottoscrizioni durature possono essere rimosse utilizzando il programma di utilità della riga comandi IBM MQ Explorer o IBM MQ .

Informazioni su questa attività

Un'applicazione MDB (message - driven bean) che rimuove una sottoscrizione durevole può essere configurata per utilizzare una porta listener o una specifica di attivazione, purché l'applicazione sia in esecuzione all'interno di un'istanza WebSphere Application Server 7.0 o IBM MQ 8.0 che utilizza la modalità normale del provider di messaggistica IBM MQ per connettersi a IBM MQ.

Se l'applicazione MDB (message - driven bean) è collegata a una porta listener, il provider di messaggistica IBM MQ crea la sottoscrizione durevole per l'applicazione la prima volta che l'applicazione viene avviata. La sottoscrizione durevole viene rimossa quando l'applicazione bean basato sui messaggi viene disinstallata da un server delle applicazioni e il server delle applicazioni viene riavviato.

Un'applicazione MDB (message - driven bean) collegata a una specifica di attivazione funziona in un modo leggermente diverso. La sottoscrizione durevole viene creata per l'applicazione la prima volta che l'applicazione viene avviata. Tuttavia, la sottoscrizione durevole non viene rimossa quando l'applicazione viene disinstallata e il server delle applicazioni riavviato.

Ciò può portare a un numero di sottoscrizioni durevoli che rimangono su un motore di pubblicazione / sottoscrizione IBM MQ per le applicazioni che non sono più installate in un sistema WebSphere Application Server . Queste sottoscrizioni sono note come "sottoscrizioni orfane" e possono causare problemi sul gestore code quando il motore di pubblicazione / sottoscrizione è in esecuzione.

Quando un messaggio viene pubblicato su un argomento, il motore di pubblicazione / sottoscrizione IBM MQ crea una copia di tale messaggio per ciascuna sottoscrizione durevole registrata su tale argomento e lo inserisce in una coda interna. Le applicazioni che utilizzano tale sottoscrizione duratura raccoglieranno e consumeranno il messaggio da questa coda interna.

Se l'applicazione MDB (message - driven bean) che stava utilizzando tale sottoscrizione durevole non è più installata, le copie dei messaggi pubblicati per l'applicazione continueranno ad essere eseguite. Tuttavia, questi messaggi non saranno mai elaborati, il che significa che potrebbe esserci un numero elevato di messaggi rimanenti nella coda interna che non verranno mai rimossi.

Prima di iniziare

Le sottoscrizioni registrate con il motore di pubblicazione / sottoscrizione IBM MQ avranno un nome sottoscrizione associato.

Le sottoscrizioni durevoli create dal provider di messaggistica WebSphere Application Server IBM MQ per i bean basati sui messaggi collegati alle specifiche di attivazione avranno un nome sottoscrizione nel seguente formato:

```
JMS:queue manager name:client identifier:subscription name
```

Dove:

nome gestore code
Questo è il nome del gestore code IBM MQ in cui è in esecuzione il motore di pubblicazione / sottoscrizione.

Identificativo client
Questo è il valore della proprietà ID client della specifica di attivazione a cui è collegato il bean basato sui messaggi.

Nome sottoscrizione
Questo è il valore della proprietà della specifica di attivazione Nome sottoscrizione per la specifica di attivazione che l'applicazione MDB (message - driven bean) è stata configurata per utilizzare.

Ad esempio, si supponga di disporre di una specifica di attivazione impostata per la connessione al gestore code testQM. La specifica di attivazione ha le seguenti proprietà impostate:

- ID client = testClientID
- Nome sottoscrizione = durableSubscription1

Se un bean basato sui messaggi che esegue una sottoscrizione durevole è collegato a questa specifica di attivazione, viene creata una sottoscrizione sul IBM MQ motore di pubblicazione / sottoscrizione sul gestore code testQM che ha il seguente nome sottoscrizione:

- JMS:testQM:testClientID:durableSubscription1

Le sottoscrizioni che sono state registrate con il motore di pubblicazione / sottoscrizione IBM MQ per un determinato gestore code possono essere visualizzate in uno dei due seguenti modi:

- La prima opzione consiste nell'utilizzare MQ Explorer. Quando MQ Explorer è stato connesso ad un gestore code utilizzato per il lavoro di pubblicazione / sottoscrizione, l'elenco dei sottoscrittori attualmente registrati con il motore di pubblicazione / sottoscrizione può essere visualizzato facendo clic sulla voce `IBM WebSphere MQ ->`*`queue manager name`*`-> Subscriptions` nel riquadro di navigazione.
- L'altro modo per visualizzare le sottoscrizioni che sono state registrate con un motore di pubblicazione / sottoscrizione è utilizzare il IBM MQ programma di utilità della riga comandi **runmqsc** ed eseguire il comando **display sub**. A tale scopo, visualizzare un prompt dei comandi, passare alla directory *`WebSphere MQ`*`\bin` e immettere il comando seguente per avviare **runmqsc**:

  – `runmqsc` *`queue manager name`*

  Una volta avviato il programma di utilità **runmqsc** , immettere il seguente comando per elencare tutte le sottoscrizioni durevoli attualmente registrate con il motore di pubblicazione / sottoscrizione in esecuzione sul gestore code a cui è connesso **runmqsc** :

  – `display sub(*) durable`

Per verificare se le sottoscrizioni durevoli registrate con i motori di pubblicazione / sottoscrizione sono ancora attive:

1. Generare l'elenco delle sottoscrizioni durevoli che sono state registrate con il motore di pubblicazione / sottoscrizione.
2. Per ogni sottoscrizione durevole:
   - Controllare il nome della sottoscrizione per il sottoscrittore durevole e annotare il valore *identificativo client* e *nome sottoscrizione* .
   - Esaminare i sistemi WebSphere Application Server che si stanno collegando a questo motore di pubblicazione / sottoscrizione. Verificare se sono state definite specifiche di attivazione che hanno la proprietà ID client che corrisponde al valore *identificativo client* e la proprietà del nome sottoscrizione che corrisponde al *nome sottoscrizione*.
   - Se non viene trovata alcuna specifica di attivazione che abbia le proprietà ID client e nome sottoscrizione che corrispondono ai campi *identificativo client* e *nome sottoscrizione* nel nome sottoscrizione IBM MQ , non ci sono specifiche di attivazione che utilizzano questa sottoscrizione durevole. La sottoscrizione durevole può essere eliminata.

- Se è stata definita una specifica di attivazione che corrisponde al nome della sottoscrizione durevole, il controllo finale che deve essere effettuato è quello di verificare se esiste un'applicazione MDB (message - driven bean) che utilizza questa specifica di attivazione. Per far ciò:
  - Prendere nota del nome JNDI per la specifica di attivazione che ha preso la sottoscrizione durevole che si sta attualmente cercando.
  - Visualizzare il riquadro Configurazione nella console di gestione WebSphere Application Server per ogni applicazione bean basato sui messaggi installata.
  - Fare clic sul collegamento Bind del listener MDB (Message Driven Bean) nel riquadro Configurazione.
  - Viene visualizzata una tabella con le informazioni sull'applicazione MDB (message - driven bean). Se il pulsante di opzione della specifica di attivazione è selezionato nella colonna Bind e il campo del nome della risorsa di destinazione JNDI contiene il nome JNDI per la specifica di attivazione che ha eliminato la sottoscrizione durevole, la sottoscrizione è ancora in uso e non può essere eliminata.
  - Se non è possibile trovare alcuna applicazione bean basata sui messaggi che utilizza la specifica di attivazione, è possibile eliminare la sottoscrizione durevole.

Procedura

Una volta identificata una sottoscrizione duratura "orfana", è possibile eliminarla utilizzando il IBM MQ Explorer o il IBM MQ programma di utilità della riga comandi **runmqsc**.

Per eliminare una sottoscrizione durevole "orfana" utilizzando il IBM MQ Explorer:

1. Evidenziare la voce per la sottoscrizione
2. Fare clic con il tasto destro del mouse sulla voce e selezionare **Elimina ...** dal menu. Viene visualizzata una finestra di conferma.
3. Verificare che il nome della sottoscrizione visualizzato nella finestra di conferma sia corretto e fare clic su **Sì**.

Il IBM MQ Explorer ora elimina la sottoscrizione dal motore di pubblicazione / sottoscrizione e ripulisce tutte le risorse interne associate ad essa (ad esempio i messaggi non elaborati che sono stati pubblicati per l'argomento su cui è stata registrata la sottoscrizione durevole).

Per eliminare una sottoscrizione durevole "orfana" utilizzando l'utilità della riga comandi IBM MQ **runmqsc**, è necessario eseguire il comando **delete sub** :

1. Aprire una sessione del prompt dei comandi
2. Passare alla directory *IBM MQ*\bin
3. Immettere il seguente comando per avviare **runmqsc**:

```
runmqsc queue manager name
```

4. Una volta avviato il programma di utilità **runmqsc** , immettere:

```
delete sub(Subscription name)
```

   dove *Nome sottoscrizione* è il nome della sottoscrizione durevole, che assume il seguente formato:

   - JMS:*queue manager name*:*client identifier*:*subscription name*

Configurazione di Managed File Transfer

È possibile configurare le funzioni di Managed File Transfer dopo l'installazione.

Puoi sfruttare le soluzioni di alta disponibilità IBM MQ per migliorare la resilienza della tua configurazione Managed File Transfer . Se gli agent utilizzano gestori code di dati replicati (RDQM), è necessario

configurarli per utilizzare la funzione di indirizzo IP mobile. Ciò significa che gli agenti utilizzano lo stesso indirizzo IP per comunicare con una delle tre istanze RDQM attualmente in esecuzione e si riconnettono automaticamente in caso di failover (consultare Alta disponibilità RDQM e Creazione ed eliminazione di un indirizzo IP mobile). Se si utilizza la soluzione del gestore code a più istanze, le applicazioni utilizzano un indirizzo IP differente per comunicare con ciascuna istanza, gestita dalla riconnessione client in caso di failover (consultare Gestori code a più istanze e Riconnessione canale e client).

Concetti correlati

Suggerimenti e suggerimenti per l'utilizzo di Managed File Transfer

Attività correlate

Monitoraggio delle risorse MFT

Personalizzare MFT con uscite utente

Configurazione di MQMFTCredentials.xml

protezioneManaged File Transfer

Specifica dei programmi da eseguire con MFT

Risoluzione dei problemiManaged File Transfer

AmministrazioneManaged File Transfer

Riferimenti correlati

MFT Comandi

Il file MFT`agent.properties`

Ripristino e riavvio di MFT

Opzioni di configurazione MFT su Multiplatforms

Managed File Transfer fornisce una serie di file delle proprietà che contengono le informazioni chiave sull'impostazione e sono richiesti per l'operazione. Questi file delle proprietà si trovano nella directory di configurazione definita quando è stato installato il prodotto.

È possibile avere più serie di opzioni di configurazione, ogni serie di opzioni di configurazione contiene una serie di directory e file delle proprietà. I valori definiti in questi file delle propriet ... vengono utilizzati come parametri predefiniti per tutti i comandi Managed File Transfer , a meno che non si specifichi esplicitamente un altro valore sulla riga comandi.

Per modificare la serie predefinita di opzioni di configurazione che si stanno utilizzando, è possibile utilizzare il comando **fteChangeDefaultConfigurationOptions** . Per modificare la serie di opzioni di configurazione che si sta utilizzando per un singolo comando, è possibile utilizzare il parametro **-p** con qualsiasi comando Managed File Transfer .

Il nome di una serie di opzioni di configurazione è il nome del gestore code di coordinamento e si consiglia di non modificarlo. Tuttavia, è possibile modificare il nome di una serie di opzioni di configurazione, ma è necessario modificare il nome delle directory `config` e `logs` . Nei seguenti esempi, il nome della serie di opzioni di configurazione è rappresentato come *coordination_qmgr_name*.

Struttura di directory delle opzioni di configurazione

Quando si configura il prodotto, le directory e i file delle proprietà vengono creati nella seguente struttura nella directory di configurazione. È inoltre possibile modificare tali directory e file delle proprietà con i seguenti comandi: **fteSetupCoordination**, **fteSetupCommands**, **fteChangeDefaultConfiguration**e **fteCreateAgent**.

```
MQ_DATA_PATH/mqft/
    config/
       coordination_qmgr_name/
            coordination.properties
            command.properties
            agents/
               agent_name/
                    agent.properties
                    exits
            loggers/
```

```
            logger_name
                 logger.properties
  installations/
     installation_name/
          installation.properties
```

La directory *coordination_qmgr_name* è una directory di opzioni di configurazione. Nella directory di configurazione può essere presente più di una directory di opzioni di configurazione. La directory *agent_name* è una directory dell'agent. Oltre a contenere il file `agent.properties` , questa directory contiene la directory `exits` , che è il percorso predefinito per le routine di uscita utente e i diversi file XML generati dai comandi **`fteCreateBridgeAgent`** e **`fteCreateCDAgent`** . Può esistere più di una directory agent nella directory `agents` di una serie di opzioni di configurazione.

File Properties

installation.properties
Il file `installation.properties` specifica il nome della serie predefinita di opzioni di configurazione. Questa voce punta Managed File Transfer ad una serie strutturata di indirizzari e file delle proprietà che contengono la configurazione da utilizzare. Generalmente, il nome di una serie di opzioni di configurazione è il nome del gestore code di coordinamento associato. Per ulteriori informazioni sul file `installation.properties` , consultare Il file MFT installation.properties.

coordination.properties
Il file `coordination.properties` specifica i dettagli di collegamento al gestore code di coordinamento. Poiché diverse installazioni di Managed File Transfer potrebbero condividere lo stesso gestore code di coordinamento, è possibile utilizzare un link simbolico a un file `coordination.properties` comune su un'unità condivisa. Per ulteriori informazioni sul file `coordination.properties` , consultare Il file MFT coordination.properties.

command.properties
Il file MFT command.properties specifica il gestore code comandi a cui connettersi quando si immettono i comandi e le informazioni richieste da Managed File Transfer per contattare tale gestore code. Per ulteriori informazioni sul file `command.properties` , consultare Il file MFT command.properties.

agent.properties
Ogni Managed File Transfer Agent ha il proprio file delle proprietà, `agent.properties`, che deve contenere le informazioni che un agente utilizza per connettersi al proprio gestore code. Il file `agent.properties` può anche contenere proprietà che modificano il comportamento dell'agent. Per ulteriori informazioni relative al file `agent.properties` , consultare Il file MFT `agent.properties`.

logger.properties
Il file `logger.properties` specifica le proprietà di configurazione per i logger. Per ulteriori informazioni sul file `logger.properties` , consultare Proprietà di configurazione del programma di registrazioneMFT.

File delle proprietà e codepage

Il contenuto di tutti i file delle proprietà Managed File Transfer deve rimanere in inglese (Stati Uniti) a causa di una limitazione di Java. Se si modificano i file delle proprietà su un sistema non inglese (Stati Uniti), è necessario utilizzare le sequenze di escape Unicode.

z/OS MFT opzioni di configurazione su z/OS

Le Managed File Transfer opzioni di configurazione su z/OS sono uguali alle opzioni per le piattaforme distribuite.

Per ulteriori informazioni sulle opzioni di configurazione in Multipiattaforme, consultare “Opzioni di configurazione MFT su Multiplatforms” a pagina 670.

Su z/OS, l'ubicazione di configurazione è definita dalla variabile d'ambiente BFG_DATA. Se una configurazione non esiste già nella directory UNIX System Services a cui fa riferimento BFG_DATA, lo

script JCL BFGCUSTM di un dataset della libreria PDSE del comando MFT genera i lavori richiesti per creare la configurazione. La configurazione viene quindi creata quando si eseguono questi lavori generati. La creazione della configurazione si basa su BFG_DATA che fa riferimento a una directory esistente accessibile.

È anche possibile creare e gestire una configurazione utilizzando gli stessi comandi **fte** disponibili su Multiplatforms e z/OS. Per un elenco dei comandi **fte** , consultare ComandiMFT .

Linux Windows V 9.1.0 Configurazione di Redistributable Managed File Transfer Agent

È possibile configurare Redistributable Managed File Transfer Agent per connettersi a un'infrastruttura IBM MQ esistente e consentire agli utenti di trasferire i file senza dover installare IBM MQ per ottenere la funzione Managed File Transfer .

Prima di iniziare

Per informazioni sui termini di licenza ridistribuibili per Redistributable Managed File Transfer Agent, vedere IBM MQ Componenti ridistribuibili.

Redistributable Managed File Transfer Agent fornisce la funzionalità di Managed File Transfer con le seguenti eccezioni:

- La connessione in modalità bind ai gestori code di coordinazione, comando e agent non è supportata, è necessario utilizzare la connessione in modalità client. Quando si immettono comandi, è necessario fornire i parametri facoltativi quando si utilizza il Managed File Transfer installato come parte di IBM MQ: host del gestore code, porta, nome e nome del canale.
- I comandi seguenti non sono inclusi:
  - fteCreateCDAgent.cmd
  - fteCreateLogger.cmd
  - fteDeleteLogger.cmd
  - fteMigrateLogger.cmd
  - fteSetLoggerTraceLevel.cmd
  - fteShowLoggerDetails.cmd
  - fteStartLogger.cmd
  - fteStopLogger.cmd

  Per un elenco completo dei comandi disponibili, consultare Serie comandi MFT installati.
- Managed File Transfer Connect:Direct non è supportato.
- IBM MQ Explorer non è incluso.

Windows È necessario installare le seguenti librerie Microsoft sul sistema per utilizzare Redistributable Managed File Transfer Agent:

- Microsoft Visual C++ Redistributable 2008
- Microsoft Visual C++ Redistributable 2012

Queste librerie sono disponibili da Microsoft. Consultare Gli ultimi download Visual C+ + supportati.

Nota: Advanced Message Security non è supportato con Redistributable Managed File Transfer package.

Informazioni su questa attività

Puoi facoltativamente scaricare e configurare Redistributable Managed File Transfer Agent per connetterti a un'infrastruttura IBM MQ esistente per consentire agli utenti di trasferire i file tra il loro ambiente locale e l'infrastruttura IBM MQ esistente senza la necessità di installarli IBM MQ. Attenersi alla seguente procedura per scaricare ed estrarre il Redistributable Managed File Transfer Agent:

Procedura

1. Scarica il Pacchetto agent IBM MQ ridistribuibile Managed File Transfer da Fix Central.
   a) Scegli il pacchetto per il tuo sistema operativo:
   I nomi dei file di archivio o .zip descrivono il contenuto del file e i livelli di manutenzione equivalenti.

   V 9.1.0 Ad esempio, per IBM MQ 9.1.0, i nomi file sono i seguenti:

   - Windows `9.1.0.0-IBM-MQFA-Redist-Win64`
   - Linux `9.1.0.0-IBM-MQFA-Redist-LinuxX64`
   - Linux `9.1.0.0-IBM-MQFA-Redist-LinuxS390X`
   - Linux `9.1.0.0-IBM-MQFA-Redist-LinuxPPC64LE`

   b) Identificare la directory in cui si desidera estrarre il pacchetto, ad esempio:

   - Windows `C:\MFTZ`
   - Linux `/home/MFTZ`
2. Estrarre il contenuto del package scaricato:

   - Windows Su Windows, utilizzare gli strumenti di Windows Explorer per eseguire l'estrazione.
   - Linux Su Linux, estrarre e decomprimere come segue:

     ```
     gunzip 9.0.1.0-IBM-MQFA-Redist-LinuxX64.tar.gz
     ```

     e poi

     ```
     tar xvf 9.0.1.0-IBM-MQFA-Redist-LinuxX64.tar
     ```

     Vengono create le seguenti directory:

   - Linux Windows `bin`: contiene tutti i comandi MFT richiesti
   - Windows `bin64`: contiene le librerie richieste necessarie per il supporto SO Windows a 64 bit
   - Linux Windows `java`: contiene le librerie IBM JRE e IBM MQ .
   - Linux Windows `licenses`: contiene i file di licenza
   - Linux Windows `mqft`: contiene le directory `ant` e `lib` richieste per il supporto Ant e per il supporto della funzione MFT principale
   - Linux Windows `swtag`: contiene il file `swidtag` richiesto dai gestori delle licenze per identificare le installazioni sulla macchina

Operazioni successive

È possibile configurare l'agente MFT . Per i passi successivi, consultare “Creazione della configurazione iniziale per Redistributable Managed File Transfer Agent” a pagina 673.

Concetti correlati

Possibili errori durante la configurazione dell'agent MFT ridistribuibile

Linux Windows V 9.1.0 Creazione della configurazione iniziale per Redistributable Managed File Transfer Agent

È possibile configurare un Managed File Transfer Agent per connettersi a una configurazione IBM MQ esistente.

Prima di iniziare

Assicurarsi di scaricare ed estrarre il contenuto del pacchetto Redistributable Managed File Transfer Agent . Per ulteriori informazioni, consultare “Configurazione di Redistributable Managed File Transfer Agent” a pagina 672.

Informazioni su questa attività

Si crea innanzitutto l'ambiente di cui Redistributable Managed File Transfer Agent ha bisogno. È quindi possibile impostare la connettività con il gestore code in esecuzione sul server IBM MQ , quindi configurare un agent e il gestore code agent, prima di avviare e verificare l'agent.

Procedura

1. Creare l'ambiente per Redistributable Managed File Transfer Agent.

   Quando si esegue il comando **fteCreateEnvironment** , viene creata la directory dei dati MFT con le informazioni di configurazione per gli agent MFT . Accertarsi di trovarsi nella directory di `bin` creata quando è stato estratto il componente ridistribuibile MFT Agent scaricato. Esegui il seguente comando:

   - Windows

     ```
     fteCreateEnvironment.cmd -d datapath location
     ```

   - Linux

     ```
     . ./fteCreateEnvironment -d datapath location
     ```

   Questo comando utilizza i seguenti parametri facoltativi:

   -d
   Questo parametro specifica l'ubicazione per il percorso dati in cui viene creata, memorizzata e conservata la configurazione MFT . Se si esegue **fteCreateEnvironment** senza specificare l'ubicazione dei dati, la directory `mftdata` viene creata nell'ubicazione in cui viene estratto Redistributable Managed File Transfer Agent .

   Nota: Se l'agent ridistribuibile verrà eseguito come un servizio Windows, la variabile di ambiente **BFG_DATA** deve essere impostata nell'ambiente di sistema perché il servizio funzioni.

   V 9.1.2 **-n *nome installazione***
   Questo parametro viene utilizzato per specificare il nome di una installazione di IBM MQ o un nome univoco.

   Esempi di situazioni in cui si potrebbe voler utilizzare questo parametro sono:

   – Se si desidera testare rapidamente una nuova funzione o funzione utilizzando il pacchetto ridistribuibile con la configurazione esistente in cui gli agent sono stati configurati per connettersi al gestore code solo in modalità client. Tenere presente che questo parametro non si applica ad alcun agent configurato per la connessione a un gestore code in modalità bind.
   – Se si sta eseguendo la migrazione da un'installazione standard di Managed File Transfer a un package Redistributable Managed File Transfer Agent e si desidera utilizzare la stessa configurazione di quella creata dall'installazione standard. Questo è il caso in cui Managed File Transfer standard è stato installato ma si sta connettendo a un gestore code dell'agent in esecuzione su un'altra macchina.

   La variabile del nome di installazione predefinita è **BFG_INSTALLATION_NAME**.

   Per ulteriori informazioni relative al comando **fteCreateEnvironment** , consultare fteCreateEnvironment (set up environment for Redistributable Managed File Transfer Agent).

È anche possibile impostare la variabile di ambiente *BFG_DATA* con l'ubicazione del percorso dati:

```
BFG_DATA=Datapath location
```

Prima di creare, avviare e arrestare un agent o qualsiasi altro comando, è necessario verificare che la variabile *BFG_DATA* sia impostata sul percorso dati corretto.

2. Impostare la connettività IBM MQ .
   a) Impostare il gestore code di coordinamento utilizzando il comando **fteSetupCoordination** .

   Il comando **fteSetupCoordination** crea il set attivo richiesto per i gestori code di coordinamento e le directory necessarie per un'ulteriore configurazione. Redistributable Managed File Transfer Agent funziona in modalità client, pertanto è necessario fornire ulteriori parametri con questo comando per evitare un errore, poiché la modalità di collegamento non è supportata.

   ```
   fteSetupCoordination -coordinationQMgr PRMFTDEMO2
                -coordinationQMgrHost 9.121.59.233 -coordinationQMgrPort 3002
                -coordinationQMgrChannel SYSTEM.DEF.SVRCONN
   ```

   Per ulteriori dettagli e passi per l'utilizzo del comando **fteSetupCoordination** , consultare fteSetupCoordination. Per informazioni su come configurare il gestore code di coordinamento, consultare “Configurazione del gestore code di coordinamento per MFT” a pagina 712.

   b) Creare e impostare il gestore code comandi:

   ```
   fteSetupCommands -p PRMFTDEMO2 -connectionQMgrHost 9.121.59.233
                -connectionQMgrPort 3002 -connectionQMgrChannel SYSTEM.DEF.SVRCONN
                -connectionQMgr PRMFTDEMO2 -f
   ```

   Per ulteriori dettagli e passi per l'utilizzo del comando **fteSetupCommands** , consultare ComandifteSetup: creare il file MFT command.properties.

3. Creare la definizione dell'agent MFT per un endpoint.

   ```
   fteCreateAgent -p PRMFTDEMO2 -agentQMgrHost 9.121.59.233
              -agentQMgrPort 3002 -agentQMgrChannel SYSTEM.DEF.SVRCONN
              -agentName AGENT.TRI.BANK -agentQMgr PRMFTDEMO2 -f
   ```

   Per ulteriori informazioni sull'utilizzo del comando **fteCreateAgent** per configurare un agent e il gestore code dell'agent, consultare fteCreateAgent.

   Nei passi “2” a pagina 675 e “3” a pagina 675 per ogni agent, si creano definizioni di argomenti e code sul gestore code dell'agent.

4. Avviare l'agent e si è pronti a trasferire i file.

   ```
   fteStartAgent -p PRMFTDEMO2 AGENT.TRI.BANK
   ```

   È possibile verificare lo stato dell'agent eseguendo il seguente comando:

   ```
   fteListAgents
   ```

   Per ulteriori dettagli sull'utilizzo del comando **fteListAgents** , consultare fteListAgents.

Concetti correlati

“Configurazione di Managed File Transfer” a pagina 669
È possibile configurare le funzioni di Managed File Transfer dopo l'installazione.

“Opzioni di configurazione MFT su Multiplatforms” a pagina 670
Managed File Transfer fornisce una serie di file delle proprietà che contengono le informazioni chiave sull'impostazione e sono richiesti per l'operazione. Questi file delle proprietà si trovano nella directory di configurazione definita quando è stato installato il prodotto.

Riferimenti correlati

fteCreateTransfer: avviare un nuovo trasferimento file

z/OS Creazione di un dataset del comando Logger o dell'agent MFT

È possibile creare un dataset PDSE di comandi dal dataset del modello di comando Managed File Transfer per un Managed File Transfer Agent specifico o Managed File Transfer Logger per un coordinamento specifico.

Informazioni su questa attività

Completare i seguenti passi:

Procedura

1. Eseguire una copia del dataset della libreria PDSE del modello di comandi MFT SBFGCMDS.

   z/OS SBFGCMDS deve essere copiato in una nuova libreria, ad esempio *prefix.agent*.JCL_. È possibile utilizzare una versione aggiornata del membro SBFGCMDS (BFGCOPY) con le seguenti sostituzioni:

   - Sostituire *+ + supplied-library + +* con il nome completo di SBFGCMDS PDSE.
   - z/OS Sostituire *+ + service-library + +* con il nome completo del nuovo dataset della libreria PDSE del comando MFT . *+ + service-library + +* è il dataset di output per l'agente o il servizio logger creato.
2. Per il nuovo dataset della libreria PDSE del comando MFT , modificare il membro BFGCUSTM, che è uno script JCL per personalizzare i comandi per l'agente o il programma di registrazione. Ogni variabile viene specificata nel formato: *+ + nome variabile + +*, che è necessario sostituire con il relativo valore richiesto. Per una descrizione delle varie variabili JCL, consultare “z/OS variabili JCL” a pagina 688. L'istruzione DD BFGSTDIN definisce le variabili in tre categorie: Variabili, Proprietà e Ambiente. L'istruzione ha il seguente formato:

   ```
   [Variables]
   variable1=value1
   variable2=value2
   ....
   variableN=valueN
   [Properties]
   property1=property value1
   property2=property value2
   ...
   propertyN=property valueN
   [Environment]
   custom_variable1=value1
   custom_variable2=value2
   ....
   custom_variableN=valueN
   ```

   Le variabili definiscono la serie di variabili di impostazione e di ambiente richieste per ciascun comando.

   Le proprietà definiscono le sovrascritture per le proprietà di configurazione MFT . È possibile aggiungere le proprietà dell'agent e del logger come richiesto per personalizzare l'agent o il logger per il proprio ambiente. Per un elenco di tutte le proprietà, consultare “File delle proprietà di configurazione” a pagina 701. Questa funzione viene fornita per salvare la necessità di accedere ai file delle proprietà di configurazione MFT , conservati come file UNIX System Services.

   L'ambiente definisce eventuali variabili di ambiente personalizzate aggiuntive richieste.
3. Inoltrare il lavoro BFGCUSTM per il nuovo data set della libreria PDSE del comando MFT . Questo lavoro genera la serie di comandi JCL, come nuovi membri del PDSE, appropriati per l'agent o il logger. Per un elenco completo dei comandi, consultare “Script JCL del comando del logger e dell'agent z/OS” a pagina 693.

   Il lavoro BFGCUSTM aggiorna la libreria che contiene il JCL che include un'istruzione DD con DISP=OLD. È necessario uscire dall'editor dopo l'invio per consentire l'esecuzione del lavoro.

Esaminare il log del lavoro di output per controllare che lo script JCL sia stato eseguito correttamente. In caso di errori, correggerli e inoltrare nuovamente il lavoro BFGCUSTM.

Lo script JCL BFGCUSTM aggiorna anche i file delle proprietà di configurazione di UNIX System Services MFT come necessario per mantenere i file in fase. Se la configurazione definita dalla proprietà CoordinationQMgr non esiste, vengono emessi messaggi di avvertenza ed è necessario eseguire i lavori BFGCFCR e BFGCMCR generati per creare i file delle proprietà di configurazione. È necessario eseguire BFGAGCR per un agente e BFGLGCRS per una modifica del programma di registrazione. Se la configurazione specificata esiste già, viene aggiornata con le proprietà definite nello script JCL BFTCUSTM.

Concetti correlati

"MFT opzioni di configurazione su z/OS" a pagina 671
Le Managed File Transfer opzioni di configurazione su z/OS sono uguali alle opzioni per le piattaforme distribuite.

Attività correlate

"Aggiornamento di un dataset del comando Logger o dell'agent MFT esistente su z/OS" a pagina 688
È possibile aggiornare un dataset della libreria PDSE di comandi Managed File Transfer creato dal dataset del modello di comandi Managed File Transfer .

z/OS Configurazione di Managed File Transfer for z/OS

Managed File Transfer for z/OS richiede la personalizzazione per consentire al componente di funzionare correttamente.

Informazioni su questa attività

È necessario:

1. Modificare un membro PDSE per specificare i dati di configurazione
2. Definire il gestore code di coordinamento.
3. Definire il gestore code comandi
4. Configurare uno o più agent
5. Facoltativamente: configurare un'attività del programma di registrazione per memorizzare i dati in Db2

La sequenza delle attività che è necessario eseguire è descritta nei seguenti argomenti.

Concetti correlati

"Revisione della configurazione di MFT" a pagina 677
È necessario esaminare la configurazione del proprio sistema prima di iniziare.

Attività correlate

InstallazioneManaged File Transfer for z/OS

z/OS Revisione della configurazione di MFT

È necessario esaminare la configurazione del proprio sistema prima di iniziare.

Managed File Transfer (MFT) richiede uno o più gestori code per agire nei ruoli seguenti per ogni configurazione MFT definita:

- Un gestore code di coordinazione, che conserva le informazioni sullo stato di ciascun agent nella configurazione pubblicata in un argomento sul coordinatore.
- Uno o più gestori code di connessione o comandi che fungono da punto di ingresso alla rete IBM MQ per i comandi MFT.
- Uno o più gestori code agent che forniscono la comunicazione tra un agent MFT e la rete IBM MQ .

Ciascuno dei ruoli precedenti può essere eseguito da un gestore code separato oppure è possibile combinare i ruoli in modo che, nella configurazione più semplice, tutti i ruoli vengano eseguiti da un singolo gestore code.

Se si sta aggiungendo un gestore code z/OS a un ambiente MFT esistente, è necessario definire la connettività tra il gestore code z/OS e gli altri gestori code nella configurazione. È possibile ottenere questo risultato con code di trasmissione definite manualmente o utilizzando il clustering.

Ogni agent MFT comunica con un singolo gestore code. Se più agent comunicano con lo stesso gestore code, il gestore code dell'agent avrà più code definite per ciascun agent:

- SYSTEM.FTE.COMMAND.*nome_agent*
- SYSTEM.FTE.DATA.*nome_agent*
- SYSTEM.FTE.REPLY.*nome_agent*
- SYSTEM.FTE.STATE.*nome_agent*
- SYSTEM.FTE.EVENT.*nome_agent*
- SYSTEM.FTE.AUTHAGT1.*nome_agent*
- SYSTEM.FTE.AUTHTRN1.*nome_agent*
- SYSTEM.FTE.AUTHOPS1.*nome_agent*
- SYSTEM.FTE.AUTHSCH1.*nome_agent*
- SYSTEM.FTE.AUTHMON1.*nome_agent*
- SYSTEM.FTE.AUTHADM1.*nome_agent*

Notare che è possibile definire profili di sicurezza generici, dove si utilizza un profilo come `SYSTEM.FTE.COMMAND.*`oppure definire profili specifici per ciascun agent.

Concetti correlati

“Prima di iniziare” a pagina 678
La configurazione Managed File Transfer (MFT) utilizza i file nei dataset USS (UNIX System Services) e PDSE.

z/OS Prima di iniziare

La configurazione Managed File Transfer (MFT) utilizza i file nei dataset USS (UNIX System Services) e PDSE.

La maggior parte della configurazione e dell'operazione viene eseguita utilizzando JCL da PDSE ed è necessario avere dimestichezza con le operazioni in un ambiente USS.

È possibile accedere a OMVS da ISPF oppure utilizzare una sessione di tipo Telnet utilizzando i comandi sulla stazione di lavoro, ad esempio Telnet Putty o SSH.

Se si utilizza OMVS da ISPF, è possibile utilizzare l'editor ISPF standard e visualizzare i comandi **`oedit`** e **`obrowse`**.

È necessario avere dimestichezza con i seguenti comandi USS

Tabella 41. Comandi dei servizi di sistema UNIX comuni

Comando	**Funzione**
percorso chmod xxx	Modificare le autorizzazioni di accesso ai file.
percorso df -k	Riporta la quantità di spazio libero rimanente nel file system. -k riporta lo spazio libero in KB.
Percorso du -kt	Riporta le dimensioni delle directory nel percorso. Dimensione riportata in KB.

Tabella 41. Comandi dei servizi di sistema UNIX comuni (Continua)	
Comando	**Funzione**
trova percorso -name xxx	Ricercare il file denominato xxxx nella directory del percorso. xxx è sensibile al maiuscolo / minuscolo e può essere simile a *zzz.
directory ls -ltrd	Elenca le informazioni sulla directory specificata piuttosto che i file nella directory.
percorso ls -ltr	Elenca le informazioni sui file nel percorso.
nome file obrowse	Sfoglia il nome file.
nome file oedit	Modificare un file in OMVS.

Esaminare gli elementi nella seguente tabella e completare la tabella con le voci appropriate per la propria azienda. Questi valori sono necessari quando si modifica un membro BFGCUSTM.

Tabella 42. Parametri necessari per il membro BFGCUSTM		
Nome	**Dati di esempio**	**Commenti**
ADMIN_JOB1		Scheda di lavoro. Tutti i lavori vengono generati con la stessa scheda JCL.
armELEMENT	Se viene utilizzato ARM, utilizzare il valore ARM ELEMENT specificato nella politica ARM per questo agent o programma di registrazione. Se ARM non viene utilizzato, impostare questo parametro su uno spazio vuoto; ad esempio, armELEMENT=	
armELEMTYPE	Se si sta utilizzando ARM, utilizzare ARM ELEMTYPE specificato nella politica ARM. Ad esempio, armELEMTYPE= SYSBFGAG per un agente o armELEMTYPE= SYSBFGLG per un programma di registrazione. Se ARM non viene utilizzato, impostare questo parametro su uno spazio vuoto; ad esempio, armELEMTYPE=	
DATI_BFG		Completare come necessario
NOME_GRUPPO_BF	MQM	
BFG_JAVA_HOME	/java/java71_bit64_GA/J7.1_64/	
BFG_JVM_PROPERTIES		Completare come necessario
BFG_PROD	/var/ibm/wmqmft	
BFG_WTO	Sì	Per ottenere un messaggio MFT sul syslog.

Tabella 42. Parametri necessari per il membro BFGCUSTM (Continua)		
Nome	**Dati di esempio**	**Commenti**
CLEAN_AGENT_PROPS	-trs	Questo parametro specifica le opzioni che verranno utilizzate per ripulire un agent quando viene eseguito un membro BFGAGCL. Per ulteriori informazioni sui valori validi per questo parametro, consultare fteCleanAgent: cleanup di MFT Agent.
coordinationQMgr	MQPV	Configurazione obbligatoria
PERCORSO CREDENTIAL_PATH		Utilizzato nella migrazione
Db2_HLQ	SYS2.Db2.V10	
PERCORSO_PROP_DB		Utilizzato nella migrazione
FTE_CONFIG		Utilizzato nella migrazione
JOBCARD1		Questa è la scheda di lavoro per le attività di lunga durata, gli agent e i logger.
LIBRARY	SCEN.FTE.JCL	Nome del PDSE MFT. È necessaria una copia per ogni attività dell'agent o del programma di registrazione.
MQ_HLQ	Il qualificatore di alto livello per i dataset IBM MQ . Ad esempio, `MQM.V915`	
MQ_LANG	E	
PERCORSO MQ	`/mqm/V9R1M5`	
NOME	AGENT1	
CLASSE_OUTPUT	*	
PATH	`bin:/usr/bin:/usr/sbin`	
productId	MFT	Questo parametro viene utilizzato per impostare il tipo di prodotto per cui deve essere registrato l'uso di Managed File Transfer . Per informazioni sui valori validi per questo parametro, consultare fteSetProductId: set z/OS SCRT recording product id.
QMGR	MQPV	
service_type	AGENT o LOGGER	
TMPDIR	`/tmp`	Leggere e scrivere il percorso USS accessibile per i file temporanei.

Inoltre, è necessario rivedere le seguenti variabili e fornire i valori, se necessario:

- Host coordinationQMgr=

- coordinationQMgrPorta =
- Canale coordinationQMgr=
- connectionQMgr=
- Host connectionQMgr=
- connectionQMgrPorta =
- Canale connectionQMgr=

Queste proprietà sono comuni a AGENT o LOGGER.

Nota: Host, Porta e Canale sono richiesti per la connessione client, ma devono essere lasciati vuoti per una connessione di bind sulla macchina locale.

Concetti correlati

“Elementi da controllare” a pagina 681
Accertarsi di disporre di spazio su disco sufficiente, di una directory per la memorizzazione dei dati e di disporre dei file richiesti.

“Modifica membro BFGCUSTM” a pagina 684
È necessario modificare il membro BFGCUSTM e immettere i valori per i parametri utilizzati dall'azienda prima di eseguire il job.

z/OS Elementi da controllare

Accertarsi di disporre di spazio su disco sufficiente, di una directory per la memorizzazione dei dati e di disporre dei file richiesti.

Verificare di disporre di spazio su disco sufficiente

Verificare di disporre di spazio su disco sufficiente sul file system in cui si desidera memorizzare i file specifici della configurazione.

Se una traccia dell'agent è abilitata, per impostazione predefinita può utilizzare 100 MB di spazio su disco.

I file di configurazione stessi sono piccoli, solo pochi KB di dimensione.

Se si sta pianificando l'utilizzo di due agent e di un programma di registrazione, sono necessari almeno 300 MB. È possibile utilizzare il comando **df -k** `path`, dove `path` è l'ubicazione dei file specifici dell'installazione. Ciò fornisce lo spazio disponibile e totale in KB.

300 MB è 307.200 KB, quindi è necessario consentire almeno 310.000 KB

Creare e controllare la directory per la memorizzazione dei dati Managed File Transfer

È necessaria una directory per memorizzare i dati Managed File Transfer (MFT).

Verificare di disporre di spazio sufficiente sul file system `df -k /var`. Questo file system deve avere almeno 310.000 KB disponibili.

Se questo file system non è stato creato, utilizzare il comando **mkdir** , ad esempio **mkdir /var/mft**.

Visualizzare le autorizzazioni degli utenti su questa directory, utilizzando il comando **ls -ltrd /var/mft**.

Se il proprietario o il gruppo non è corretto, utilizzare il comando **chown owner:group /var/mft**.

Se le autorizzazioni per il gruppo non sono corrette, utilizzare il seguente comando per fornire al proprietario e al gruppo le autorizzazioni di lettura, scrittura ed esecuzione. Si noti che il seguente comando fornisce anche a tutti gli utenti autorizzazioni di lettura ed esecuzione **chmod 775 /var/mft**.

Verificare che i file esistano e che sia possibile accedervi

Utilizzare il comando **ls -ltr** per i file che verranno utilizzati durante la personalizzazione. Ad esempio:

```
ls -ltrd /java/java71_bit64_GA/J7.1_64/bin
```

fornisce

```
drwxr-xr-x  4 SYSTASK TSOUSER   8192 Nov 15 2013 /java/java71_bit64_GA/J7.1_64/bin
```

dove `drwxr-xr-x` indica

d
Questa è una directory.

rwx
Il proprietario *SYSTASK* dispone dell'accesso in lettura, scrittura ed esecuzione alla directory.

r - x
Le persone del gruppo *TSOUSER* possono leggere ed eseguire file nella directory.

r - x
Accesso universale, vale a dire, chiunque può leggere o eseguire i file nella directory.

Verificare i file specificati in:

Tabella 43. Accesso richiesto dagli utenti a file specifici

Percorso	**Accesso richiesto dagli utenti che eseguono la configurazione**
BFG_JAVA_HOME	Lettura ed esecuzione
/tmp	Lettura e scrittura
BFG_PROD	Letto
DATI_BFG	Scrivi
PERCORSO MQ	Letto

Concetti correlati

“Prima di iniziare” a pagina 678
La configurazione Managed File Transfer (MFT) utilizza i file nei dataset USS (UNIX System Services) e PDSE.

“Configurazioni comuni di MFT per z/OS” a pagina 682
Una panoramica delle diverse configurazioni Managed File Transfer

z/OS Configurazioni comuni di MFT per z/OS

Una panoramica delle diverse configurazioni Managed File Transfer

Managed File Transfer utilizza gli agent collegati a un gestore code per il trasferimento dei dati.

MFT può utilizzare più gestori code:

- Uno o più gestori code per il trasferimento dei dati.
- Un gestore code di comandi che emette le richieste. Ad esempio, una richiesta per avviare un trasferimento viene inviata a questo gestore code e i comandi associati vengono instradati agli agent MFT.
- Un gestore code di coordinamento che gestisce il lavoro.

Esistono tre configurazioni comuni di Managed File Transfer (MFT):

1. Un singolo gestore code con uno o più agent che utilizzano connessioni locali. Potrebbe essere utilizzato per inserire il contenuto di un dataset in code di IBM MQ.
2. Un singolo gestore code con un client MFT su una macchina distribuita utilizzando bind del client.
3. Due gestori code connessi mediante canali e uno o più agent su ciascuna macchina. Questi agent possono essere bind del client o locali.

Tenere presente i seguenti aspetti:

1. MFT è scritto in Java, con alcuni script di shell e JCL per configurare e utilizzare MFT.
2. È possibile registrare lo stato e l'attività di Db2 e tale registrazione può essere memorizzata nelle tabelle Db2.
3. La persona che configura MFT deve avere familiarità con Unix System Services (USS). Ad esempio:
   - La struttura di directory con file con nomi come `/u/userID/myfile.txt2`
   - Comandi USS, ad esempio:

     cd (modifica directory)
     ls (elenca)
     chmod (modifica autorizzazioni file)
     chown (modifica la proprietà dei file o i gruppi che possono accedere al file o alla directory)
4. In USS sono richiesti i seguenti prodotti per poter configurare ed eseguire MFT:
   - Java; ad esempio, `/java/java71_bit64_GA/J7.1_64/`
   - IBM MQ V800, ad esempio `/mqm/V8R0M03`.
   - Le librerie JDBC Db2, se si desidera utilizzare Db2 per lo stato e la cronologia, ad esempio `/db2/db2v10/jdbc/lib`

È necessario un gestore code di coordinamento. Tuttavia, è possibile utilizzare lo stesso gestore code per eseguire gli agent, elaborare i comandi e per il coordinamento. Se si utilizzano più gestori code, è necessario sceglierne uno che funga da coordinatore.

Verifica la connettività IBM MQ

Se si dispone di un gestore code del coordinatore MFT esistente, è necessaria la connettività tra il gestore code in cui si sta eseguendo la configurazione e i gestori code di coordinamento e di comando.

z/OS Copia SBFGCMDS per creare una libreria JCL

È necessario creare una libreria JCL per ciascun agent e logger. Il JCL contiene la configurazione e i lavori utilizzati per creare ed eseguire l'agent o il programma di registrazione.

Per ogni agent e programma di registrazione creare una copia della libreria SBFGCMDS fornita da IBM modificando ed eseguendo il membro BFGCOPY.

Questa libreria viene utilizzata per definire la configurazione per l'agent o il programma di registrazione e, dopo la personalizzazione, contiene lavori che possono essere utilizzati per creare la configurazione Managed File Transfer richiesta e l'agent o il programma di registrazione.

Creare il membro BFGCUSTM come parte di questo processo.

Nota: Se si ha familiarità con i comandi USS, è possibile configurare z/OS con gli stessi comandi utilizzati su altre piattaforme.

Concetti correlati

“Configurazioni comuni di MFT per z/OS” a pagina 682
Una panoramica delle diverse configurazioni Managed File Transfer

“Modifica membro BFGCUSTM” a pagina 684
È necessario modificare il membro BFGCUSTM e immettere i valori per i parametri utilizzati dall'azienda prima di eseguire il job.

z/OS Modifica membro BFGCUSTM

È necessario modificare il membro BFGCUSTM e immettere i valori per i parametri utilizzati dall'azienda prima di eseguire il job.

Consultare Parametri necessari per il membro BFGCUSTM, per un elenco di parametri che richiedono valori specifici.

Inoltre, è necessario rivedere le seguenti variabili e fornire i valori, se necessario:

- Host coordinationQMgr=
- coordinationQMgrPorta =
- Canale coordinationQMgr=
- connectionQMgr=
- Host connectionQMgr=
- connectionQMgrPorta =
- Canale connectionQMgr=

Queste proprietà sono comuni a AGENT o LOGGER.

Nota: Host, Porta e Canale sono richiesti per la connessione client, ma devono essere lasciati vuoti per una connessione di bind sulla macchina locale.

Se questo è il primo gestore code nell'ambiente Managed File Transfer e si desidera utilizzare lo stesso gestore code per il coordinamento, i comandi e gli agenti in esecuzione, impostare i valori sul nome del gestore code locale.

```
coordinationQMgr=MQPV
connectionQMgr=MQPV
```

dove MQPV è il nome del gestore code locale.

Inoltrare il lavoro, che aggiorna il PDSE e crea una struttura di directory nel percorso specificato.

Notare che questo lavoro richiede l'utilizzo esclusivo, quindi è necessario smettere di utilizzare PSDE durante l'esecuzione del lavoro.

Suggerimento: Ogni volta che si inoltra il lavoro BFGCUSTM, il lavoro sostituisce tutti i file JCL. È necessario ridenominare ogni membro modificato.

Concetti correlati

“Prima di iniziare” a pagina 678
La configurazione Managed File Transfer (MFT) utilizza i file nei dataset USS (UNIX System Services) e PDSE.

“Creazione di un agent” a pagina 686
È necessario copiare PDSE per rendere il PDSE specifico dell'agente, ad esempio *user.MFT.AGENT1*. Copiare il PDSE da una precedente configurazione del programma di registrazione o dell'agent, se esistono. Se questa è la prima configurazione, copiare il PDSE fornito con MFT.

z/OS Definizione del gestore code di coordinamento

Managed File Transfer richiede la creazione di un gestore code che funga da gestore code di coordinamento.

In base alla configurazione scelta, questo gestore code si trova sul sistema MVS locale o su un'altra macchina. Nel primo caso, le connessioni ad esso sono connessioni di bind e nel secondo caso, sono connessioni client.

Una volta eseguito correttamente il passaggio di configurazione, ci sono membri configurati nel PDSE.

Il membro BFGCFCR definisce il gestore code di coordinamento e questo lavoro:

1. Crea una struttura di directory nella directory Managed File Transfer (MFT) e crea file di configurazione.
2. Esegue CSQUTIL per definire le risorse IBM MQ .

Se il gestore code di coordinamento è su una macchina remota, questo passo del lavoro ha esito negativo.

Il membro BCFCFCR crea i file in USS e crea definizioni MQ . Questo lavoro:

1. Crea un argomento MFT,
2. Crea una coda MFT
3. Modifica *NAMELIST (SYSTEM.QPUBSUB.QUEUE.NAMELIST)* per essere *NAMES (SYSTEM.BROKER.DEFAULT.STREAM, SYSTEM.BROKER.ADMIN.STREAM, SYSTEM.FTE)*
4. Esegue *ALTER QMGR PSMODE (ENABLED)*

   Un *DISPLAY NAMELIST (SYSTEM.QPUBSUB.QUEUE.NAMELIST)* viene emesso prima di eseguire la modifica. Se NAMLIST non è il valore predefinito, è necessario modificare l'elenco dei nomi per aggiungere SYSTEM.FTE al tuo elenco nomi

Ridenominare il membro BCFCFCR con il proprio prefisso, ad esempio CCPCFCR, poiché la personalizzazione di questo file lo sostituisce.

Modificare questo membro ridenominato inserendo il nome del proprio file di credenziali. Ad esempio:

```
%BFGCMD CMD=fteSetupCoordination +
-credentialsFile //'<MFTCredentialsDataSet(MemberName)>'
```

Salvare e inoltrare il lavoro. Notare che se è necessario inoltrare nuovamente il lavoro, è necessario aggiungere l'opzione *-f* .

Quando questo job viene eseguito, elenca le risorse IBM MQ che crea. È necessario proteggere queste risorse.

```
DEFINE TOPIC('SYSTEM.FTE') TOPICSTR('SYSTEM.FTE') REPLACE
ALTER TOPIC('SYSTEM.FTE') NPMSGDLV(ALLAVAIL) PMSGDLV(ALLAVAIL)
DEFINE QLOCAL(SYSTEM.FTE) LIKE(SYSTEM.BROKER.DEFAULT.STREAM) REPLACE
ALTER QLOCAL(SYSTEM.FTE) DESCR('Stream for MFT Pub/Sub interface')
* Altering namelist: SYSTEM.QPUBSUB.QUEUE.NAMELIST
* Value prior to alteration:
DISPLAY NAMELIST(SYSTEM.QPUBSUB.QUEUE.NAMELIST)
ALTER NAMELIST(SYSTEM.QPUBSUB.QUEUE.NAMELIST) +
NAMES(SYSTEM.BROKER.DEFAULT.STREAM+
,SYSTEM.BROKER.ADMIN.STREAM,SYSTEM.FTE)
* Altering PSMODE. Value prior to alteration:
DISPLAY QMGR PSMODE
ALTER QMGR PSMODE(ENABLED)
```

Attività correlate

“Definizione del gestore code comandi” a pagina 685
È possibile utilizzare lo stesso gestore code dei gestori code comandi e di coordinamento oppure creare un nuovo gestore code comandi.

z/OS Definizione del gestore code comandi

È possibile utilizzare lo stesso gestore code dei gestori code comandi e di coordinamento oppure creare un nuovo gestore code comandi.

Informazioni su questa attività

È necessario disporre di un gestore code comandi, tuttavia, è possibile utilizzare lo stesso gestore code per i gestori code comandi e di coordinamento. Altrimenti, è necessario creare un nuovo gestore code comandi. Può trovarsi sulla stessa macchina del gestore code di coordinamento, ma non è necessario.

Procedura

1. Ridenominare il membro BFGCMCR con il proprio prefisso, ad esempio CCPCMCR.
   È necessario ridenominare BFGCMCR poiché la ripersonalizzazione di questo file lo sostituisce.
2. Modificare il membro rinominato inserendo il nome del file delle credenziali.
   Ad esempio:

```
%BFGCMD CMD=fteSetupCommands +
-credentialsFile //'<MFTCredentialsDataSet(MemberName)>' +
```

3. Salvare e inoltrare il lavoro.
   Notare che se è necessario inoltrare nuovamente il lavoro, è necessario aggiungere l'opzione *-f* .
   Questo gestore code viene utilizzato per comandi quali **ftePingAgent**.
4. Esaminare questo membro, inoltrarlo e rivedere l'output.

Operazioni successive

Consultare “Creazione di un agent” a pagina 686 per informazioni su come creare un agente.

Concetti correlati

“Definizione del gestore code di coordinamento” a pagina 684
Managed File Transfer richiede la creazione di un gestore code che funga da gestore code di coordinamento.

Attività correlate

Configurazione di MQMFTCredentials.xml

Riferimenti correlati

Formato file credenziali MFT

z/OS Creazione di un agent

È necessario copiare PDSE per rendere il PDSE specifico dell'agente, ad esempio *user.MFT.AGENT1*. Copiare il PDSE da una precedente configurazione del programma di registrazione o dell'agent, se esistono. Se questa è la prima configurazione, copiare il PDSE fornito con MFT.

Esaminare il membro BFGCUSTM e se è necessario utilizzare un file di credenziali differente, crearne uno.

Gran parte del contenuto rimane lo stesso dalla personalizzazione descritta in “Modifica membro BFGCUSTM” a pagina 684.

È necessario modificare:

- // SYSEXEC DD DSN=SCEN.FTE.JCL.AGENT1
- LIBRARY per corrispondere al PDSE dell'agente
- TIPO_SERVIZIO=AGENT
- NAME deve essere il nome dell'agent (corrispondente al PDSE) JOBCARD
- Modifica di BFG_JVM_PROPERTIES = "-Xmx1024M"

Inoltrare questo lavoro, ricordando che il lavoro richiede l'accesso esclusivo al dataset.

I lavori per l'agente hanno tutti i nomi nel formato *BFGAG**

Ridenominare il membro *BFGAGCR*. Questo lavoro aggiorna i file nella directory Managed File Transfer e utilizza CSQUTIL per creare code specifiche dell'agente nel gestore code locale. Specificare il nome del file delle credenziali, ad esempio `-credentialsFile //'SCEN.FTE.JCL.VB(CREDOLD)`. Se non si specifica il nome, il lavoro per avviare l'agente non utilizza un file di credenziali.

Controllare l'output per assicurarsi che il processo sia eseguito correttamente.

Suggerimento: Copiare il percorso del file *agent.properties* dall'output del lavoro a un membro nel PDSE per l'agente.

Ad esempio, copiare `/u/userid/fte/wmqmft/mqft/config/MQPA/agents/AGENT1/agent.properties` nel membro AGENT.

Ciò è utile se è necessario visualizzare il file delle proprietà e aggiungere la riga `/u/userid/fte/wmqmft/mqft/logs/MQPA/agents/AGENT1/logs`.

Questo è il punto in cui vengono memorizzati i file di traccia.

Concetti correlati

"Definizione del gestore code di coordinamento" a pagina 684
Managed File Transfer richiede la creazione di un gestore code che funga da gestore code di coordinamento.

"Utilizzo dell'agente" a pagina 687
Come utilizzare i vari comandi per garantire che l'agent funzioni correttamente.

Attività correlate

"Definizione del gestore code comandi" a pagina 685
È possibile utilizzare lo stesso gestore code dei gestori code comandi e di coordinamento oppure creare un nuovo gestore code comandi.

z/OS Utilizzo dell'agente

Come utilizzare i vari comandi per garantire che l'agent funzioni correttamente.

Avviare l'agent

Rinominare il membro BFGAGST, esaminare il membro e inoltrare il lavoro.

Se funziona, si riceve il messaggio BFGAG0059I: l'agent è stato avviato correttamente.

Visualizza gli agent attivi

Ridenominare il membro BFGAGLI, esaminare il membro e inoltrare il lavoro che utilizza il gestore code di coordinamento.

È necessario risolvere eventuali problemi di connettività

Eseguire il ping dell'agent per verificarne il funzionamento

Ridenominare il membro BFGAGPI, esaminare il membro e inoltrare il lavoro che utilizza il gestore code comandi.

È necessario risolvere eventuali problemi di connettività

Effettuare un trasferimento di prova

Consultare "Esecuzione di un trasferimento di verifica" a pagina 695 per ulteriori informazioni.

Arrestare l'agent

Ridenominare il membro BFGAGSP, esaminare il membro e inoltrare il lavoro.

Riavviare l'agent utilizzando il membro BFGAGST.

Concetti correlati

"Creazione di un agent" a pagina 686
È necessario copiare PDSE per rendere il PDSE specifico dell'agente, ad esempio *user.MFT.AGENT1*. Copiare il PDSE da una precedente configurazione del programma di registrazione o dell'agent, se esistono. Se questa è la prima configurazione, copiare il PDSE fornito con MFT.

z/OS Aggiornamento di un dataset del comando Logger o dell'agent MFT esistente su z/OS

È possibile aggiornare un dataset della libreria PDSE di comandi Managed File Transfer creato dal dataset del modello di comandi Managed File Transfer .

Procedura

1. Modificare il membro dello script JCL BFGCUSTM e aggiornare le variabili e proprietà nell'istruzione DD BFGSTDIN.

   Se si desidera rimuovere una proprietà precedentemente definita, impostare il relativo valore su uno spazio vuoto, invece di rimuovere la voce. Quando viene eseguito lo script JCL BFGCUSTM, le proprietà specificate vengono applicate come un aggiornamento ai file delle proprietà UNIX System Services dell'agent e del programma di registrazione; l'impostazione di una proprietà su un valore vuoto indica che la proprietà deve essere rimossa
2. Inoltrare il lavoro BFGCUSTM. Questo lavoro genera nuovamente la serie di comandi JCL, appropriati per l'agent o il programma di registrazione. Per un elenco completo dei comandi, consultare “Script JCL del comando del logger e dell'agent z/OS” a pagina 693. Esaminare il log del lavoro di output per controllare che lo script JCL sia stato eseguito correttamente. In caso di errori, correggerli e inoltrare nuovamente il lavoro BFGCUSTM.

Risultati

È possibile modificare gli script JCL generati e aggiungere la propria logica. Tuttavia, prestare attenzione quando si esegue nuovamente BFGCUSTM perché si potrebbe sovrascrivere la logica personalizzata.

Concetti correlati

“MFT opzioni di configurazione su z/OS” a pagina 671
Le Managed File Transfer opzioni di configurazione su z/OS sono uguali alle opzioni per le piattaforme distribuite.

Attività correlate

“Creazione di un dataset del comando Logger o dell'agent MFT” a pagina 676
È possibile creare un dataset PDSE di comandi dal dataset del modello di comando Managed File Transfer per un Managed File Transfer Agent specifico o Managed File Transfer Logger per un coordinamento specifico.

z/OS *z/OS variabili JCL*

È possibile utilizzare valori di sostituzione, variabili JCL e proprietà di configurazione nello script BFGCUSTM.

La seguente tabella elenca i valori di sostituzione per lo script JCL BFGCUSTM in un dataset della libreria PDSE del comando MFT . È necessario sostituire questi valori di sostituzione con valori appropriati prima di inoltrare il lavoro BFGCUSTM.

Tabella 44. Valori di sostituzione per lo script JCL BFGCUSTM

Variabile di sostituzione	Valore
+ + libreria + +	Il nome del dataset della libreria PDSE del comando MFT contenitore.
+ + bfg_java_home + +	L'ubicazione dell'installazione di Java .
+ + bfg_prod + +	L'ubicazione della directory root dei servizi di sistema UNIX di installazione del prodotto MFT .

La tabella riportata di seguito descrive le variabili di ambiente per l'istruzione DD BFGSTDIN per lo script JCL BFGCUSTM, in un dataset della libreria PDSE del comando MFT (nella sezione [Variabili]). È

necessario sostituire tutte le variabili specificate con valori di sostituzione (ovvero, valori racchiusi tra due segni più, + +) con valori appropriati prima di inoltrare il lavoro BFGCUSTM.

Tabella 45. Variabili di ambiente

Variabile di ambiente	**Valore**
LIBRARY	Il nome del dataset della libreria PDSE del comando MFT contenitore.
TMPDIR	Directory UNIX System Services per i file temporanei.
BFG_PROD	L'ubicazione della directory root dei servizi di sistema UNIX di installazione del prodotto MFT .
DATI_BFG	L'ubicazione della directory di dati per Managed File Transfer per z/OS, che è il percorso a *DATA_DIR*.
BFG_JAVA_HOME	L'ubicazione dell'installazione di Java .
BFG_JVM_PROPERTIES	Facoltativo. Imposta un valore per la variabile di ambiente BFG_JVM_PROPERTIES. Queste proprietà vengono trasmesse alla macchina virtuale Java .

Tabella 45. Variabili di ambiente (Continua)

Variabile di ambiente	Valore
NOME_GRUPPO_BF	Il gruppo di file mqm è generalmente associato ai comandi e ai file di dati di configurazione MFT . Di conseguenza, tutti gli utenti membri del gruppo mqm possono accedere e apportare modifiche alla configurazione di MFT . Per ulteriori informazioni, vedere Autorizzazioni del file system per MFT in IBM MQ. Per un sistema z/OS , un gruppo di file è un'entità di file system USS e il gruppo di file mqm non è necessariamente definito. È possibile associare un gruppo di file system z/OS USS per i file di dati di configurazione MFT utilizzando la variabile di ambiente BFG_GROUP_NAME. Ad esempio, al prompt della shell USS utilizzare: `export BFG_GROUP_NAME=FTEGB` che definisce un gruppo *FTEGB* da associare a qualsiasi file di configurazione creato successivamente per la sessione USS corrente. È possibile impostare BFG_GROUP_NAME su un valore vuoto o rimuoverlo. **Nota:** Quando si esegue BFGCUSTM per la prima volta, se la configurazione MFT deve essere utilizzata da più ID utente, è importante che BFG_GROUP_NAME sia impostato su un gruppo accessibile a tutti gli ID utente richiesti. Se BFGCUSTM viene eseguito di nuovo, BFG_GROUP_NAME non deve essere modificato (altrimenti, le autorizzazioni del file di gruppo USS per tutti i file e le directory nella directory a cui fa riferimento BFG_DATA devono essere modificate per riflettere la nuova impostazione BFG_GROUP_NAME). Se si esegue il comando **fteMigrateAgent** su un sistema z/OS con la variabile di ambiente BFG_GROUP_NAME impostata su un valore non vuoto, il comando controlla se l'utente è un membro del gruppo denominato dalla variabile BFG_GROUP_NAME. Se l'utente non si trova nel gruppo denominato, il comando potrebbe riportare il messaggio di errore `BFGCL0502E: non si è autorizzati ad eseguire l'operazione richiesta.` e non viene eseguito. Per i dettagli sui criteri che l'utente deve soddisfare per eseguire correttamente tale comando, consultare fteMigrateAgent .

Tabella 45. Variabili di ambiente (Continua)	
Variabile di ambiente	**Valore**
BFG_WTO	La registrazione z/OS è abilitata quando BFG_WTO è impostato su YES, ON o TRUE. Ciò controlla se i messaggi scritti nel log eventi dell'agent vengono scritti anche nella funzione di log dell'operatore z/OS , che consente un accesso più semplice per i prodotti di automazione quando si esegue un agent da JCL. Il codice di instradamento è Informazioni programmatore (11) e il codice descrittore è Informativo (12).
service_type	Specifica se la libreria comandi MFT è per un agente o un programma di registrazione. I valori validi sono AGENT o LOGGER.
NOME	Il nome dell'agent o del programma di registrazione per il valore SERVICE_TYPE.
QMGR	Il nome del gestore code locale associato all'agent o al logger per il valore SERVICE_TYPE.
CLASSE_OUTPUT	La classe di output per i dataset SYSOUT. Il valore predefinito è * che richiede la stessa classe di emissione del parametro MSGCLASS dall'istruzione del lavoro.
PERCORSO MQ	Utilizzato in BFGPROF per creare la variabile di ambiente LIBPATH.
MQ_HLQ	Il qualificatore di alto livello per i dataset IBM MQ .
MQ_LANG	La lingua richiesta.
DB2_HLQ	Facoltativo. Qualificatore di alto livello per i dataset Db2 .
JOBCARD1	Riga di intestazione 1 per un lavoro di comando JCL.
JOBCARD2	Riga intestazione 2 per un lavoro di comando JCL.
JOBCARD3	Riga intestazione 3 per un lavoro di comando JCL.
ADMIN_JOB1	Riga di intestazione 1 per un lavoro admin.
ADMIN_JOB2	Riga intestazione 2 per un lavoro di gestione.
ADMIN_JOB3	Riga intestazione 3 per un lavoro di gestione.
FTE_CONFIG	Configurazione WMQFTE esistente per la migrazione. Impostare su un valore vuoto se la migrazione non è richiesta.

Tabella 45. Variabili di ambiente (Continua)	
Variabile di ambiente	**Valore**
PERCORSO CREDENTIAL_PATH	Percorso del file delle credenziali per la migrazione, ad esempio `/u/user1/agent3`. I file delle credenziali per la migrazione per Managed File Transfer devono essere ubicati in un file separato per le informazioni di configurazione e i file di configurazione su IBM WebSphere MQ File Transfer Edition 7.0.4.4. Richiesto solo per i comandi di migrazione **BFGAGMG** e **BFGLGMG** JCL. Impostare su un valore vuoto se la migrazione non è richiesta.
PERCORSO_PROP_DB	Specifica il file delle proprietà del programma di registrazione database per la migrazione. Questa opzione è richiesta solo se il file delle proprietà non utilizza il seguente nome e percorso predefinito: `config_directory/coordination_qmgr/databaselogger.properties`. Impostare su un valore vuoto se la migrazione non è richiesta.

Nota: I file jar IBM MQ vengono forniti con MFT, nella directory *`MQMFT product root`*`/java/lib`, sono sempre utilizzati e non configurabili.

La seguente tabella descrive le proprietà di configurazione obbligatorie di MFT per l'istruzione DD BFGSTDIN per lo script JCL BFGCUSTM in un dataset della libreria PDSE del comando MFT . È necessario sostituire le proprietà specificate con valori di sostituzione (vale a dire, valori racchiusi tra due segni più, + +) con un valore non vuoto adatto prima di inoltrare il lavoro BFGCUSTM. Queste proprietà definiscono le sostituzioni per le proprietà di configurazione MFT . È possibile aggiungere le proprietà dell'agent e del logger per personalizzare gli agent o i logger per il proprio ambiente. Per un elenco di tutte le proprietà, consultare “File delle proprietà di configurazione” a pagina 701.

Tabella 46. Proprietà di configurazione obbligatorie per l'istruzione BFGSTDIN DD	
Proprietà	**Valore**
coordinationQMgr	Il nome del gestore code di coordinamento per la configurazione a cui è associato l'agent o il programma di registrazione.
Host coordinationQMgr	Facoltativo. Nome host del sistema su cui è in esecuzione il gestore code di coordinamento. Se si lascia vuoto il valore per questa proprietà, si presuppone una connessione in modalità bind.
Porta coordinationQMgr	Facoltativo. Numero di porta su cui è in ascolto il gestore code di coordinamento. Questo parametro viene utilizzato solo se si specifica anche un valore non vuoto per la proprietà Host coordinationQMgr.
Canale coordinationQMgr	Facoltativo. Canale da utilizzare per connettersi al gestore code di coordinamento. Questo parametro viene utilizzato solo se si specifica anche un valore non vuoto per la proprietà Host coordinationQMgr.
connectionQMgr	Il nome del gestore code comandi per la configurazione a cui è associato l'agent o il programma di registrazione.

Tabella 46. Proprietà di configurazione obbligatorie per l'istruzione BFGSTDIN DD (Continua)	
Proprietà	**Valore**
Host connectionQMgr	Facoltativo. Nome host del sistema su cui è in esecuzione il gestore code comandi. Se si lascia vuoto il valore per questa proprietà, si presuppone una connessione in modalità bind.
Porta connectionQMgr	Facoltativo. Numero di porta su cui è in ascolto il gestore code comandi. Questo parametro viene utilizzato solo se si specifica anche un valore non vuoto per la proprietà Host connectionQMgr.
Canale connectionQMgr	Facoltativo. Canale da utilizzare per la connessione al gestore code comandi. Questo parametro viene utilizzato solo se si specifica anche un valore non vuoto per la proprietà Host connectionQMgr.

z/OS *Script JCL del comando del logger e dell'agent z/OS*

La serie di comandi JCL disponibili in un dataset della libreria PDSE del comando MFT

Tabella 47. Comandi JCL disponibili in un dataset della libreria PDSE del comando MFT	
Membro	**Descrizione o comando della riga comandi fte**
BFGCOPY	Lavoro per creare una copia di questa libreria
BFGCUSTM	Lavoro per personalizzare questa libreria per l'agent o il logger
BFGCFCR	fteSetupCoordinamento
BFGCMCR	ComandifteSetup: creare il file MFT command.properties
BFGAGCR	fteCreateAgent. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
BFGLGCRS	fteCreateLogger. Creato solo quando si imposta la variabile SERVICE_TYPE su LOGGER.
GAGBF	Agente fteStart. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
BFGAGSTP	Procedura **fteStartAgent** . Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
BFGAGPI	Agent ftePing. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
BFGAGSP	fteStopAgent. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
GGGLBF	fteStartProgramma di registrazione. Creato solo quando si imposta la variabile SERVICE_TYPE su LOGGER.
GSTGGLBF	Procedura **fteStartLogger** . Creato solo quando si imposta la variabile SERVICE_TYPE su LOGGER.

Tabella 47. Comandi JCL disponibili in un dataset della libreria PDSE del comando MFT (Continua)	
Membro	**Descrizione o comando della riga comandi fte**
BFGLGSP	fteStopLogger. Creato solo quando si imposta la variabile SERVICE_TYPE su LOGGER.
BFGAGSH	fteShowAgentDetails. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
BFGLGSH	fteShowLoggerDetails. Creato solo quando si imposta la variabile SERVICE_TYPE su LOGGER.
BFGCFF	fteChangeDefaultConfigurationOpzioni
BFGAGCL	Agent fteClean. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
GAGBF	fteDeleteAgent. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
BFGLGDE	fteDeleteProgramma di registrazione. Creato solo quando si imposta la variabile SERVICE_TYPE su LOGGER.
BFGPRSH	fteDisplayVersione
BFGAGLI	fteListAgent. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
BFGMNLI	fteListMonitor
BFGSTLI	fteListScheduledTransfers
BFGTMLI	fteListModelli
BFGAGMG	**fteMigrateAgent**. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
BFGLGMG	**fteMigrateLogger**. Creato solo quando si imposta la variabile SERVICE_TYPE su LOGGER.
BFGCROBS	**fteObfuscate** esempio
BFGZRAS	**fteRAS**
GAGBF	fteSetAgentTraceLivello. Creato solo quando si imposta la variabile SERVICE_TYPE su AGENT.
BFGLGTC	fteSetLoggerTraceLivello. Creato solo quando si imposta la variabile SERVICE_TYPE su LOGGER.
BFGPRAN	**fteAnt** esempio
BFGTRCAS	**fteCancelTransfer** esempio
BFGMNCRS	**fteCreateMonitor** esempio
BFGTMCRS	**fteCreateTemplate** esempio
BFGTRCRS	**fteCreateTransfer** esempio
BFGMNDI	**fteDeleteMonitor** esempio
BFGSTDI	**fteDeleteScheduledTransfer** esempio
BFGTMDI	**fteDeleteTemplates** esempio

Note:

- Il JCL, per i comandi che creano MQSC o fanno riferimento a script di eliminazione, richiede di eseguire uno script, ma lo script è già stato eseguito dal job.
- BFGZRAS crea il membro BFGRAS quando viene eseguito il lavoro BGCUSTM.

z/OS Esecuzione di un trasferimento di verifica

Come si effettua un trasferimento per controllare che il prodotto funzioni correttamente.

Ridenominare e modificare il membro BFGTRCRS.

1. Aggiungere un `/*` prima del `%BFGCMD CMD=fteCreateTransfer -h`
2. Rimuovere gli altri commenti nel membro.
3. Specificare il nome agent corrente per `-sa` e `-da`
4. Salva il JCL
5. Inoltra il JCL

Questo JCL si connette al gestore code comandi.

z/OS Configurazione di un'attività di registrazione

L'attività di registrazione deve essere eseguita sulla stessa immagine del gestore code di coordinamento. È possibile accedere a Db2.

Creazione di un'attività di registrazione

Copiare il PDSE per rendere il PDSE specifico del programma di registrazione. Ad esempio, `user.MFT.LOGGER`.

Se è necessario utilizzare un file di credenziali diverso, crearne uno. Per ulteriori informazioni, consultare Configurazione di MQMFTCredentials.xml su z/OS.

Membro di riesame BFGCUSTM. Si noti che la maggior parte del contenuto rimane lo stesso della personalizzazione precedente.

Tuttavia, è necessario:

- Modificare // SYSEXEC DD DSN=SCEN.FTE.JCL....
- Modificare LIBRARY in modo che corrisponda al PDSE agent
- Modificare QMGR con il nome del gestore code di coordinamento
- Rendi TIPO_SERVIZIO=LOGGER
- Modificare NAME in modo che sia il nome del programma di registrazione (corrispondente al PDSE)
- Rivedere JOBCARD e modificare il nome lavoro in modo che sia diverso dai nomi lavoro degli agent.
- Esaminare BFG_JVM_PROPERTIES = "-Xmx1024M"

Se si utilizza il programma di registrazione Db2 , è utile creare un file, in modo da poter catturare le tracce Db2 per identificare i problemi Db2 .

Il nome del file viene specificato nelle proprietà JVM, in cui il file delle proprietà di traccia JDBC ha il contenuto come

```
db2.jcc.traceDirectory=/u/johndoe/fte
db2.jcc.traceFile=jccTrace1
db2.jcc.traceFileAppend=false
# turn on all traces
# db2.jcc.traceLevel=-1
# turn off all traces
db2.jcc.traceLevel=0
```

Imposta due proprietà JVM

```
BFG_JVM_PROPERTIES=-Ddb2.jcc.propertiesFile=/u/.../sql.properties
-Ddb2.jcc.ssid=DBCA
```

dove `/u/.../sql.properties` è il nome del file delle proprietà di traccia Db2 e *DBCA* è il nome del sottosistema Db2 .

Inoltrare questo lavoro, notando che il lavoro richiede accesso esclusivo al dataset. I lavori per l'agent hanno tutti nomi come *BFGLG**.

Registrazione nei file

Per ulteriori informazioni sulla registrazione in Db2, consultare “Creazione di un'attività di registrazione, quando si accede a Db2” a pagina 697

Ridenominare il membro BFGLGCRS. Questo lavoro aggiorna i file nella directory Managed File Transfer (MFT) e utilizza CSQUTIL per creare code specifiche dell'agente nel gestore code locale.

Il file originale ha il comando `%BFGCMD CMD=fteCreateLogger -h` che elenca la sintassi del comando.

To create the logger task comment out the `%BFGCMD CMD=fteCreateLogger -h` by putting `/*` in front of the statement, making sure that column one is blank.

Rimuovere i commenti dal secondo comando e configurare le istruzioni. Ad esempio:

```
%BFGCMD CMD=fteCreateLogger   +
-p MQPH     +
-loggerQMgr MQPH      +
-loggerType FILE        +
-fileLoggerMode circular    +
-fileSize 5MB +
-fileCount 5 +
-p MQPH +
-credentialsFile //'<MFTCredentialsDataSet(MemberName)>'
LOGGER
```

Controllare l'output per verificare che sia stato elaborato correttamente.

Suggerimento: Copiare il nome percorso del file `logger.properties` dall'emissione del lavoro ad un membro nel PDSE dell'agente.

Ad esempio, copia nel membro APATH

```
/u/user_ID/fte/wmqmft/mqft/config/MQPH/loggers/LOGGER/logger.properties
```

Ciò è utile se è necessario visualizzare il file delle proprietà.

Aggiungere la directory a questo file:

```
/u/user_ID/fte/wmqmft/mqft/logs/MQPH/loggers/LOGGER/
```

Se si sta eseguendo l'accesso al file, i file di log vengono memorizzati in questa directory, ad esempio `LOGGER0-20140522123654897.log`.

I file di traccia si trovano nella sottodirectory di log, ad esempio

```
/u/user_ID/fte/wmqmft/mqft/logs/MQPH/loggers/LOGGER/logs
```

È ora possibile avviare l'attività di registrazione.

Creazione di un'attività di registrazione, quando si accede a Db2

Ridenominare il membro BFGLGCRS.

Questo lavoro aggiorna i file nella directory MFT e utilizza CSQUTIL per creare code specifiche dell'agente nel gestore code locale.

Devi sapere:

Tabella 48. Db2 variabili

Nome Db2	**Esempio**
-dbName databaseName	È possibile ottenere questo valore dal valore di posizione nel messaggio DSNL004I per il proprio sottosistema Db2
- dbDriver filePath	Ad esempio `/db2/db2v10/jdbc/classes/db2jcc.jar`
-dbLib filePath	Ad esempio `/db2/db2v10/jdbc/lib/libdb2jcct2zos_64.so`

Modifica il file. Il file originale ha il comando `%BFGCMD CMD=fteCreateLogger -h` che elenca la sintassi del comando.

Rimuovere i commenti dal secondo comando e configurare le istruzioni. Per esempio

```
%BFGCMD CMD=fteCreateLogger   +
-p MQPH     +
-loggerQMgr MQPH      +
-loggerType DATABASE      +
-dbType DB2           +
-dbName DSNDBCP         +
-dbDriver /db2/db2v10/jdbc/classes/db2jcc.jar  +
-dbLib /db2/db2v10/jdbc/lib/            +
-credentialsFile //'<MFTCredentialsDataSet(MemberName)>' +
LOGGER
```

To create the logger task comment out the `%BFGCMD CMD=fteCreateLogger -h` by putting `/*` in front of the statement, making sure that column one is blank.

Inoltrare il lavoro e controllare l'output per verificare che sia stato elaborato correttamente.

Suggerimento: Copiare il nome percorso del file `logger.properties` dall'emissione del lavoro a un membro nel PDSE degli agenti.

Ad esempio, copiare nel membro APATH:

```
/u/user_ID/fte/wmqmft/mqft/config/MQPH/loggers/LOGGER/logger.properties into member USS
```

Ciò è utile se è necessario visualizzare il file delle proprietà

I file di traccia si trovano nella sottodirectory di log, ad esempio:

```
/u/user_ID/fte/wmqmft/mqft/logs/MQPH/loggers/LOGGER/logs
```

Creazione di tabelle Db2

È necessario creare le tabelle Db2 . Le definizioni si trovano nel file USS `mqft/sql/ftelog_tables_zos.sql`.

Creare un membro Db2 nel PDSE. Modificare questo membro e usare il comando COPY sulla riga comandi. Copiare dal file di definizioni USS.

Poiché i requisiti specifici del sito possono variare notevolmente, questo file specifica solo le strutture di base delle tabelle e un tablespace in cui si trovano.

Lo spazio tabella viene specificato, mediante lo script SQL, per garantire che venga creato utilizzando un pool di buffer con una dimensione di pagina sufficiente a contenere le righe di tabelle più grandi possibili. Notare che gli attributi come le ubicazioni LOB e così via non vengono specificati.

L'amministratore del database potrebbe voler modificare una copia di questo file, per definire questi attributi relativi alle prestazioni.

Questo file assume anche un nome schema predefinito di FTEL0G, un nome tablespace predefinito di FTEL0GTSe un nome database FTEL0GDB. È possibile modificare questi nomi se necessario, in modo che corrispondano a un database esistente e a qualsiasi convenzione di denominazione locale, seguendo il processo descritto nei commenti all'inizio del file.

Importante: Utilizzare funzioni in linea come **SPUFI** per eseguire i comandi, poiché nel file sono presenti commenti e i programmi batch come **DSNTINAD** non accettano commenti.

Avvio dell'attività del logger

Ridenominare, esaminare e inoltrare il membro BFGLGST. Si dovrebbe ricevere il messaggio BFGDB0023I: il programma di registrazione ha completato attività di avvio ed è ora in esecuzione.

Operazioni logger

Per visualizzare lo stato del programma di registrazione, ridenominare, esaminare e inoltrare il membro BFGLGSH

Per arrestare il programma di registrazione, rinominare, rivedere e inoltrare il membro BFGLGSP.

z/OS Variabili di ambiente per MFT su z/OS

Se si stanno eseguendo comandi direttamente dall'ambiente USS o dai propri script JCL, dopo la personalizzazione e la configurazione è necessario impostare un numero di variabili di ambiente prima di eseguire gli script di configurazione e di gestione forniti da Managed File Transfer. È necessario impostare queste variabili per ogni utente e in ogni ambiente da cui verranno richiamati gli script.

Per evitare conflitti con altri prodotti, è possibile scegliere di creare uno script di `.wmqfterc` nella directory home. Lo script `.wmqfterc` viene quindi richiamato da ogni script Managed File Transfer ed è possibile utilizzare questo script per fornire impostazioni di ambiente personalizzate per Managed File Transfer.

Esiste anche una variabile di ambiente facoltativa, BFG_WTO, che è possibile impostare per inviare messaggi al log dell'operatore durante l'esecuzione di agent da JCL.

Tabella 49. Variabili di ambiente z/OS richieste

Variabile di ambiente	**Valore**
BFG_JAVA_HOME	L'ubicazione dell'installazione di Java . Per ulteriori informazioni sui livelli di Java supportati, consultare Requisiti di sistema per IBM MQ.
DATI_BFG	L'ubicazione della directory di dati per Managed File Transfer for z/OS. Questo è il percorso per *DATA_DIR*.

Tabella 49. Variabili di ambiente z/OS richieste (Continua)	
Variabile di ambiente	**Valore**
STEPLIB	Deve includere i seguenti dataset IBM MQ : • SCSQAUTH • SSQANLE • SSQLOAD Se si desidera eseguire il componente del programma di registrazione database su un sistema z/OS , STEPLIB deve includere anche i seguenti dataset Db2 nell'ordine mostrato: • SDSNEXIT • SDSNLOD2 • SDSNLOAD
LIBPATH	Deve includere l'ubicazione delle librerie IBM MQJava nello spazio z/OS UNIX System Services (per IBM MQ 8.0, il valore predefinito è `/mqm/V8R0M0/java/lib`).

Di seguito viene riportato un `.profile` di esempio che configura correttamente le variabili di ambiente per Managed File Transfer:

```
LIBPATH=/mqm/V8R0M0/java/lib:$LIBPATH
STEPLIB=MQM.V800.SCSQAUTH:MQM.V800.SCSQANLE:MQM.V800.SCSQLOAD
PATH=/u/fteuser/bin:/u/fteuser/J7.0/bin:/bin:/usr/bin:/u/fteuser/extras/bin:/bin:$PATH
BFG_JAVA_HOME=/u/fteuser/J7.0
BFG_DATA=/u/fteuser/DATA_DIR
export PATH LIBPATH STEPLIB BFG_JAVA_HOME BFG_DATA
```

Facoltativamente, è anche possibile impostare le seguenti variabili di ambiente:

Tabella 50. Variabile di ambiente z/OS facoltativa

Variabile di ambiente	**Valore**
BFG_WTO	Uno dei seguenti valori abiliterà BFG_WTO: • Sì • SU • TRUE Uno dei seguenti valori disabiliterà BFG_WTO. Questi valori non sono sensibili al maiuscolo / minuscolo. • NULL • NO • OFF • FALSE Abilita la registrazione z/OS . Per impostazione predefinita, questa variabile di ambiente è disabilitata. I messaggi scritti nel log eventi dell'agent vengono scritti anche nella funzione di log dell'operatore z/OS , che consente un accesso più semplice per i prodotti di automazione quando si esegue un agent da JCL. Il codice di instradamento è Informazioni programmatore (11) e il codice descrittore è Informativo (12).

Tabella 50. Variabile di ambiente z/OS facoltativa (Continua)	
Variabile di ambiente	**Valore**
NOME_GRUPPO_BF	Il gruppo di file `mqm` è generalmente associato a comandi e file di dati di configurazione Managed File Transfer . Di conseguenza, tutti gli utenti che sono membri del gruppo `mqm` possono accedere e apportare modifiche alla configurazione Managed File Transfer . Per ulteriori informazioni, vedere Autorizzazioni del file system per MFT in IBM MQ. Per un sistema z/OS , un gruppo di file è un'entità del file system USS e il gruppo di file `mqm` non è necessariamente definito. È possibile definire un altro gruppo di file system USS z/OS esistente per i file di dati di configurazione Managed File Transfer utilizzando la variabile di ambiente BFG_GROUP_NAME. Ad esempio, al prompt della shell USS: `export BFG_GROUP_NAME=FTEGB` che definisce il gruppo FTEGB da associare ai file di configurazione creati successivamente per la sessione USS corrente. È possibile impostare BFG_GROUP_NAME su un valore vuoto o rimuoverlo. Se si esegue il comando **fteMigrateAgent** su un sistema z/OS con la variabile di ambiente BFG_GROUP_NAME impostata su un valore non vuoto, il comando controlla se l'utente è un membro del gruppo denominato dalla variabile BFG_GROUP_NAME. Se l'utente non si trova nel gruppo denominato, il comando potrebbe riportare il messaggio di errore `BFGCL0502E: non si è autorizzati ad eseguire l'operazione richiesta.` e non viene eseguito. Per i dettagli sui criteri che l'utente deve soddisfare per eseguire correttamente tale comando, consultare fteMigrateAgent .

z/OS File delle proprietà di configurazione

Un riepilogo delle proprietà utilizzate in Managed File Transfer.

- Il file MFT coordination.properties
- Il file MFT command.properties
- Il file MFT agent.properties
- File delle proprietà di configurazione del programma di registrazione

z/OS Configurazione di MFT per z/OS ARM (Automatic Restart Manager)

Managed File Transfer è un'applicazione abilitata ARM.

Prima di iniziare

Per ulteriori informazioni sull'abilitazione di ARM e sulla definizione delle politiche ARM per il proprio sistema, consultare Utilizzo di z/OS ARM (Automatic Restart Manager).

Se si desidera utilizzare la funzione Logger DB MFT per riavviare automaticamente e riconnettersi a un database Db2 , ARM è l'unico gestore di riavvio supportato disponibile.

Informazioni su questa attività

Utilizzando ARM, gli agenti e i logger possono essere configurati per il riavvio impostando le proprietà agent / logger armELEMTYPEe armELEMENT. La proprietà armELEMTYPE definisce il tipo di elemento ARM e la proprietà armELEMENT è il nome dell'elemento che ARM deve registrare:

- È possibile impostare l'agent ELEMTYPE su SYSBFGAG e armELEMENT può essere impostato in modo da corrispondere al nome dell'agent.
- È possibile impostare il programma di registrazione ELEMTYPE su SYSBFGLG e armELEMENT può essere impostato in modo da corrispondere al nome del programma di registrazione.

Nota: Gli agent e i logger configurati per il riavvio da ARM possono essere eseguiti correttamente solo da un lavoro batch o da un'attività avviata. I tentativi di avviare l'agente o il programma di registrazione direttamente dalla riga comandi USS avranno esito negativo con un codice di errore ARM.

Esempio

Il seguente esempio di un criterio di riavvio definisce l'agent BFGFT7CAG1 come dipendente dal gestore code FT7C: :

```
RESTART_ORDER
   LEVEL(3)
   ELEMENT_TYPE(SYSBFGAG,SYSBFGLG)

RESTART_GROUP(GROUP7C)
   ELEMENT(SYSMQMGRFT7C)
   ELEMENT(BFGFT7CAG1)
       RESTART_ATTEMPTS(3,300)
```

z/OS Esempio: creazione di JCL per agent Managed File Transfer su z/OS

Utilizzare queste informazioni per creare alcuni JCL che possono essere utilizzati per creare e avviare un agent su IBM MQ for z/OS.

Copia la libreria di esempio

Effettuare la seguente procedura:

1. Eseguire una copia della libreria SBFGCMDS (consultare “Copia SBFGCMDS per creare una libreria JCL” a pagina 683) aprendo la libreria.

   La maggior parte dei membri, quelli che iniziano con BFGX, BFGY o BFGZ, sono modelli che vengono utilizzati per generare il JCL personalizzato per l'agent in seguito.

   Il membro importante è BFGCOPY.
2. Aprire BFGCOPY e sostituire:

   + + libreria_fornita + +
   con il nome della libreria SBFGCMDS installata come parte del prodotto.

   + + libreria dei servizi + +
   con il nome della libreria che si desidera utilizzare per l'agente (la libreria di destinazione).
3. Inoltrare il lavoro e si dispone di una nuova libreria che è possibile utilizzare.

Modifica BFGCUSTM

Effettuare la seguente procedura:

1. Aprire la nuova libreria in modo da poter modificare il membro BFGCUSTM (consultare “Modifica membro BFGCUSTM” a pagina 684)
2. Modificare tutti i parametri nel membro racchiusi tra ++ caratteri e sostituirli con i valori appropriati. Ad esempio, modificare:

   + + bfg_prod + +
   Puntare alla directory USS in cui è stato installato IBM MQ Managed File Transfer for z/OS .

   + + bfg_dati + +
   Per essere la directory USS in cui deve essere memorizzata la propria configurazione IBM MQ Managed File Transfer for z/OS .

   + + tipo_servizio + +
   alla parola AGENT

   + + nome_agent + +
   Per essere il nome del tuo agente

Note:

1. Alcune delle voci, come ad esempio ++options++ richiesto per CLEAN_AGENT_PROPS, non sono necessarie, pertanto è necessario rimuoverle.
2. Consultare “Prima di iniziare” a pagina 678 per un elenco completo di tutti i parametri nel membro BFGCUSTM, insieme a una descrizione dei valori che devono avere.

Inoltrare il JCL BFGCUSTM

Effettuare la seguente procedura:

1. Inoltrare il lavoro.
2. Uscire dalla libreria in ISPF.

   Ciò è necessario perché il lavoro BFGCUSTM sta aggiornando la libreria e non può farlo mentre la libreria è aperta.
3. Una volta completato il lavoro, consultare la registrazione lavori.

   Verrà visualizzato un numero di messaggi, che indicano che sono stati creati nuovi membri all'interno della libreria.

   Ognuno di questi membri contiene JCL che può essere utilizzato per eseguire attività specifiche per l'agente. Consultare “Script JCL del comando del logger e dell'agent z/OS” a pagina 693 per un elenco di questi membri, insieme ai comandi IBM MQ Managed File Transfer a cui corrispondono.

Inoltra BFGAGCR per creare l'agent

Il nuovo membro BFGAGCR contiene alcuni JCL che creano un agent richiamando il comando **`fteCreateAgent`** .

Effettuare la seguente procedura:

1. Aprire il membro BFGAGCR.

   Dovresti vedere che BFGAGCR è stato popolato con il nome del tuo:

   - Agent
   - Gestore code agent
   - Il gestore code di coordinamento per la topologia MFT
2. Inoltrare il membro BFGAGCR.

   Quando il membro viene eseguito:

- Crea i file di configurazione richiesti per l'agent.
- Si connette al gestore code dell'agent e crea le code di sistema di cui l'agent ha bisogno, utilizzando CSQUTIL.
- Registra l'agent con il gestore code di coordinamento.

Avviare l'agent inoltrando BFGAGST

Effettuare la seguente procedura:

1. Inoltrare il membro BFGAGST. Consultare utilizzo dell'agente per i vari comandi che mostrano il funzionamento corretto dell'agente.
2. Una volta completato il lavoro, verificare che la registrazione lavori contenga i seguenti messaggi:

   ```
   BFGAG0058I: The agent has successfully initialized.
   BFGAG0059I: The agent has been successfully started.
   ```

   che significa che l'agente è attivo, in esecuzione e pronto per eseguire i trasferimenti gestiti.

z/OS Spostamento di un agent MFT in una nuova LPAR z/OS

A volte è necessario spostare un agent IBM MQ Managed File Transfer for z/OS da una LPAR all'altra, mantenendo l'agent nella stessa topologia IBM MQ Managed File Transfer con gli stessi gestori code comandi e di coordinamento. Le operazioni necessarie per eseguire questa operazione dipendono dal modo in cui l'agente migrato è stato originariamente creato.

Informazioni su questa attività

Spostare l'agent IBM MQ Managed File Transfer for z/OS in uno dei seguenti modi:

- Se l'agent è stato originariamente creato utilizzando una versione personalizzata della libreria SBFGCMDS, utilizzare la libreria per ricrearlo su una nuova LPAR.
- Se l'agent è stato originariamente creato eseguendo i comandi USS, utilizzare i comandi per ricrearlo su una nuova LPAR.

Nota:

I trasferimenti pianificati e i modelli di trasferimento vengono memorizzati sul gestore code di coordinamento per una topologia IBM MQ Managed File Transfer . Questa attività presuppone che il gestore code di coordinamento non faccia parte del lavoro di spostamento. In questo caso, tutti i trasferimenti pianificati e i modelli di trasferimento associati all'agent da spostare rimangono sul gestore code di coordinamento esistente una volta completato lo spostamento.

Procedura

- Spostare un agent creato utilizzando una versione personalizzata della libreria SBFGCMDS.

  Se l'agent è stato creato utilizzando una versione personalizzata della libreria SBFGCMDS, è possibile utilizzare tale libreria per ricreare l'ambiente IBM MQ Managed File Transfer for z/OS e la configurazione dell'agent sulla nuova LPAR. Per effettuare questa operazione, completa la seguente procedura:

  1. Copiare la versione personalizzata della libreria dalla LPAR originale alla nuova LPAR.
  2. Modificare il membro BFGCUSTM nella versione personalizzata della libreria sulla nuova LPAR e assicurarsi che i valori del parametro siano ancora validi.
  3. Eseguire il membro BFGCUSTM sulla nuova LPAR per creare tutto il JCL necessario per configurare l'ambiente e creare l'agente.
  4. Eseguire il componente BFGCFCR per definire il gestore code di coordinamento che deve essere utilizzato dall'agent sulla nuova LPAR e creare la struttura di directory necessaria per memorizzare la configurazione di IBM MQ Managed File Transfer .

5. Successivamente, eseguire il membro BFGCMCR per definire il gestore code comandi che deve essere utilizzato dall'agente sulla nuova LPAR.
6. Eseguire il membro BFGAGCR per creare nuovamente l'agente e la sua configurazione.
7. Verificare che le code di sistema utilizzate dall'agente esistano sul gestore code per tale agente.

Se all'agent che si sta spostando sono associati dei monitoraggi risorse, è necessario ricreare i monitoraggi sul nuovo agent. Per effettuare questa operazione, completa la seguente procedura:

1. Sulla LPAR originale, eseguire il membro BFGMNLI per esportare le definizioni per il monitoraggio risorse associato all'agent originale in file XML.
2. Copiare i file XML contenenti le definizioni del controllo risorse nella nuova LPAR.
3. Utilizzare il membro BFGMNCRS nella libreria SBFGCMDS sulla nuova LPAR per importare le definizioni del monitoraggio risorse memorizzate nei file XML. Ciò determina la creazione dei monitor sul nuovo agent.

- Spostare un agent creato eseguendo comandi in USS.

  Se l'agent è stato originariamente creato eseguendo comandi USS, è possibile utilizzare i comandi per ricreare l'agent su una nuova LPAR. Per effettuare questa operazione, completa la seguente procedura:

  1. Eseguire il comando fteSetupCoordination sulla nuova LPAR, per definire il gestore code di coordinamento che deve essere utilizzato dall'agente e creare la struttura di directory necessaria per memorizzare la configurazione IBM MQ Managed File Transfer .
  2. Eseguire il comando fteSetupCommands per definire il gestore code comandi che deve essere utilizzato dall'agente sulla nuova LPAR.
  3. Eseguire il comando fteCreateAgent per creare nuovamente l'agente e la sua configurazione.
  4. Verificare che le code di sistema utilizzate dall'agente esistano sul gestore code per tale agente.

  Se all'agent che si sta spostando sono associati dei monitoraggi risorse, è necessario ricreare i monitoraggi sul nuovo agent. Per effettuare questa operazione, completa la seguente procedura:

  1. Sulla LPAR originale, eseguire il comando fteListMonitors , specificando il parametro **-ox** , per esportare le definizioni per il monitoraggio risorse, associato all'agente originale, nei file XML.
  2. Copiare i file XML contenenti le definizioni del controllo risorse nella nuova LPAR.
  3. Eseguire il comando fteCreateMonitor sulla nuova LPAR, specificando il parametro **-ix** , per importare definizioni di monitoraggio risorse memorizzate nei file XML. Ciò determina la creazione dei monitor sul nuovo agent.

Utilizzo di Managed File Transfer for z/OS con l'utilità di avvio JZOS Java

È possibile applicare le istruzioni in questo argomento come metodo alternativo di utilizzo di Managed File Transfer nell'azienda, sul sistema IBM MQ for z/OS .

Panoramica

Managed File Transfer for z/OS (MFT) utilizza la procedura di installazione standard di z/OS . Un modo alternativo per eseguire i comandi MFT consiste nell'utilizzare JCL e JZOS Java Launcher.

Consultare JZOS Batch Launcher and Toolkit per ulteriori dettagli.

Se il JCL non riesce ad elaborare correttamente, consultare Problemi MFT comuni con JZOS.

JCL di esempio per IBM MQ 8.0 e versioni successive

Attenzione: Per IBM WebSphere MQ File Transfer Edition 7.0, i parametri iniziano con FTE_ anziché con BFG_.

```
//JOHNDOEA JOB 1,MSGCLASS=H
// JCLLIB ORDER=(SCEN.MFT.JCL)   (1)
// INCLUDE MEMBER=BFGJCL8       (2)
```

```
//     DD * (2A)
. ${BFG_PROD}/bin/fteBatch createAgent  (3)
export IBM_JAVA_OPTIONS="${BFG_JAVA_OPTIONS} ${BFG_LANG}"  (4)
export JZOS_MAIN_ARGS="${BFG_MAIN_ARGS}" (4)
//MAINARGS DD *
-agentName MYAGENT  (5)
-f
-agentQMgr MQPD
-p MQPD
/*
```

dove:

- (1) è l'ubicazione delle istruzioni JCL incluse
- (2) Includere il membro JCL specificato dall'ubicazione in 1)
- (2A) Si estende // STDENV - vedere di seguito
- (3) Questo è il comando da eseguire, senza il prefisso fte iniziale
- (4) Queste linee sono necessarie, impostano le informazioni per JZOS
- (5) I parametri del comando
- Il membro BFGJCL8 (è possibile selezionare il proprio nome) richiama JZOS. Questo membro dispone di STEPLIB e di altri JCL necessari per eseguire MFT.

Altro JCL da includere

È necessario includere JCL per le librerie IBM MQ for z/OS e, se si utilizza il programma di registrazione Db2 , le librerie Db2 .

Ad esempio:

```
//WMQFTE EXEC PGM=JVMLDM86,REGION=0M PARM='+T'  (1)
//STEPLIB  DD DSN=SYS1.SIEALNKE,DISP=SHR        (2)
//* MQ libraries
//   DD DSN=MQM.V800.SCSQAUTH,DISP=SHR MQ Bindings
//   DD DSN=MQM.V800.SCSQANLE,DISP=SHR MQ Bindings
//   DD DSN=MQM.V800.SCSQLOAD,DISP=SHR MQ Bindings

//* DB2 libraries
//   DD DISP=SHR,DSN=SYS2.DB2.V10.SDSNEXIT.DBCP
//   DD DISP=SHR,DSN=SYS2.DB2.V10.SDSNLOAD
//   DD DISP=SHR,DSN=SYS2.DB2.V10.SDSNLOD2
//SYSOUT  DD SYSOUT=H
//SYSPRINT DD SYSOUT=H
//STDOUT  DD SYSOUT=H
//STDERR  DD SYSOUT=H

//STDENV  DD DSN=SCEN.MFT.JCL(BFGZENV8),DISP=SHR  (3)
```

dove:

- (1) è il nome del programma JZOS. Cercare in SYS1.SIEALNKE la versione sul sistema. Aggiungere PARM = '+ T' per fornire ulteriori informazioni diagnostiche.
- (2) Questo è il dataset con il programma JZOS.
- (3) Questo è il nome del membro di uno script shell. Definisce i parametri necessari per MFT. Vedere “Script shell per definire MFT” a pagina 706.

  Può essere qualsiasi dataset e membro. Deve essere l'ultimo nel file perché il lavoro JCL lo estende. Consultare 2A in “JCL di esempio per IBM MQ 8.0 e versioni successive” a pagina 705.

Script shell per definire MFT

Nell'esempio “Altro JCL da includere” a pagina 706 , viene utilizzato il membro BFGZENV8 . Si basa sul profilo JZOS.

È possibile utilizzare lo stesso file di configurazione per MFT V8 e IBM WebSphere MQ File Transfer Edition 7.0, con alcune modifiche minori. Tenere presente che prima di MFT V8 i parametri iniziano con FTE. Consultare: “File di esempio” a pagina 707.

Devi sapere:

- L'ubicazione in cui è installato Java
- L'ubicazione delle librerie IBM MQ for z/OS Java
- L'ubicazione dei file MFT
- Un ID utente deve essere presente in un gruppo specifico per essere considerato come amministratore IBM MQ for z/OS . È necessario il nome di questo gruppo
- Se non si utilizza l'inglese per i messaggi, è necessario conoscere la lingua da specificare.

File di esempio

```
# This is a shell script that configures
# any environment variables for the Java JVM.
# Variables must be exported to be seen by the launcher.
# Use PARM='+T' and set -x to debug environment script problems
set -x
# . /etc/profile
#
# Java configuration (including MQ Java interface)
#
export _BPXK_AUTOCVT="ON"
export JAVA_HOME="/java/java71_bit64_sr3_fp30/J7.1_64/"
export PATH="/bin:${JAVA_HOME}/bin/classic/"
LIBPATH="/lib:/usr/lib:${JAVA_HOME}/bin"
LIBPATH="$LIBPATH:${JAVA_HOME}/bin/classic"
LIBPATH=$LIBPATH:"/mqm/V8R0M0/java/lib/"
export LIBPATH

export BFG_JAVA_HOME="${JAVA_HOME}"
export BFG_WTO="YES"
export BFG_GROUP_NAME=MQADM
export BFG_PROD="/HMF8800/"
export BFG_CONFIG="/u/johndoe/fteconfig"
# export BFG_LANG=" -Duser.language=de "
export BFG_LANG=" "

____________________
```

dove:

export _BPXK_AUTOCVT = "ON "
È richiesto per la conversione Unicode

export JAVA_HOME = "/java/java71_bit64/J7.1_64/"
Indica l'ubicazione della directory Java. Specificare il nome del percorso per Java. Questa directory contiene bin e altre directory.

export PATH= "/bin: ${JAVA_HOME}/bin/classic/"
Imposta l'istruzione del percorso per le istruzioni eseguibili Java

LIBPATH= "/lib:/usr/lib:${JAVA_HOME}/bin"
Imposta il percorso della libreria per le istruzioni eseguibili Java

LIBPATH=" $LIBPATH: ${JAVA_HOME}/bin/classic"
Aggiunge altre librerie Java all'istruzione LIBPATH.

LIBPATH=$LIBPATH:/mqm/V8R0M0/java/lib/"
Aggiunge le librerie IBM MQ for z/OS nel percorso della libreria. Specificare il nome delle librerie IBM MQ for z/OS in USS.

esporta LIBPATH
Rende LIBPATH disponibile per JZOS

esporta BFG_JAVE_HOME = "${JAVA_HOME}"
Imposta BFG_JAVA_HOME sul valore di JAVA_HOME specificato in precedenza

esporta BFG_WTO = "YES "
L'impostazione di BFG_WTO su YES fa sì che i messaggi vengano visualizzati nel joblog utilizzando WTO

esporta BFG_GROUP_NAME=MQADM
Gli ID utente, che sono membri del gruppo specificato, sono considerati amministratori IBM MQ for z/OS

esporta BFG = "/HMF8800/"
È il percorso in cui si trova il codice MFT

export BFG_DATA= "/u/johndoe/fteconfig"
Indica dove sono memorizzate le informazioni di configurazione MFT

 # export BFG_LANG = " -Duser.language= de"
È un'istruzione commentata per definire la lingua come tedesco

esporta BFG = ""
Specifica la lingua come predefinita, l'inglese.

Il contenuto del prodotto MFT in `/lib/messages/BFGNVMessages_*.properties` elenca le lingue disponibili. Il valore predefinito è lasciare vuoto, il che significa che viene utilizzato l'inglese.

Per V7 specificare:

```
export FTE_JAVA_HOME="${JAVA_HOME}"
export FTE_WTO="YES"
export FTE_GROUP_NAME=SCENU
export FTE_PROD=""/HMF7100/"
export FTE_CONFIG="/u/johndoe/fteconfig"
export BFG_LANG=" "
```

Si noti che il `/u/johndoe/fteconfig` è diverso da quello in BFG_DATA

Attività correlate

“Configurazione di Managed File Transfer for z/OS” a pagina 677
Managed File Transfer for z/OS richiede la personalizzazione per consentire al componente di funzionare correttamente.

pianificazione per Managed File Transfer

IBM i Configurazione di MFT su IBM i

Per iniziare a utilizzare Managed File Transfer dopo averlo installato, è necessario completare una configurazione per il gestore code di coordinamento e l'agent.

Informazioni su questa attività

Dopo l'installazione, è necessario eseguire gli script di configurazione forniti da Managed File Transfer per i nuovi gestori code di coordinamento e i nuovi agenti prima di poter utilizzare i gestori code di coordinamento e gli agent per trasferire i file. È quindi necessario avviare gli agent creati.

Procedura

1. Per tutti i nuovi gestori code di coordinamento: eseguire i comandi MQSC nel file *coordination_qmgr_name*.mqsc rispetto al gestore code di coordinamento. Se il gestore code di coordinamento non si trova sullo stesso computer dell'installazione, copiare il file di script MQSC sul computer su cui si trova il gestore code, quindi eseguire lo script.
   a) Da una riga comandi IBM i , avviare qshell utilizzando il seguente comando: `CALL QSHELL`
   b) Modificare la seguente directory: `/QIBM/UserData/mqm/mqft/config/` *coordination_qmgr_name*
   c) Immettere il seguente comando, sostituendo *coordination_qmgr_name* con il nome del proprio gestore code:

```
/QSYS.LIB/QMQM.LIB/RUNMQSC.PGM coordination_qmgr_name < coordination_qmgr_name.mqsc
```

È possibile invece configurare manualmente il gestore code di coordinamento. Per ulteriori informazioni, consultare “Configurazione del gestore code di coordinamento per MFT” a pagina 712.

2. Per tutti i nuovi agent: eseguire i comandi MQSC nel file *agent_name*_create.mqsc sul gestore code dell'agent.

   Se il gestore code dell'agent non si trova sullo stesso computer dell'agent, copiare il file di script MQSC sul computer in cui si trova il gestore code ed eseguire lo script.

   a) Da una riga comandi IBM i , avviare qshell utilizzando il seguente comando: CALL QSHELL

   b) Modificare la seguente directory: /QIBM/UserData/mqm/mqft/config/*agent_qmgr_name*/agents

   c) Immettere il seguente comando, sostituendo *agent_qmgr_name* con il nome del gestore code dell'agent e sostituendo *agent_name* con il nome dell'agent:

```
/QSYS.LIB/QMQM.LIB/RUNMQSC.PGM agent_qmgr_name < agent_name_create.mqsc
```

   È invece possibile configurare manualmente il gestore code agent. Per ulteriori informazioni, fare riferimento a “Configurazione dei gestori code dell'agent MFT” a pagina 712.

3. Se il sottosistema QMFT non è stato ancora avviato come parte dell'installazione, dalla riga comandi IBM i , avviare il sottosistema QMFT utilizzando il seguente comando: STRSBS SBSD(QMQMMFT/QMFT) o STRSBS QMQMMFT/QMFT

4. Avviare i nuovi agent utilizzando il comando **fteStartAgent** .

   a) Da una riga comandi IBM i , avviare qshell utilizzando il seguente comando: CALL QSHELL

   b) Modificare la seguente directory: /QIBM/ProdData/mqm/bin

   c) Immettere il seguente comando, sostituendo AGENT con il nome del proprio agente:

```
./fteStartAgent AGENT
```

Operazioni successive

Si consiglia di impostare le sandbox per limitare le aree del file system a cui un agent può accedere. Questa funzione è descritta in Utilizzo delle sandbox dell'agent MFT.

Concetti correlati

“Configurazione di MFT per il primo utilizzo” a pagina 709
È necessario eseguire alcune attività di configurazione per gli agent Managed File Transfer e i gestori code una volta, la prima volta che si desidera utilizzarli.

Configurazione di MFT per il primo utilizzo

È necessario eseguire alcune attività di configurazione per gli agent Managed File Transfer e i gestori code una volta, la prima volta che si desidera utilizzarli.

Connessione a IBM MQ

Tutte le comunicazioni di rete con i gestori code IBM MQ , incluse le comunicazioni correlate a Managed File Transfer, riguardano i canali IBM MQ . Un canale IBM MQ rappresenta un'estremità di un collegamento di rete. I canali sono classificati come canali di messaggi o canali MQI.

Managed File Transfer e canali

Managed File Transfer utilizza canali MQI per connettere gli agent in modalità client ai relativi gestori code agent e per connettere le applicazioni di comando (ad esempio, **fteCreateTransfer**) ai relativi gestori code di comando e coordinamento. Nella configurazione predefinita, queste connessioni

vengono effettuate utilizzando un canale SVRCONN denominato SYSTEM.DEF.SVRCONN, che esiste per impostazione predefinita su tutti i gestori code. A causa di questi valori predefiniti, non è necessario modificare i canali MQI per un'installazione di Managed File Transfer di base.

Esistono sei tipi di endpoint del canale di messaggi, ma questo argomento riguarda solo le coppie mittente - destinatario. Consultare Componenti di accodamento distribuiti per informazioni su altre combinazioni di canali.

Percorsi dei messaggi richiesti

I messaggi IBM MQ possono viaggiare solo su canali di messaggi, quindi è necessario assicurarsi che i canali siano disponibili per tutti i percorsi di messaggi richiesti da Managed File Transfer. Questi percorsi non devono essere diretti; i messaggi possono viaggiare attraverso i gestori code intermedi, se necessario. Questo argomento riguarda solo la comunicazione diretta punto a punto. Per ulteriori informazioni su queste opzioni, consultare Come accedere al gestore code remoto .

I percorsi di comunicazione utilizzati da Managed File Transfer sono i seguenti:

Da agent a agent
I due agent tra cui vengono trasferiti i file richiedono la comunicazione bidirezionale tra i gestori code associati. Poiché questo percorso trasporta i dati di massa, considerare di rendere il percorso il più breve, veloce o economico possibile in base alle proprie necessità.

Da agente a coordinamento
I messaggi di log dagli agenti che partecipano a un trasferimento devono essere in grado di raggiungere il gestore code di coordinamento.

Comando per l'agente
Qualsiasi gestore code a cui si collegano le applicazioni di comandi o IBM MQ Explorer (utilizzando il gestore code comandi) deve essere in grado di inviare messaggi ai gestori code degli agent che tali applicazioni di comandi vengono utilizzate per il controllo. Per consentire ai messaggi di feedback di essere visualizzati dai comandi, utilizzare una connessione bidirezionale.

Per ulteriori informazioni, consultare *Verifica di un'installazione di IBM MQ* per la piattaforma o le piattaforme utilizzate dall'azienda.

Concetti correlati

“Configurazione di un gestore code a più istanze per utilizzare MFT” a pagina 716
IBM WebSphere MQ 7.0.1 in poi supporta la creazione di gestori code a più istanze. Un gestore code a più istanze si riavvia automaticamente su un server standby. Managed File Transfer supporta la connessione ai gestori code dell'agent a più istanze, a un gestore code di coordinamento a più istanza e a un gestore code di comando a più istanze.

Attività correlate

“Configurazione dei gestori code di rete MFT” a pagina 710
Se la propria rete Managed File Transfer include più di un gestore code IBM MQ , tali gestori code IBM MQ devono essere in grado di comunicare in remoto tra loro.

“Configurazione del gestore code di coordinamento per MFT” a pagina 712
Dopo aver eseguito il comando **fteSetupCoordination** , eseguire lo script *coordination_qmgr_name*.mqsc nella directory *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* per eseguire la configurazione necessaria per il gestore code di coordinamento. Tuttavia, se si desidera eseguire questa configurazione manualmente, completare la seguente procedura sul gestore code di coordinamento.

Configurazione dei gestori code di rete MFT

Se la propria rete Managed File Transfer include più di un gestore code IBM MQ , tali gestori code IBM MQ devono essere in grado di comunicare in remoto tra loro.

Informazioni su questa attività

Esistono due modi per configurare i gestori code in modo che siano in grado di comunicare tra loro:

- Impostando un cluster di gestori code IBM MQ .

  Per informazioni sui cluster di gestori code IBM MQ e su come configurarli, consultare “Configurazione di un cluster di gestore code” a pagina 275.
- Impostando i canali tra i gestori code, descritto di seguito:

Impostazione dei canali tra i gestori code

Configurare i seguenti canali di messaggi tra gestori code:

- Dal gestore code dell'agente al gestore code di coordinazione
- Dal gestore code comandi al gestore code agent.
- Dal gestore code dell'agente al gestore code comandi (per consentire la visualizzazione dei messaggi di feedback da parte dei comandi).
- Dal gestore code comandi al gestore code di coordinamento
- Dal gestore code dell'agent a qualsiasi altro gestore code dell'agent nella rete Managed File Transfer

Se sono necessarie ulteriori informazioni su come impostare questa comunicazione, iniziare con queste informazioni: Amministrazione di oggetti IBM MQ remoti mediante MQSC.

Alcuni passi di esempio consigliati sono:

Procedura

1. Creare una coda di trasmissione sul gestore code IBM MQ con lo stesso nome del gestore code di coordinamento.

   È possibile utilizzare il seguente comando MQSC:

   ```
   DEFINE QLOCAL(coordination-qmgr-name) USAGE(XMITQ)
   ```
2. Sul gestore code IBM MQ , creare un canale mittente per il gestore code di coordinamento Managed File Transfer . Il nome della coda di trasmissione creata nel passo precedente è un parametro obbligatorio per questo canale. Se è richiesta la comunicazione con Managed File Transfer per gli agenti IBM WebSphere MQ 7.5 o Managed File Transfer , assicurarsi che il parametro CONVERT del canale mittente sia impostato su no. (Le versioni precedenti di IBM WebSphere MQ File Transfer Edition pubblicavano sempre i messaggi in formato UTF-8 , il che significa che qualsiasi conversione di dati danneggia il messaggio. Ciò non è necessario per gli agenti su Managed File Transfer per IBM MQ 8.0 o versioni successive, poiché i messaggi vengono pubblicati con un formato vuoto.)

   È possibile utilizzare il seguente comando MQSC:

   ```
   DEFINE CHANNEL(channel-name) CHLTYPE(SDR) CONNAME('coordination-qmgr-host(coordination-qmgr-port)')
    XMITQ(coordination-qmgr-name) CONVERT(NO)
   ```

   Nota: Impostare CONVERT (NO), solo se richiesto.
3. Sul gestore code di coordinamento Managed File Transfer , creare un canale ricevente per il gestore code IBM MQ . Assegnare a questo canale ricevente lo stesso nome del canale mittente sul gestore code IBM MQ .

   È possibile utilizzare il seguente comando MQSC:

   ```
   DEFINE CHANNEL(channel-name) CHLTYPE(RCVR)
   ```

Operazioni successive

Successivamente, attenersi alla procedura di configurazione per il gestore code di coordinamento: “Configurazione del gestore code di coordinamento per MFT” a pagina 712.

Configurazione del gestore code di coordinamento per MFT

Dopo aver eseguito il comando **fteSetupCoordination** , eseguire lo script *coordination_qmgr_name*.mqsc nella directory *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* per eseguire la configurazione necessaria per il gestore code di coordinamento. Tuttavia, se si desidera eseguire questa configurazione manualmente, completare la seguente procedura sul gestore code di coordinamento.

Informazioni su questa attività

Procedura

1. Creare una coda locale denominata SYSTEM.FTE.
2. Aggiungere SYSTEM.FTE nella coda SYSTEM.QPUBSUB.QUEUE.NAMELIST .
3. Creare un argomento denominato SYSTEM.FTE con una stringa di argomenti SYSTEM.FTE.
4. Verificare gli attributi Consegna messaggi non persistenti (NPMSGDLV) e Consegna messaggi persistenti (PMSGDLV) di SYSTEM.FTE FTE è impostato su ALLAVAIL.
5. Verificare che l'attributo della modalità di pubblicazione / sottoscrizione (PSMODE) del gestore code di coordinamento sia impostato su ENABLED.

Operazioni successive

Se si esegue il comando `strmqm -c` su un gestore code configurato come gestore code di coordinamento, il comando elimina la modifica apportata al passo 2 (aggiungendo il SISTEMA SYSTEM.FTE nella coda SYSTEM.QPUBSUB.QUEUE.NAMELIST elenco nomi). Ciò è dovuto al fatto che `strmqm -c` ricrea gli oggetti IBM MQ predefiniti e inverte le Managed File Transfer modifiche. Pertanto, se il gestore code è stato avviato con `strmqm -c`, completare una delle seguenti operazioni:

- Eseguire nuovamente lo script *coordination_qmgr_name*.mqsc sul gestore code.
- Ripetere il passo 2.

Concetti correlati

“Connessione a IBM MQ” a pagina 709
Tutte le comunicazioni di rete con i gestori code IBM MQ , incluse le comunicazioni correlate a Managed File Transfer, riguardano i canali IBM MQ . Un canale IBM MQ rappresenta un'estremità di un collegamento di rete. I canali sono classificati come canali di messaggi o canali MQI.

“Configurazione di un gestore code a più istanze per utilizzare MFT” a pagina 716
IBM WebSphere MQ 7.0.1 in poi supporta la creazione di gestori code a più istanze. Un gestore code a più istanze si riavvia automaticamente su un server standby. Managed File Transfer supporta la connessione ai gestori code dell'agent a più istanze, a un gestore code di coordinamento a più istanza e a un gestore code di comando a più istanze.

Attività correlate

“Configurazione dei gestori code di rete MFT” a pagina 710
Se la propria rete Managed File Transfer include più di un gestore code IBM MQ , tali gestori code IBM MQ devono essere in grado di comunicare in remoto tra loro.

Riferimenti correlati

Coordinamento fteSetup

Configurazione dei gestori code dell'agent MFT

In seguito all'installazione, eseguire lo script *agent_name*_create.mqsc nella directory *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name*/agents/*agent_name* per eseguire la configurazione necessaria per il gestore code dell'agent. Tuttavia, se si desidera eseguire questa configurazione manualmente, completare la seguente procedura sul gestore code dell'agent.

Procedura

1. Creare le code di operazione dell'agent.
   Queste code sono denominate:
   - SYSTEM.FTE.COMMAND.*nome_agent*
   - SYSTEM.FTE.DATA.*nome_agent*
   - SYSTEM.FTE.EVENT.*nome_agent*
   - SYSTEM.FTE.REPLY.*nome_agent*
   - SYSTEM.FTE.STATE.*nome_agent*

   Per informazioni sui parametri della coda, vedere MFT Impostazioni della coda agent.
2. Creare le code di autorizzazioni agent.
   Queste code sono denominate:
   - SYSTEM.FTE.AUTHADM1.*nome_agent*
   - SYSTEM.FTE.AUTHAGT1.*nome_agent*
   - SYSTEM.FTE.AUTHMON1.*nome_agent*
   - SYSTEM.FTE.AUTHOPS1.*nome_agent*
   - SYSTEM.FTE.AUTHSCH1.*nome_agent*
   - SYSTEM.FTE.AUTHTRN1.*nome_agent*

   Per informazioni sui parametri della coda, vedere MFT Impostazioni della coda agent.

Operazioni successive

Per informazioni sulla creazione e la configurazione di un agent bridge di protocollo, consultare fteCreateBridgeAgent (creare e configurare un agent bridge di protocollo MFT) e Configurazione di un bridge di protocollo per un server FTPS.

Creazione di una IBM MQ File Transfer Structure

È possibile configurare una struttura Managed File Transfer , basata su un singolo agent connesso a un gestore code sulla stessa macchina.

Informazioni su questa attività

La configurazione di MFT viene memorizzata in una struttura file in IBM MQ DataPath, sulla macchina su cui si trova l'agent.

La seguente configurazione di esempio è per un gestore code MFT su IBM MQ 8.0 denominato SAMPLECOORD (con la sicurezza disabilitata) e un singolo agent MFT denominato SAMPLEAGENT:

```
+--- config
             +--- SAMPLECOORD
                            +--- command.properties
                            +--- coordination.properties
                            +--- SAMPLECOORD.mqsc
                            +--- agents
                                          +--- SAMPLEAGENT
                                                        +--- agent.properties
                                                        +--- SAMPLEAGENT_create.mqsc
                                                        +--- SAMPLEAGENT_delete.mqsc

+---logs
             +--- SAMPLECOORD
                            +--- agents
                                          +--- SAMPLEAGENT
                                                        +--- logs
```

Questo esempio presuppone che la sicurezza del gestore code sia stata disabilitata. I seguenti comandi, eseguiti in **runmqsc**, disabiliteranno la sicurezza dopo il riavvio del gestore code:

```
runmqsc queue manager
 alter qmgr CONNAUTH(NONE);
 alter qmgr CHLAUTH(DISABLED);
 end;
```

Per la configurazione con la sicurezza abilitata in MFT per IBM MQ 8.0 o versioni successive, **CONNAUTH** richiede tutti i comandi MFT che si connettono a un gestore code per fornire le credenziali ID utente e password. È possibile applicare i parametri aggiuntivi **-mquserid** e **-mqpassword** per ogni comando oppure definire un file MQMFTCredentials.xml . Il seguente file di credenziali di esempio definisce l'ID utente di fteuser, per cui la password di MyPassword deve essere utilizzata durante la connessione al gestore code SAMPLECOORD:

```
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MQMFTCredentials"
        xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://wmqfte.ibm.com/MQMFTCredentials MQMFTCredentials.xsd">
    <tns:qmgr mqPassword="MyPassword" MyUserId="fteuser" name="SAMPELCOORD"/>
</tns:mqmftCredentials>
```

Per ulteriori informazioni, vedi Autenticazione della connessioneMFT e IBM MQ.

Note:

- Per individuare la propria directory di configurazione MFT , utilizzare il comando **fteDisplayVersion -v** .
- Per gli utenti z/OS , il file MQMFTCredential.xml può essere individuato come membro in un dataset partizionato con formato record variabile (RECFM = V) o formato record non definito (RECFM = U).
- Per la configurazione con la sicurezza abilitata, aggiungere il seguente parametro ai seguenti passi per associare le credenziali con il gestore code pertinente: -credentialsFile *full credential file path*.
- La password in testo chiaro in MQMFTCredential.xml può essere offuscata utilizzando il seguente comando:

  ```
  fteObfuscate -credentialsFile full file path to MQMFTCredentials.xml
  ```

Procedura

1. Creare un gestore code di coordinamento.

   Un gestore code di coordinamento è un singolo gestore code, utilizzato per ricevere tutte i log di trasferimento e le informazioni sullo stato dagli agent. Esegui il seguente comando:

   ```
   fteSetupCoordination -coordinationQMgr coordination_qmgr_name
   ```

   Questo crea la configurazione di base di livello superiore e crea un IBM MQ file script da richiamare *coordination_qmgr_name*.mqsc.

   La configurazione deve quindi essere caricata nel gestore code, eseguendo il seguente comando IBM MQ :

   ```
   runmqsc queue manager name < coordination_qmgr_name.mqsc
   ```

   Nota: Per la connessione del client TCP a un gestore code, è possibile utilizzare:

   ```
   fteSetupCoordination -coordinationQMgr coordination_qmgr_name
   -coordinationQMgrHost coordination_qmgr_host -coordinationQMgrPort coordination_qmgr_port
   -coordinationQMgrChannel coordination_qmgr_channel
   ```

Per *coordination_qmgr_name*.mqsccreato, sarà necessario eseguire il comando **runmqsc** sulla stessa macchina su cui è in esecuzione il gestore code di coordinamento.

2. Creare il gestore code comandi.

   Un gestore code comandi è un singolo gestore code che è stato preconfigurato in modo che l'infrastruttura IBM MQ possa instradare le richieste MFT all'agent pertinente. Esegui il seguente comando:

   ```
   fteSetupCommands -connectionQMgr Command QM Name -p Coordination QM Name
   ```

   Questo crea un file command.properties nella directory di coordinazione. Si noti che il -p è facoltativo e non è richiesto se i comandi vengono impostati per il coordinamento predefinito.

   Nota: Per la connessione del client TCP a un gestore code, è possibile utilizzare:

   ```
   fteSetupCommands -p coordination_qmgr_name -commandQMgr connection_qmgr_name
   -commandQMgrHost connection_qmgr_host -commandQMgrPort connection_qmgr_port
   -commandQMgrChannel connection_qmgr_channel
   ```

3. Creare l'agent.

   Un agent è un'applicazione che può inviare e ricevere file. Esegui il seguente comando:

   ```
   fteCreateAgent -p coordination_qmgr_name -agentName agent_name -agentQMgr agent_qmgr_name
   ```

   Ciò crea la configurazione dell'agent sotto il coordinamento e crea un file script IBM MQ per richiamare *agent_name*.mqsc nella directory di configurazione dell'agent.

   Eseguire questo comando IBM MQ per caricare il file script IBM MQ nel gestore code:

   ```
   runmqsc agent_qmgr_name < agent_name_create.mqsc file
   ```

   Nota: Per la connessione del client TCP a un gestore code, è possibile utilizzare:

   ```
   fteCreateAgent -p coordination_qmgr_name -agentName agent_name -agentQMgr agent_qmgr_name
   -agentQMgrHost agent_qmgr_host -agentQMgrPort agent_qmgr_port -agentQMgrChannel
   agent_qmgr_channel
   ```

4. Avviare l'agent.

   Esegui il seguente comando:

   ```
   fteStartAgent -p coordination_qmgr_name agentName
   ```

   L'agent viene avviato in background e viene restituito il prompt dei comandi. Per verificare che l'agente sia in esecuzione, eseguire il seguente comando:

   ```
   fteListAgents -p coordination_qmgr_name
   ```

   Mostra lo stato degli agent. Se l'esecuzione dell'agent ha esito positivo, viene riportato come nello stato READY.

Risultati

Un'infrastruttura MFT di base è pronta per l'uso e ora puoi utilizzare il comando **fteCreateTransfer** per richiedere un trasferimento. In alternativa, se IBM MQ Explorer è disponibile, utilizzare i plug-in MFT per creare e monitorare i trasferimenti.

È possibile aggiungere ulteriori agenti alla configurazione ripetendo il passo 3: Creare l'agente. Se viene utilizzata la connessione client TCP, queste possono trovarsi su macchine differenti. Per macchine

differenti, i comandi **fteSetupCoordination** e **fteSetupCommands** devono essere ripetuti per ciascuna macchina, tuttavia non è necessario eseguire gli script mqsc.

Configurazioni più complesse possono avere gestori code separati per il coordinamento e ciascun agent. In questi casi, i vari gestori code dovranno essere connessi tra loro.

Attività correlate

Operazioni da eseguire se l'agent MFT non è elencato dal comando **fteListAgents**

Riferimenti correlati

Coordinamento fteSetup

Comandi fteSetup: creare il file MFT command.properties

Agent fteCreate

fteObfuscate: crittografare i dati sensibili

Formato file credenziali MFT

Il file MFT`agent.properties`

Configurazione di un gestore code a più istanze per utilizzare MFT

IBM WebSphere MQ 7.0.1 in poi supporta la creazione di gestori code a più istanze. Un gestore code a più istanze si riavvia automaticamente su un server standby. Managed File Transfer supporta la connessione ai gestori code dell'agent a più istanze, a un gestore code di coordinamento a più istanza e a un gestore code di comando a più istanze.

Configurazione di un gestore code a più istanze

Importante: Per informazioni sulla configurazione di un gestore code a più istanze IBM MQ , consultare “Gestori code a più istanze” a pagina 475. Accertarsi di aver letto queste informazioni prima di provare a configurare un gestore code a più istanze per l'utilizzo con Managed File Transfer.

Utilizzo di un gestore code a più istanze come gestore code agent

Per consentire a un agente di connettersi sia all'istanza attiva che a quella in standby del gestore code a più istanze, aggiungere la proprietà `agentQMgrStandby` al file `agent.properties` dell'agente. La proprietà `agentQMgrStandby` definisce il nome host e il numero di porta utilizzati per connessioni client per l'istanza del gestore code in standby. Il valore della proprietà deve essere fornito nel formato CONNAME di MQ , ossia *host_name*(*port_number*).

La proprietà `agentQMgr` specifica il nome del gestore code a più istanze. La proprietà `agentQMgrHost` specifica il nome host per l'istanza del gestore code attivo e la proprietà `agentQMgrPort` specifica il numero di porta per l'istanza del gestore code attivo. L'agent deve connettersi in modalità client sia all'istanza attiva che all'istanza standby del gestore code a più istanze.

Per ulteriori informazioni, consultare Il file MFT `agent.properties` .

Questo esempio mostra il contenuto del file `agent.properties` per AGENT1 che si connette a un gestore code a più istanze denominato QM_JUPITER. L'istanza attiva di QM_JUPITER si trova nel sistema host1 e utilizza il numero di porta 1414 per connessioni client. L'istanza standby di QM_JUPITER si trova sul sistema host2 e utilizza il numero porta 1414 per le connessioni client.

```
agentName=AGENT1
agentDesc=
agentQMgr=QM_JUPITER
agentQMgrPort=1414
agentQMgrHost=host1
agentQMgrChannel=SYSTEM.DEF.SVRCONN
agentQMgrStandby=host2(1414)
```

Utilizzo di un gestore code a più istanze come gestore code di coordinamento

Per abilitare le connessioni sia all'istanza attiva che a quella in standby del gestore code di coordinamento a più istanze, aggiungere la proprietà `coordinationQMgrStandby` a tutti i `coordination.properties` file nella topologia Managed File Transfer .

Per ulteriori informazioni, consultare Il file MFT coordination.properties .

Questo esempio mostra il contenuto di un file `coordination.properties` che specifica i dettagli di connessione a un gestore code di coordinamento a più istanze denominato QM_SATURN. L'istanza attiva di QM_SATURN è sul sistema coordination_host1 e utilizza il numero di porta 1420 per le connessioni client. L'istanza in standby di QM_SATURN si trova sul sistema coordination_host2 e utilizza il numero di porta 1420 per connessioni client.

```
coordinationQMgr=QM_SATURN
coordinationQMgrHost=coordination_host1
coordinationQMgrPort=1420
coordinationQMgrChannel=SYSTEM.DEF.SVRCONN
coordinationQMgrStandby=coordination_host2(1420)
```

Il programma di registrazione autonomo Managed File Transfer deve sempre connettersi al proprio gestore code in modalità bind. Quando si utilizza il programma di registrazione autonomo con un gestore code di coordinamento a più istanze, connettere il programma di registrazione autonomo, in modalità bind, a un gestore code differente. I passi per eseguire questa operazione sono descritti in “Configurazioni alternative per un logger autonomo MFT” a pagina 731. È necessario definire i canali tra il gestore code del programma di registrazione autonomo e il gestore code di coordinamento con il nome host e il numero di porta di entrambe le istanze del gestore code di coordinamento a più istanze. Per informazioni su come svolgere questa procedura, consultare “Gestori code a più istanze” a pagina 475.

Il plug-in Managed File Transfer per IBM MQ Explorer si connette al gestore code di coordinamento in modalità client. Se l'istanza attiva del gestore code di coordinamento a più istanze ha esito negativo, l'istanza in standby del gestore code di coordinamento diventa attiva e il plugin si riconnette.

I Managed File Transfer comandi **`fteList*`** e **`fteShowAgentDetails`** si connettono direttamente al gestore code di coordinamento. Se l'istanza attiva del coordinamento a più istanze non è disponibile, questi comandi tenteranno di connettersi all'istanza in standby del gestore code di coordinamento.

Utilizzo di un gestore code a più istanze come gestore code comandi

Per abilitare le connessioni sia all'istanza attiva che a quella in standby del gestore code comandi a più istanze, aggiungere la proprietà `connectionQMgrStandby` a tutti i file `command.properties` nella topologia Managed File Transfer .

Per ulteriori informazioni, consultare Il file MFT command.properties .

Questo esempio mostra i contenuti di un file `command.properties` che specifica i dettagli di connessione a un gestore code di comandi a più istanze denominato QM_MARS. L'istanza attiva di QM_MARS si trova sul sistema command_host1 e utilizza il numero di porta 1424 per le connessioni client. L'istanza di standby di QM_MARS si trova sul sistema command_host2 e utilizza il numero porta 1424 per le connessioni client.

```
connectionQMgr=QM_SATURN
connectionQMgrHost=command_host1
connectionQMgrPort=1424
connectionQMgrChannel=SYSTEM.DEF.SVRCONN
connectionQMgrStandby=command_host2(1424)
```

Concetti correlati

“Connessione a IBM MQ” a pagina 709
Tutte le comunicazioni di rete con i gestori code IBM MQ , incluse le comunicazioni correlate a Managed File Transfer, riguardano i canali IBM MQ . Un canale IBM MQ rappresenta un'estremità di un collegamento di rete. I canali sono classificati come canali di messaggi o canali MQI.

Attività correlate

“Configurazione dei gestori code di rete MFT” a pagina 710
Se la propria rete Managed File Transfer include più di un gestore code IBM MQ , tali gestori code IBM MQ devono essere in grado di comunicare in remoto tra loro.

“Configurazione del gestore code di coordinamento per MFT” a pagina 712
Dopo aver eseguito il comando **fteSetupCoordination** , eseguire lo script *coordination_qmgr_name*.mqsc nella directory *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* per eseguire la configurazione necessaria per il gestore code di coordinamento. Tuttavia, se si desidera eseguire questa configurazione manualmente, completare la seguente procedura sul gestore code di coordinamento.

Conservazione dei messaggi di log MFT

Managed File Transfer invia l'avanzamento del trasferimento file e le informazioni di log al gestore code di coordinamento. Il gestore code di coordinamento pubblica queste informazioni in tutte le sottoscrizioni corrispondenti al SISTEMA SYSTEM.FTE . Se non ci sono sottoscrizioni, queste informazioni non vengono conservate.

Modalità per garantire la conservazione delle informazioni

Se l'avanzamento del trasferimento o le informazioni di log sono importanti per la propria azienda, è necessario effettuare una delle seguenti operazioni per garantire che le informazioni vengano conservate:

- Utilizzare il programma di registrazione database Managed File Transfer per copiare i messaggi pubblicati nel SYSTEM.FTE/Log in un database Oracle o Db2 .
- Definire una sottoscrizione al SISTEMA SYSTEM.FTE , che memorizza le pubblicazioni su una coda IBM MQ . Definire questa sottoscrizione prima di trasferire qualsiasi trasferimento file per garantire che tutti i messaggi di avanzamento e di log vengano conservati nella coda.
- Scrivere un'applicazione che utilizza l'interfaccia MQI (Message Queue Interface) o IBM MQ JMS per creare una sottoscrizione durevole ed elaborare le pubblicazioni consegnate alla sottoscrizione. Questa applicazione deve essere in funzione prima che i file vengano trasferiti per garantire che l'applicazione riceva tutti i messaggi di avanzamento e di log.

Ciascuno di questi approcci è descritto più dettagliatamente nelle seguenti sezioni.

Non basarsi sul plugin IBM MQ Explorer per conservare le informazioni di log.

Utilizzo del programma di registrazione database Managed File Transfer per conservare i messaggi di registrazione

Il programma di registrazione database è un componente facoltativo di Managed File Transfer che è possibile utilizzare per copiare le informazioni di log in un database per scopi di analisi e controllo. Il programma di registrazione database è un'applicazione Java autonoma che viene installata su un sistema che ospita il gestore code di coordinamento e il database. Per ulteriori informazioni sul programma di registrazione database, consultare “Configurazione di un programma di registrazione MFT” a pagina 719.

Conservazione dell'avanzamento e dei messaggi di log utilizzando il plugin IBM MQ Explorer

Quando un'istanza del plug-in di IBM MQ Explorer viene avviata per la prima volta, l'istanza crea una sottoscrizione durevole sul gestore code di coordinamento. Questa sottoscrizione durevole è utilizzata per raccogliere le informazioni visualizzate nelle viste **Log trasferimenti** e **Avanzamento trasferimento corrente** .

Al nome della sottoscrizione durevole viene aggiunto un prefisso per mostrare che la sottoscrizione era stata creata dal plug-in IBM MQ Explorer MFT, il nome host e il nome dell'utente, ad esempio `MQExplorer_MFT_Plugin_HOST_TJWatson`.

Questo prefisso viene aggiunto nel caso in cui un amministratore desideri eliminare una sottoscrizione duratura che non è più in uso attivo da parte di un'istanza del plugin IBM MQ Explorer .

L'uso di una sottoscrizione durevole sul gestore code di coordinamento può causare la creazione di messaggi sul SISTEMA SYSTEM.MANAGED.DURABLE code. Se si dispone di una rete Managed File Transfer di volumi elevati, utilizzare il plug-in IBM MQ Explorer raramente o entrambi, questi dati del messaggio possono riempire il filesystem locale.

Per evitare che ciò accada, è possibile specificare che il plug-in IBM MQ Explorer utilizzi una sottoscrizione non durevole al gestore code di coordinamento. Eseguire questa procedura in IBM MQ Explorer:

1. Selezionare **Finestra** > **Preferenze** > **MQ Explorer** > **Managed File Transfer**
2. Dall'elenco **Tipo di sottoscrizione log trasferimenti**, scegliere NON_DURABLE.

Memorizzazione delle pubblicazioni su una coda IBM MQ

Per archiviare i messaggi di log o di avanzamento su una coda IBM MQ , configurare una sottoscrizione sul gestore code di coordinamento che inoltra i messaggi a questa coda. Ad esempio, per inoltrare tutti i messaggi di log a una coda denominata LOG.QUEUE, inoltrare il seguente comando MQSC:

```
define sub(MY.SUB) TOPICSTR('Log/#') TOPICOBJ(SYSTEM.FTE) DEST(LOG.QUEUE)WSCHEMA(TOPIC)
```

Dopo che i messaggi di log sono stati inoltrati a una coda IBM MQ , vengono conservati nella coda fino a quando non vengono elaborati da un'applicazione IBM MQ che utilizza la coda.

Scrittura di applicazioni che gestiscono una sottoscrizione duratura al SISTEMA SYSTEM.FTE FTE

È possibile scrivere le applicazioni che gestiscono le proprie sottoscrizioni durevoli in SYSTEM.FTE utilizzando una delle API (application programming interface) supportate da IBM MQ. Queste applicazioni possono ricevere messaggi di log o coda IBM MQ e agire su di essi in modo appropriato per le proprie esigenze aziendali.

Per ulteriori informazioni sulle API (application programming interface) disponibili, consultare Sviluppo di applicazioni.

Configurazione di un programma di registrazione MFT

Quando Managed File Transfer trasferisce i file, pubblica le informazioni sulle sue azioni in un argomento sul gestore code di coordinamento. Il programma di registrazione database è un componente facoltativo di Managed File Transfer che è possibile utilizzare per copiare queste informazioni in un database per scopi di analisi e controllo.

Esistono tre versioni del logger:

- ULW logger di file autonomo
- programma di registrazione database autonomo
- logger Java Platform, Enterprise Edition (Java EE)

Logger su IBM i

IBM i

I logger Managed File Transfer non sono supportati sulla piattaforma IBM i .

Programma di registrazione file autonomo

ULW

Il programma di registrazione file autonomo è un processo Java che viene eseguito sul sistema su cui è presente il gestore code di coordinamento o su un sistema su cui è presente un gestore code con connettività al gestore code di coordinamento. Il programma di registrazione file autonomo utilizza i bind IBM MQ per connettersi al gestore code associato. Il programma di registrazione autonomo viene creato utilizzando il comando **fteCreateLogger** .

Windows È possibile eseguire il programma di registrazione file autonomo come servizio Windows per garantire che il programma di registrazione file continui l'esecuzione quando si scollega dalla sessione Windows e può essere configurato per essere avviato automaticamente al riavvio di un sistema. Per ulteriori informazioni, consultare “Installazione del programma di registrazione file autonomo MFT” a pagina 720.

Il programma di registrazione file autonomo non è supportato sulle piattaforme riportate di seguito:

- z/OS z/OS
- IBM i IBM i

Programma di registrazione database autonomo

Il programma di registrazione database autonomo è un'applicazione Java che viene installata su un sistema che contiene un gestore code e un database. Il programma di registrazione database autonomo è spesso installato sullo stesso sistema del gestore code di coordinamento, tuttavia può essere installato anche sullo stesso sistema di qualsiasi gestore code che abbia la connettività al gestore code di coordinamento. Il programma di registrazione database autonomo utilizza i bind IBM MQ per collegarsi al gestore code associato e un driver JDBC di tipo 2 o 4 per connettersi a un database Db2 o Oracle . Questi tipi di connessione sono richiesti perché il programma di registrazione database autonomo utilizza il supporto XA del gestore code per coordinare una transazione globale sia sul gestore code che sul database, proteggendo i dati.

Windows Se si utilizza un sistema Windows , è possibile eseguire i logger autonomi come servizi Windows per garantire che i logger continuino l'esecuzione quando ci si scollega dalla sessione Windows . Per ulteriori informazioni, consultare “Installazione del programma di registrazione database autonomo MFT” a pagina 728 per un programma di registrazione database autonomo.

Programma di registrazione database Java EE

Il programma di registrazione del database Java EE viene fornito come file EAR, che viene installato in un server delle applicazioni. Ciò può essere più conveniente rispetto all'utilizzo del programma di registrazione database autonomo se si dispone di un ambiente del server delle applicazioni Java EE esistente, poiché il programma di registrazione database Java EE può essere gestito insieme alle altre applicazioni enterprise. È anche possibile installare il programma di registrazione database Java EE su un sistema separato sui sistemi che ospitano il server IBM MQ e il database. Il programma di registrazione database Java EE viene supportato per l'utilizzo con i database Db2 e Oracle . Il programma di registrazione database Java EE supporta anche Oracle Real Application Clusters quando installato su WebSphere Application Server 7.0.

Per istruzioni su come configurare un programma di registrazione, consultare i seguenti argomenti:

- “Installazione del programma di registrazione file autonomo MFT” a pagina 720
- “Installazione del programma di registrazione database autonomo MFT” a pagina 728
- “Installazione del programma di registrazione database Java EE per MFT” a pagina 732

ULW Installazione del programma di registrazione file autonomo MFT

Il programma di registrazione file autonomo è un processo Java che deve connettersi a un gestore code di coordinamento utilizzando i collegamenti IBM MQ . Per definire un programma di registrazione file autonomo, utilizzare il comando **fteCreateLogger** e seguire i passi riportati in questo argomento.

Informazioni su questa attività

Per ulteriori informazioni sul programma di registrazione file autonomo, consultare “Configurazione di un programma di registrazione MFT” a pagina 719. I passaggi in questo argomento configurano un programma di registrazione per la connessione a un gestore code di coordinazione. Per configurazioni di logger alternative, consultare “Configurazioni alternative per un logger autonomo MFT” a pagina 731

Il programma di registrazione file autonomo non è supportato sulle piattaforme riportate di seguito:

- z/OS z/OS
- IBM i IBM i

Procedura

1. Assicurarsi di avere installato il componente Managed File Transfer Logger . Per ulteriori informazioni, consultare Opzioni del prodotto Managed File Transfer
2. Eseguire il comando **fteCreateLogger** specificando il gestore code di coordinamento e impostando il parametro -loggerType su `FILE` per creare il programma di registrazione file autonomo. Per ulteriori informazioni, vedi fteCreateLogger.
3. Opzionale: Se si desidera utilizzare un formato personalizzato, è possibile modificare il file XML creato dal comando **fteCreateLogger** . La definizione del formato di log si trova nel file `FileLoggerFormat.xml` . Per ulteriori informazioni, consultare “Formato del programma di registrazione file autonomo MFT” a pagina 722.
4. Eseguire i comandi MQSC, forniti dal comando **fteCreateLogger** , sul gestore code di coordinamento per creare le code del programma di registrazione.
5. Identificare un utente per eseguire il processo del logger e configurare le autorizzazioni per tale utente. Per ulteriori informazioni, consultare “Configurazione dell'accesso utente per un programma di registrazione file autonomo MFT” a pagina 727.
6. Opzionale: È possibile configurare ulteriormente il programma di registrazione file autonomo modificando il file `logger.properties` creato quando è stato eseguito il comando **fteCreateLogger** . Questo file è un file delle proprietà Java costituito da coppie chiave - valore. Il file `logger.properties` è nella directory *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/loggers/`*logger_name* . Per ulteriori informazioni sulle proprietà disponibili e sui relativi effetti, vedere MFT proprietà di configurazione del programma di registrazione.
7. Windows
   Opzionale: Se si sta utilizzando un sistema Windows , è possibile eseguire il programma di registrazione file autonomo come servizio Windows . Eseguire il comando **fteModifyLogger** con il parametro **-s** . Per ulteriori informazioni, consultare fteModifyLogger.
8. Avviare il programma di registrazione file autonomo con il comando **fteStartLogger** . Per ulteriori informazioni, vedi fteStartLogger.

   Se hai eseguito il passo precedente e hai utilizzato il comando **fteModifyLogger** con il parametro **-s** su Windows, il programma di registrazione file autonomo viene avviato come servizio Windows .
9. Controllare l'output del programma di registrazione. Il programma di registrazione file autonomo genera due tipi di output, dati di controllo trasferimento file e dati di diagnostica del programma di registrazione. I dati di controllo del trasferimento file sono disponibili in *MQ_DATA_PATH*`/mqft/logs/`*coordination_qmgr_name*`/loggers/`*logger_name*`/logs`. I dati diagnostici del programma di registrazione possono essere trovati in *MQ_DATA_PATH*`/mqft/logs/`*coordination_qmgr_name*`/loggers/`*logger_name*
10. È possibile arrestare il programma di registrazione utilizzando il comando **fteStopLogger** . Per ulteriori informazioni, vedi fteStopLogger.

Risultati

ULW *Formato del programma di registrazione file autonomo MFT*

Il formato delle informazioni del messaggio scritte dal programma di registrazione file può essere definito nel file `FileLoggerFormat.xml` .

La directory di configurazione per il programma di registrazione si trova in *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/loggers/`*logger_name*. Quando si crea un nuovo programma di registrazione file, viene creata una versione di questo file che contiene una serie predefinita di definizioni utilizzate dal programma di registrazione file. Per ulteriori informazioni sulla definizione del formato di log predefinito, consultare MFT formato di log predefinito del programma di registrazione file autonomo.

Se si desidera specificare il proprio formato di log personalizzato, modificare il file `FileLoggerFormat.xml` .

Una definizione del formato di log personalizzato

Una definizione del formato di log è costituita da una serie di tipi di messaggi con ciascun tipo di messaggio che dispone di una definizione del formato. Una definizione di formato per un tipo di messaggio consiste in una serie di inserimenti forniti in formato XPATH e in un separatore utilizzato per separare ciascun inserimento. L'ordine degli inserimenti determina l'ordine in cui il contenuto viene inserito nelle linee generate per l'output nei file di log. Ad esempio, questa è la definizione per il tipo di messaggio `callStarted` :

```
<callStarted>
  <format>
    <inserts>
      <insert type="user"   width="19" ignoreNull="false">/transaction/action/
       @time</insert>
      <insert type="user"   width="48" ignoreNull="false">/transaction/@ID</insert>
      <insert type="system" width="6"  ignoreNull="false">type</insert>
      <insert type="user"   width="0"  ignoreNull="false">/transaction/agent/
       @agent</insert>
      <insert type="user"   width="0"  ignoreNull="false">/transaction/agent/@QMgr</insert>
      <insert type="user"   width="0"  ignoreNull="false">/transaction/job/name</insert>
      <insert type="user"   width="0"  ignoreNull="true">/transaction/transferSet/
       call/command/@type</insert>
      <insert type="user"   width="0"  ignoreNull="true">/transaction/transferSet/
      call/command/@name</insert>
      <insert type="system" width="0"  ignoreNull="true">callArguments</insert>
    </inserts>
    <separator></separator>
  </format>
</callStarted>
```

Questo formato produce una riga nel file di log simile alla seguente:

```
2011-11-25T10:53:04;414d5120514d5f67627468696e6b20206466cf4e20004f02;[CSTR];
  AGENT1;AGENT_QM;Managed Call;executable;echo;call test;
```

Gli inserimenti forniti nella definizione del formato sono nell'ordine in cui le informazioni vengono visualizzate sulla riga del file di log. Per ulteriori informazioni sullo schema XML che definisce il formato per il file `FileLoggerFormat.xml` , consultare Stand-alone file logger format XSD.

Tipi di messaggio

Gli agent FTE scrivono una serie di tipi di messaggi differenti nell'argomento secondario `SYSTEM.FTE/Log` . Per ulteriori informazioni, consultare SYSTEM.FTE ArgomentoFTE. La definizione del file di log può contenere definizioni di formato per questi tipi di messaggi:

```
callCompleted
callStarted
monitorAction
monitorCreate
monitorFired
notAuthorized
```

```
scheduleDelete
scheduleExpire
scheduleSkipped
scheduleSubmitInfo
scheduleSubmitTransfer
scheduleSubmitTransferSet
transferStarted
transferCancelled
transferComplete
transferDelete
transferProgress
```

Il formato dei messaggi può variare. La maggior parte dei tipi di messaggi scrive una riga singola nel file di log per ogni messaggio di log utilizzato dall'argomento secondario SYSTEM.FTE/Log . Ciò porta al caso semplice in cui gli indirizzi XPATH forniti nella definizione del formato di log si riferiscono alla root del messaggio. Questi sono i tipi di messaggi che utilizzano questo metodo per scrivere l'output:

```
callCompleted
callStarted
monitorAction
monitorCreate
monitorFired
notAuthorized
scheduleDelete
scheduleExpire
scheduleSkipped
scheduleSubmitInfo
scheduleSubmitTransfer
transferStarted
transferCancelled
transferComplete
transferDelete
```

L'altro metodo utilizzato per scrivere un messaggio di log utilizza più righe per rappresentare gli elementi in una serie di trasferimenti all'interno di un messaggio di log. In questo caso, il formato fornito viene applicato a ciascun elemento nella serie di trasferimenti all'interno del messaggio di log. Se si desidera includere informazioni specifiche per ciascun elemento all'interno della serie di trasferimenti, è necessario che l'XPATH fornito utilizzi l'elemento come root XPATH. Questi sono i tipi di messaggi che utilizzano questo metodo per scrivere l'output:

```
scheduleSubmitTransferSet
transferProgress
```

Viene scritta una riga di output per ogni elemento nella serie di trasferimento. Le informazioni che si desidera correggere per tutti gli elementi in una serie di trasferimento possono ancora utilizzare gli indirizzi XPATH relativi al root del messaggio di log. Nel seguente esempio di definizione del formato `transferProgress` semplificato, sono corretti la data / ora e l'ID trasferimento. Tutte le informazioni relative a un elemento come root varieranno per ogni riga scritta. In questo esempio vengono scritte le informazioni sul file di origine e di destinazione per ogni elemento.

```
<transferProgress>
      <format>
        <inserts>
          <insert type="user"   width="19" ignoreNull="false">/transaction/action/
           @time</insert>
          <insert type="user"   width="48" ignoreNull="false">/transaction/@ID</insert>
          <insert type="system" width="6"  ignoreNull="false">type</insert>
          <insert type="user"   width="3"  ignoreNull="true">status/@resultCode</insert>
          <insert type="user"   width="0"  ignoreNull="false">source/file |
           source/queue</insert>
          <insert type="user"   width="0"  ignoreNull="false">source/file/@size |
           source/queue/@size</insert>
          <insert type="user"   width="5"  ignoreNull="true">source/@type</insert>
          <insert type="user"   width="6"  ignoreNull="true">source/@disposition</insert>
          <insert type="user"   width="0"  ignoreNull="false">destination/file |
            destination/queue</insert>
          <insert type="user"   width="0"  ignoreNull="false">destination/file/@size |
            destination/queue/@size</insert>
          <insert type="user"   width="5"  ignoreNull="true">destination/@type</insert>
          <insert type="user"   width="9"  ignoreNull="true">destination/@exist</insert>
          <insert type="user"   width="0"  ignoreNull="true">status/supplement</insert>
```

```
        </inserts>
        <separator></separator>
      </format>
    </transferProgress>
```

Ciò produce una voce del file di log di una o più righe in questo formato:

```
2011-11-25T13:45:16;414d5120514d5f67627468696e6b20206466cf4e20033702;[TPRO];0
  ;/src/test1.file;3575;file;leave ;/dest/test1.file;3575;file;overwrite;;
2011-11-25T13:45:16;414d5120514d5f67627468696e6b20206466cf4e20033702;[TPRO];0
  ;/src/test2.file;3575;file;leave ;/dest/test2.file;3575;file;overwrite;;
```

Inserisci formato

Sono disponibili due tipi di inserimento quando si definisce un formato per un tipo di messaggio: `utente` e `sistema`. Il tipo di un inserimento è definito nell'attributo `type` dell'elemento di inserimento. Entrambi i tipi di inserimenti possono anche avere il layout personalizzato utilizzando gli attributi **`width`** e **`ignoreNull`** dell'elemento di inserimento. Ad esempio:

```
<insert type="user" width="48" ignoreNull="false">/transaction/@ID</insert>
```

In questo esempio, l'inserimento prende le informazioni trovate nel messaggio di log in `/transaction/@ID` e le elimina o le riempisce di 48 caratteri prima di scriverle nel log. Se il contenuto di `/transaction/@ID` è null, scrive la stringa null dopo averla riempita con 48 caratteri perché l'attributo `ignoreNull` è impostato su `false`. Se `ignoreNull` è impostato su `true` , viene invece scritta la stringa vuota, riempita con 48 caratteri. L'impostazione width="0 " indica che la larghezza della colonna non è ritagliata, non significa che la larghezza è ritagliata a 0. L'attributo `ignoreNull` può essere utilizzato in questo modo per rilevare nel log quando viene rilevato un valore null quando non era previsto. Ciò può essere utile quando si esegue il debug di una nuova definizione del file di log.

Inserimenti definiti dall'utente

Un inserimento utente contiene un indirizzo XPATH per le informazioni da scrivere in tale inserimento. Questo indirizzo fa riferimento a una parte di informazioni trovata nel messaggio di log FTE. Per ulteriori informazioni sui formati dei messaggi di log, consultare:

- Formati dei messaggi del log di trasferimenti file
- Formati del messaggio di registrazione del trasferimento file pianificato
- Formato del messaggio di log del monitoraggio MFT

Inserimenti definiti dal sistema

Gli inserimenti definiti dal sistema contengono una parola chiave che fa riferimento a una parte di informazioni che non è possibile trovare nel messaggio di log o che non è facile definire utilizzando il linguaggio XPATH.

Gli inserimenti di sistemi supportati sono:

- `type` - Scrive il tipo di messaggio di log in un formato breve.
- `callArguments` - Scrive la serie di argomenti forniti a una chiamata gestita in formato separato da spazi.
- `transferMetaData` - Scrive la serie di voci di metadati definite per un trasferimento in formato *chiave*=*value* separato da virgole.

La seguente tabella elenca il valore di "tipo" per gli inserimenti definiti dal sistema per ciascun tipo di messaggio.

Tabella 51. Riepilogo dei tipi di messaggio supportati e relativi inserimenti di sistema "tipo".	
Tipo messaggio	**Valore dell'inserimento di sistema "type"**
callCompleted	[CCOM]
callStarted	[CSTR]
monitorAction	[MACT]
monitorCreate	[MCRT]
monitorFired	[MFIR]
notAuthorized	[AUTH]
scheduleDelete	[MODELLO]
scheduleExpire	[SEXP]
scheduleSkipped	[SSKP]
Informazioni scheduleSubmit	[SSIN]
Trasferimento scheduleSubmit	[SSTR]
scheduleSubmitTransferSet	[SSTS]
transferStarted	[TSTR]
transferCancelled	[TCAN]
transferComplete	[TCOM]
transferDelete	[DEL]
transferProgress	[TPRO]

ULW *Esclusione dei tipi di messaggi dal programma di registrazione file autonomo MFT*

Se si desidera escludere un determinato tipo di messaggio dall'output del programma di registrazione file, è possibile utilizzare elementi del tipo di messaggio vuoti.

Esempio

Ad esempio, la seguente definizione del formato arresta i messaggi `transferProgress` emessi dal programma di registrazione file.

```
<?xml version="1.0" encoding="UTF-8"?>
<logFormatDefinition  xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance" version="1.00"
 xsi:noNamespaceSchemaLocation="FileLoggerFormat.xsd">
  <messageTypes>
    <transferProgress></transferProgress>
  </messageTypes>
</logFormatDefinition>
```

ULW *Definizione di formati personalizzati per il programma di registrazione file autonomo MFT*

È possibile definire un sottoinsieme di tipi di messaggi personalizzati all'interno di una definizione del formato di log per ridurre la quantità di configurazione richiesta per personalizzare il formato del file di log.

Informazioni su questa attività

Se un elemento `messageTypes` non è incluso nel file `FileLoggerFormat.xml` , il formato per quel tipo di messaggio utilizza quello predefinito. È necessario solo specificare i formati che si desidera siano diversi da quelli predefiniti.

Esempio

In questo esempio, la definizione del formato sostituisce il formato predefinito per il tipo di messaggio `transferStarted` , con questa versione ridotta che emette solo l'utente che ha avviato il trasferimento. Tutti gli altri tipi di messaggio utilizzano il formato predefinito poiché non sono inclusi in questa definizione del formato di log:

```
<?xml version="1.0" encoding="UTF-8"?>
<logFormatDefinition  xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance" version="1.00"
 xsi:noNamespaceSchemaLocation="FileLoggerFormat.xsd">
  <messageTypes>
    <transferStarted>
      <format>
        <inserts>
          <insert type="user"   width="19" ignoreNull="false">/transaction/action/
           @time</insert>
          <insert type="user"   width="48" ignoreNull="false">/transaction/@ID</insert>
          <insert type="system" width="6"  ignoreNull="false">type</insert>
          <insert type="user"   width="0"  ignoreNull="true">/transaction/originator/
           userID</insert>
        </inserts>
        <separator>;</separator>
      </format>
    </transferStarted>
  </messageTypes>
</logFormatDefinition>
```

Riferimenti correlati

Formato di log predefinito del programma di registrazione file autonomo MFT

Formato del programma di registrazione file autonomo XSD

ULW *Riduzione dei messaggi duplicati nel programma di registrazione file autonomo MFT*

I messaggi di log duplicati possono verificarsi nel log del programma di registrazione file autonomo. Utilizzando un file `logger.properties` è possibile ottimizzare il programma di registrazione file autonomo e ridurre il numero di duplicati.

Messaggi duplicati nel log del programma di registrazione file

In caso di errore, un messaggio di log potrebbe essere scritto nel log del programma di registrazione file autonomo senza l'utilizzo del messaggio di log da SYSTEM.FTE/Log# argomento di cui si sta eseguendo il commit in IBM MQ. Se ciò si verifica, quando il programma di registrazione file autonomo viene riavviato, richiamerà lo stesso messaggio una seconda volta e lo scriverà nuovamente nel file di log. Pianificare la gestione di questi duplicati quando si esaminano i file di log manualmente o quando vengono elaborati automaticamente. Per facilitare il rilevamento dei duplicati, il programma di registrazione file autonomo emette il seguente messaggio nel file di log quando viene avviato:

```
BFGDB0054I: The file logger has successfully started
```

I duplicati si verificano sempre intorno all'ora di inizio del programma di registrazione file autonomo, perché questo è quando viene elaborato l'ultimo messaggio letto prima dell'errore dell'istanza

precedente. Sapendo quando la nuova istanza è stata avviata, è possibile rilevare se i duplicati devono essere previsti e se devono essere gestiti o meno.

Riduzione del numero di duplicati

Il programma di registrazione file autonomo raggruppa insieme i messaggi di log che elabora in transazioni per migliorare le prestazioni. Questa dimensione batch è il numero massimo di messaggi duplicati che è possibile visualizzare in caso di errore. Per ridurre il numero di duplicati è possibile ottimizzare la seguente proprietà nel file `logger.properties` :

```
wmqfte.max.transaction.messages
```

Ad esempio, impostandolo su 1, il numero massimo di messaggi duplicati viene ridotto a 1. Tenere presente che la modifica di questo valore ha un effetto sulle prestazioni del programma di registrazione file autonomo, pertanto è necessario un test completo per garantire che ciò non influisca negativamente sul sistema.

Il file `logger.properties` è nella directory *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/loggers/`*logger_name* . Per ulteriori informazioni sulle proprietà disponibili e i relativi effetti, vedere MFT proprietà di configurazione del programma di registrazione

ULW *Configurazione dell'accesso utente per un programma di registrazione file autonomo MFT*

In un ambiente di test, è possibile aggiungere qualsiasi nuovo privilegio necessario al proprio account utente normale. In un ambiente di produzione, si consiglia di creare un nuovo utente con le autorizzazioni minime richieste per eseguire il lavoro.

Informazioni su questa attività

È necessario installare il programma di registrazione file autonomo e IBM MQ su un singolo sistema. Configurare le autorizzazioni dell'utente come segue:

Procedura

1. Verificare che l'utente disponga dell'autorizzazione per leggere e, se necessario, eseguire i file installati come parte dell'installazione di Managed File Transfer .
2. Assicurarsi che l'utente disponga dell'autorizzazione per creare e scrivere in qualsiasi file nella directory `logs` che si trova nella directory di configurazione. Questa directory viene utilizzata per un log eventi e, se necessario, per la traccia diagnostica e i file FFDC (First Failure Data Capture).
3. Assicurarsi che l'utente disponga di un proprio gruppo e che non appartenga ad alcun gruppo con ampie autorizzazioni sul gestore code di coordinamento. L'utente non deve essere nel gruppo mqm. Su alcune piattaforme, al gruppo staff viene automaticamente fornito l'accesso al gestore code; l'utente del programma di registrazione file autonomo non dovrebbe essere nel gruppo staff. È possibile visualizzare i record di autorizzazioni per il gestore code stesso e per gli oggetti in esso contenuti utilizzando IBM MQ Explorer. Fare clic con il pulsante destro del mouse sull'oggetto e selezionare **Autorizzazioni oggetto> Gestisci record di autorizzazione**. Nella riga di comando, è possibile utilizzare i comandi dspmqaut (visualizza autorità) o dmpmqaut (dump autorità).
4. Utilizzare la finestra **Gestisci record di autorizzazione** nel comando IBM MQ Explorer o setmqaut (concessione o revoca dell'autorizzazione) per aggiungere le autorizzazioni per il gruppo dell'utente (su UNIX, IBM MQ le autorizzazioni sono associate solo ai gruppi, non ai singoli utenti). Le autorità richieste sono le seguenti:
   - Connettere e richiedere sul gestore code (le librerie di IBM MQ Java richiedono l'autorizzazione di interrogazione per funzionare).
   - Sottoscrivere l'autorizzazione sul SISTEMA SYSTEM.FTE .
   - Inserire l'autorizzazione su SYSTEM.FTE.LOG.RJCT.*nome_programma di registrazione* .

- Ottenere l'autorizzazione su SYSTEM.FTE.LOG.CMD.*nome_programma di registrazione* .

I nomi delle code di comando e di rifiuto forniti sono i nomi predefiniti. Se sono stati scelti nomi di coda differenti quando sono state configurate le code del programma di registrazione file autonomo, aggiungere le autorizzazioni a tali nomi di coda.

Installazione del programma di registrazione database autonomo MFT

Completare la seguente procedura per installare e configurare il programma di registrazione database autonomo.

Informazioni su questa attività

Importante: I logger Managed File Transfer non sono supportati sulla piattaforma IBM i .

Per ulteriori informazioni sul programma di registrazione database autonomo, consultare "Configurazione di un programma di registrazione MFT" a pagina 719.

Nota: Non è possibile eseguire più di un programma di registrazione database (autonomo o Java EE) sullo stesso schema in un database alla volta. Se si tenta di eseguire questa operazione, si verificherebbe un conflitto durante il tentativo di scrivere i dati del log di trasferimento nel database.

Procedura

1. Installare il proprio software di database utilizzando la relativa documentazione.

   Se il supporto JDBC è un componente facoltativo per il database, è necessario installare questo componente.
2. Eseguire il comando **fteCreateLogger** impostando il parametro **-loggerType** su DATABASE per creare un programma di registrazione database autonomo. Per ulteriori informazioni, vedi fteCreateLogger.

   Il nome schema predefinito è FTELOG. Se si utilizza un nome schema diverso da FTELOG, è necessario modificare il file SQL fornito appropriato per il database, `ftelog_tables_db2.sql` o `ftelog_tables_oracle.sql`, in modo da riflettere questo nome schema prima di procedere al passo successivo. Per ulteriori informazioni, consultare wmqfte.database.schema in MFT logger configuration properties.
3. Creare le tabelle di database richieste utilizzando gli strumenti del database.

   Multi Su Multipiattaforme, i file `ftelog_tables_db2.sql` e `ftelog_tables_oracle.sql` contengono comandi SQL che è possibile eseguire per creare le tabelle.

   z/OS Su z/OS, il file da eseguire dipende dalla versione di Db2 for z/OS che si sta utilizzando:

   - Per Db2 for z/OS 9.0 e versioni precedenti, eseguire il file `ftelog_tables_zos.sql` per creare le tabelle. Questo file crea le tabelle utilizzando un tipo di dati INTEGER per i campi che indicano le dimensioni dei file trasferiti e l'ID tabella associato a ogni trasferimento.
   - Per Db2 for z/OS 9.1 e versioni successive, eseguire il file `ftelog_tables_zos_bigint.sql` per creare le tabelle. Questo file crea le tabelle utilizzando un tipo di dati BIGINT per i campi che indicano le dimensioni dei file trasferiti e l'ID tabella associato a ogni trasferimento.
4. Eseguire i comandi MQSC, forniti dal comando **fteCreateLogger** , sul gestore code dei comandi del programma di registrazione per creare le code del programma di registrazione. Il programma di registrazione database autonomo utilizza due code sul gestore code di coordinazione. La prima coda è una coda comandi in cui vengono inseriti i messaggi per controllare il funzionamento del programma di registrazione database autonomo. Il nome predefinito di questa coda comandi è SYSTEM.FTE.LOG.CMD.*nome_logger*. La seconda coda è una coda elementi respinti. Poiché il programma di registrazione database autonomo non elimina mai i messaggi di log, se il programma di registrazione rileva un messaggio che non è in grado di gestire, inserisce il messaggio nella coda di elementi respinti per l'esame e la possibile rielaborazione. Non si consiglia di utilizzare la coda dei messaggi non recapitabili del gestore code per questo scopo, poiché i messaggi rifiutati non hanno

un'intestazione DLH e perché i messaggi rifiutati non devono essere combinati con i messaggi inseriti nella coda dei messaggi non recapitabili per altri motivi. Il nome predefinito per la coda di elementi respinti è SYSTEM.FTE.LOG.RJCT.*nome_logger*. Queste due code vengono definite nei file di script MQSC generati dal comando **fteCreateLogger** .

5. Scegliere un utente e configurare le autorizzazioni
6. Opzionale: È possibile configurare ulteriormente il programma di registrazione database autonomo modificando il file `logger.properties` creato dal comando **fteCreateLogger** nel passo “2” a pagina 728. Questo file è un file delle proprietà Java costituito da coppie chiave - valore. Il file `logger.properties` è nella directory *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/loggers/`*logger_name* . Per ulteriori informazioni sulle proprietà disponibili e sui relativi effetti, consultare MFT proprietà di configurazione del programma di registrazione.
7. Windows
   Opzionale: Se si sta utilizzando un sistema Windows , è possibile eseguire il programma di registrazione database autonomo come un servizio Windows . Eseguire il comando **fteModifyLogger** con il parametro **-s** . Per ulteriori informazioni, consultare fteModifyLogger.
8. Opzionale: Se il database utilizzato è Oracle o si sta eseguendo la connessione a un database Db2 in remoto, sarà necessario specificare un nome utente e una password che il programma di registrazione utilizzerà per eseguire l'autenticazione con il server di database. Questo nome utente e password vengono specificati in un file di credenziali conforme al formato definito dallo schema `MQMFTCredentials.xsd` . Per ulteriori informazioni, consultare Formato file delle credenziali MFT. Dopo aver creato il file delle credenziali, è necessario specificare l'ubicazione del file delle credenziali nel file `logger.properties` utilizzando la proprietà `wmqfte.database.credentials.file` .
9. Avviare il programma di registrazione database autonomo utilizzando il comando **fteStartLogger** . Per impostazione predefinita, il programma di registrazione database autonomo viene eseguito in background e il programma di registrazione database autonomo inserisce l'output in un file nella directory `logs` . Se si desidera eseguire il programma di registrazione database autonomo in primo piano e produrre l'output sulla console e sul file di log, aggiungere il parametro **-F** al comando **fteStartLogger** .

   Se hai eseguito il passo precedente e hai utilizzato il comando **fteModifyLogger** con il parametro **-s** su Windows, il programma di registrazione database autonomo viene avviato come un servizio Windows .

Utilizzo di MFT con un database remoto

È possibile utilizzare il programma di registrazione Managed File Transfer per comunicare con un database su un sistema remoto.

Informazioni su questa attività

Se si dispone di un database installato su una macchina diversa da quella su cui è installato Managed File Transfer , completare la seguente procedura. La procedura si applica sia a Db2 che a Oracle , se non diversamente specificato.

Procedura

1. Installare un client database sul sistema su cui è stato installato Managed File Transfer .
2. Aggiungere il server database remoto alla configurazione del client database locale. Questo aggiornamento della configurazione è necessario per Managed File Transfer e IBM MQ per accedere correttamente al database.
3. Specificare le nuove proprietà nel file di `logger.properties` per connettersi al database utilizzando il file delle credenziali **wmfte.database.credentials.file**.

   Nota: Le versioni precedenti di Managed File Transfer utilizzavano le proprietà **wmqfte.oracle.user** o **wmqfte.database.user**e **wmqfte.oracle.password** o **wmqfte.database.password**. Queste proprietà sono ora obsolete. Utilizzare invece **wmfte.database.credentials.file** .

4. **SoloOracle :** per consentire una connessione remota al database, modificare la stanza XAResourceManager nel file `qm.ini` del gestore code di coordinamento nel seguente modo (assicurandosi di modificare il nome del database, il nome utente e la password utente in modo che corrispondano alle proprie informazioni):

   `Oracle_XA+Acc=P/ftelog/qgw783jhT+SesTm=35+DB=FTEAUDIT1`**`+SqlNet=FTEAUDIT1`**`+threads=false`,
   la modifica viene evidenziata in grassetto.
5. **SoloOracle :** specificare host e porta nel file `logger.properties` , utilizzando le proprietà **`wmqfte.oracle.host`** e **`wmqfte.oracle.port`** . I valori predefiniti per l'host e la porta consentono di lavorare con un client di database locale, quindi se è stato precedentemente utilizzato un database locale, è possibile che questi valori non siano stati impostati.

Riferimenti correlati

Proprietà di configurazione del programma di registrazione MFT

Configurazione dell'accesso utente per un programma di registrazione database autonomo MFT

In un ambiente di test, è possibile aggiungere qualsiasi nuovo privilegio necessario al proprio account utente normale. In un ambiente di produzione, si consiglia di creare un nuovo utente con le autorizzazioni minime richieste per eseguire il lavoro.

Informazioni su questa attività

Il numero e il tipo di account utente necessari per eseguire il programma di registrazione database autonomo dipendono dal numero di sistemi utilizzati. È possibile installare il programma di registrazione database autonomo, IBM MQ e il proprio database su un singolo sistema o su due sistemi. Il programma di registrazione database autonomo deve trovarsi sullo stesso sistema di IBM MQ. I componenti possono essere installati nelle seguenti topologie:

Logger del database autonomo, IBM MQ e il database tutti sullo stesso sistema
: È possibile definire un singolo utente del sistema operativo da utilizzare con tutti e tre i componenti. Questa è una configurazione adatta per il programma di registrazione database autonomo. Il programma di registrazione database autonomo utilizza la modalità Bindings per connettersi a IBM MQ e una connessione nativa per connettersi al database.

Programma di registrazione del database autonomo e IBM MQ su un sistema, il database su un sistema separato
: Si creano due utenti per questa configurazione: un utente del sistema operativo sul sistema che esegue il programma di registrazione database autonomo e un utente del sistema operativo con accesso remoto al database sul server database. Questa è una configurazione adatta per il programma di registrazione database autonomo che utilizza un database remoto. Il programma di registrazione database autonomo utilizza la modalit ... Bind per connettersi a IBM MQ e una connessione client per accedere al database.

Come esempio, il resto di queste istruzioni presuppone che l'utente sia denominato `ftelog`, ma è possibile utilizzare qualsiasi nome utente. Configurare le autorizzazioni dell'utente come segue:

Procedura

1. Verificare che l'utente disponga dell'autorizzazione per leggere e, se necessario, eseguire i file installati come parte dell'installazione di Managed File Transfer Strumenti remoti e Documentation .
2. Verificare che l'utente disponga dell'autorizzazione per creare e scrivere in qualsiasi file nella directory `logs` (nella directory di configurazione). Questa directory viene utilizzata per un log eventi e, se necessario, per la traccia diagnostica e i file FFDC.
3. Verificare che l'utente disponga di un proprio gruppo e che non sia presente anche in gruppi con autorizzazioni di ampio respiro sul gestore code di coordinamento. L'utente non deve essere nel gruppo mqm. Su alcune piattaforme, al gruppo di staff viene automaticamente fornito l'accesso al gestore code; l'utente del programma di registrazione database autonomo non deve far parte del

gruppo di staff. È possibile visualizzare i record di autorizzazioni per il gestore code stesso e per gli oggetti in esso contenuti utilizzando IBM MQ Explorer. Fare clic con il pulsante destro del mouse sull'oggetto e selezionare **Autorizzazioni oggetto> Gestisci record di autorizzazione**. Nella riga di comando, è possibile utilizzare i comandi dspmqaut (visualizza autorità) o dmpmqaut (dump autorità).

4. Utilizzare la finestra **Gestisci record di autorizzazione** nel comando IBM MQ Explorer o setmqaut (concessione o revoca dell'autorizzazione) per aggiungere le autorizzazioni per il gruppo dell'utente (su UNIX, IBM MQ le autorizzazioni sono associate solo ai gruppi, non ai singoli utenti). Le autorità richieste sono le seguenti:
   - Connettere e richiedere sul gestore code (le librerie di IBM MQ Java richiedono l'autorizzazione di interrogazione per funzionare).
   - Sottoscrivere l'autorizzazione sul SISTEMA SYSTEM.FTE .
   - Inserire l'autorizzazione su SYSTEM.FTE.LOG.RJCT.*nome_programma di registrazione* .
   - Ottenere l'autorizzazione su SYSTEM.FTE.LOG.CMD.*nome_programma di registrazione* .

   I nomi delle code di comando e di rifiuto forniti sono i nomi predefiniti. Se sono stati scelti nomi di coda differenti quando sono state configurate le code del programma di registrazione database autonomo, aggiungere le autorizzazioni a tali nomi di coda.
5. Eseguire la configurazione utente specifica per il database che si sta utilizzando.
   - Se il database è Db2, effettuare le seguenti operazioni:

     Esistono diversi meccanismi per la gestione degli utenti del database con Db2. Queste istruzioni si applicano allo schema predefinito in base agli utenti del sistema operativo.

     – Assicurarsi che l'utente `ftelog` non si trovi in alcun gruppo di gestione Db2 (ad esempio, db2iadm1, db2fadm1o dasadm1)
     – Fornire all'utente l'autorizzazione per connettersi al database e l'autorizzazione per selezionare, inserire e aggiornare le tabelle create come parte del Passo 2: creare le tabelle di database richieste
   - Se il database è Oracle, effettuare le seguenti operazioni:
     – Assicurarsi che l'utente `ftelog` non si trovi in alcun gruppo di gestione Oracle (ad esempio, ora_dba su Windows o dba su UNIX)
     – Fornire all'utente l'autorizzazione per connettersi al database e l'autorizzazione per selezionare, inserire e aggiornare le tabelle create come parte del Passo 2: creare le tabelle di database richieste

Configurazioni alternative per un logger autonomo MFT

Generalmente, un programma di registrazione autonomo Managed File Transfer , sia esso un file o un tipo di database, si trova sullo stesso sistema del gestore code di coordinamento ed è connesso al gestore code di coordinazione in modalità di bind IBM MQ . Tuttavia, può anche essere installato sullo stesso sistema di qualsiasi gestore code che abbia la connettività al gestore code di coordinamento. Il programma di registrazione autonomo riceve i messaggi utilizzando una sottoscrizione, che il programma di registrazione autonomo crea automaticamente. Questa è la configurazione descritta nelle istruzioni di installazione.

Tuttavia, se si hanno considerazioni specifiche del sito, è possibile configurare un programma di registrazione autonomo per ricevere i messaggi in altri due modi, controllati dalla proprietà wmqfte.message.source.type . Questa proprietà è descritta in MFT proprietà di configurazione del programma di registrazione.

Sottoscrizione amministrativa

Per impostazione predefinita, un programma di registrazione autonomo crea la propria sottoscrizione a SYSTEM.FTE/Log/#, utilizzando le opzioni di sottoscrizione durevole predefinite e una sottoscrizione gestita (ossia, il gestore code controlla la coda di backup utilizzata per conservare i messaggi prima che vengano trasmessi all'applicazione). Se sono richieste altre opzioni sulla sottoscrizione o sulla coda, è

possibile creare una sottoscrizione da soli, impostare le opzioni richieste e configurare il programma di registrazione autonomo per utilizzare tale sottoscrizione. Ricordarsi di aggiungere l'autorizzazione per il programma di registrazione autonomo per utilizzare la sottoscrizione creata.

Un esempio di utilizzo di questa configurazione è la partizione dello spazio di log utilizzando due sottoscrizioni jolly, per inviare i log dagli agent il cui nome inizia con FINANCE in un database e i log dagli agent che iniziano con ACCOUNTING in un altro. Questo tipo di configurazione richiede due istanze del programma di registrazione autonomo, ciascuna con il proprio file `logger.properties` che fa riferimento alla richiesta e la propria coda comandi e coda di elementi respinti.

Per raccogliere i messaggi di log solo dagli agent i cui nomi iniziano con ACCOUNTING, creare un oggetto sottoscrizione sul gestore code di coordinazione con una stringa di argomenti SYSTEM.FTE/Log/ ACCOUNTING*. Impostare il valore **Utilizzo carattere jolly** su **Carattere jolly di livello carattere**. È inoltre necessario aggiungere voci al file `logger.properties` per il logger. Ad esempio, se si crea un oggetto sottoscrizione denominato ACCOUNTING.LOGS con queste impostazioni, aggiungere le voci seguenti al file `logger.properties` :

```
wmqfte.message.source.type=administrative subscription
wmqfte.message.source.name=ACCOUNTING.LOGS
```

Il programma di registrazione autonomo gestisce i messaggi di log che iniziano con la stringa di argomenti SYSTEM.FTE/Log/ . È possibile specificare una stringa di argomenti più restrittiva, ma non è possibile specificare una stringa meno restrittiva. Se si specifica una stringa meno restrittiva in errore, tutte le pubblicazioni relative a una stringa di argomenti diversa da SYSTEM.FTE/Log/ passare alla coda di elementi respinti e il programma di registrazione autonomo produce il messaggio di errore BFGDB0002E. Questo messaggio di errore implica un problema con la configurazione del programma di registrazione autonomo.

Coda

La topologia tipica è quella in cui il programma di registrazione autonomo viene eseguito sullo stesso sistema del gestore code di coordinamento. Se ciò non è possibile, è possibile creare una sottoscrizione sul gestore code di coordinamento utilizzando una coda su un altro gestore code come destinazione della sottoscrizione (utilizzando una definizione della coda remota o utilizzando la proprietà DESTQMGR della sottoscrizione). Il programma di registrazione può quindi essere eseguito sul sistema che ospita il secondo gestore code e leggere i messaggi dalla coda. Per garantire l'integrità delle transazioni, il programma di registrazione autonomo deve sempre connettersi al proprio gestore code in modalità di bind. È necessario definire la coda di elementi respinti e la coda comandi sullo stesso gestore code a cui si connette il programma di registrazione autonomo. I gestori code devono essere IBM WebSphere MQ 7.5 o successivi.

Ad esempio, per raccogliere i messaggi di log che vengono inseriti nella coda USER.QUEUE da una richiesta, aggiungere le seguenti voci al file `logger.properties` :

```
wmqfte.message.source.type=queue
wmqfte.message.source.name=USER.QUEUE
```

Installazione del programma di registrazione database Java EE per MFT

Seguire queste istruzioni per installare e configurare il programma di registrazione database JEE da utilizzare con Managed File Transfer.

Informazioni su questa attività

Per ulteriori informazioni sul programma di registrazione database Java EE , consultare l'argomento “Configurazione di un programma di registrazione MFT” a pagina 719.

Nota: Non è possibile eseguire un programma di registrazione database Java EE contemporaneamente a un programma di registrazione autonomo, a meno che tali programmi di registrazione non utilizzino istanze separate del database.

Procedura

1. Prima di installare il programma di registrazione database Java EE , è necessario preparare il proprio ambiente. Utilizzare le istruzioni nell'argomento “Preparazione all'installazione del programma di log del database Java EE per MFT” a pagina 733.
2. Si installa il programma di registrazione database Java EE in un server delle applicazioni conforme a Java Platform, Enterprise Edition (Java EE). Per istruzioni, consultare i seguenti argomenti:
   - “Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server 7.0” a pagina 736
   - “Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server Community Edition” a pagina 741

Attività correlate

“Preparazione all'installazione del programma di log del database Java EE per MFT” a pagina 733
Seguire queste istruzioni per preparare l'ambiente Managed File Transfer prima di installare il programma di registrazione database Java EE .

“Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server 7.0” a pagina 736
Seguire queste istruzioni per installare e configurare il programma di registrazione database Java Platform, Enterprise Edition (Java EE) per Managed File Transfer con WebSphere Application Server 7.0.

“Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server Community Edition” a pagina 741
Seguire queste istruzioni per installare e configurare il programma di registrazione database Java Platform, Enterprise Edition (Java EE) per Managed File Transfer con WebSphere Application Server Community Edition.

“Configurazione dell'accesso utente per il logger del database Java EE per MFT” a pagina 744
Quando si configura il programma di registrazione database Java Platform, Enterprise Edition (Java EE) per Managed File Transfer, sono necessari gli account utente per accedere a IBM MQ, al database e al sistema operativo. Il numero di utenti del sistema operativo richiesto dipende dal numero di sistemi utilizzati per ospitare questi componenti.

“Migrazione dal programma di registrazione database autonomo al programma di registrazione database di Java EE per MFT” a pagina 747
È possibile eseguire la migrazione dal programma di registrazione database autonomo al programma di registrazione database Java EE . È necessario arrestare il programma di registrazione database autonomo e installare il programma di registrazione database JEE. Per evitare la perdita o la duplicazione delle voci di log, è necessario arrestare la pubblicazione dei messaggi nel sistema SYSTEM.FTE prima di arrestare il programma di registrazione database autonomo e riavviarlo dopo aver installato il programma di registrazione database Java EE . Eseguire il backup del database prima della migrazione.

Riferimenti correlati

Autorità per il logger MFT

Preparazione all'installazione del programma di log del database Java EE per MFT

Seguire queste istruzioni per preparare l'ambiente Managed File Transfer prima di installare il programma di registrazione database Java EE .

Informazioni su questa attività

Per ulteriori informazioni sul programma di registrazione database Java EE , consultare l'argomento “Configurazione di un programma di registrazione MFT” a pagina 719.

Procedura

1. Installare il proprio software di database utilizzando la relativa documentazione.

   Se il supporto JDBC è un componente facoltativo per il database, è necessario installare questo componente.
2. Creare un database utilizzando gli strumenti forniti dal proprio database. Il database deve avere un tablespace e una dimensione pagina bufferpool di almeno 8K.

   Il nome schema predefinito è FTELOG. Se si utilizza un nome schema diverso da FTELOG, è necessario modificare il file SQL fornito appropriato per il proprio database, `ftelog_tables_db2.sql` o `ftelog_tables_oracle.sql`, per rispecchiarlo prima di procedere al passo successivo.
3. Creare le tabelle di database richieste utilizzando gli strumenti del database.

   Multi Su Multipiattaforme, i file `ftelog_tables_db2.sql` e `ftelog_tables_oracle.sql` contengono comandi SQL che è possibile eseguire per creare le tabelle.

   z/OS Su z/OS, il file da eseguire dipende dalla versione di Db2 for z/OS che si sta utilizzando:

   - Per Db2 for z/OS 9.0 e versioni precedenti, eseguire il file `ftelog_tables_zos.sql` per creare le tabelle. Questo file crea le tabelle utilizzando un tipo di dati INTEGER per i campi che indicano le dimensioni dei file trasferiti e l'ID tabella associato a ogni trasferimento.
   - Per Db2 for z/OS 9.1 e versioni successive, eseguire il file `ftelog_tables_zos_bigint.sql` per creare le tabelle. Questo file crea le tabelle utilizzando un tipo di dati BIGINT per i campi che indicano le dimensioni dei file trasferiti e l'ID tabella associato a ogni trasferimento.
4. Se è stato modificato il nome dello schema da FTELOG, è necessario modificare il nome dello schema nel file EAR. Per ulteriori informazioni, fare riferimento a “Modifica del nome dello schema nel programma di registrazione database Java EE per MFT” a pagina 734.
5. Creare una coda di elementi respinti in IBM MQ.

   Poiché il programma di registrazione non elimina mai i messaggi di log, se il programma di registrazione rileva un messaggio che non può gestire, inserisce il messaggio nella coda di elementi respinti per l'esame e la possibile rielaborazione. Non utilizzare la coda di messaggi non recapitabili del gestore code per questo scopo, perché i messaggi rifiutati non dispongono di un'intestazione DLH e perché i messaggi rifiutati non devono essere combinati con i messaggi inseriti nella coda di messaggi non recapitabili per altri motivi. Il comando **`fteCreateLogger`** crea una coda di elementi respinti. Il nome predefinito per questa coda elementi respinti è SYSTEM.FTE.LOG.RJCT.*nome_programma di registrazione*
6. Seguire le istruzioni riportate nell'argomento “Configurazione dell'accesso utente per il logger del database Java EE per MFT” a pagina 744.

Operazioni successive

Ora è possibile installare il programma di registrazione del database Java EE in un server delle applicazioni compatibile con Java EE. Utilizzare le istruzioni riportate nei seguenti argomenti, in base al server delle applicazioni utilizzato:

- “Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server 7.0” a pagina 736
- “Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server Community Edition” a pagina 741

Modifica del nome dello schema nel programma di registrazione database Java EE per MFT

Il programma di registrazione database Java Platform, Enterprise Edition (Java EE) può utilizzare un database che ha un nome schema non predefinito. È necessario modificare il nome schema nel file EAR del programma di registrazione database Java EE .

Informazioni su questa attività

Per modificare il nome dello schema utilizzato dal programma di registrazione database Java EE , completare la seguente procedura:

Procedura

1. Estrarre il file JAR JPA dal file EAR utilizzando il seguente comando:

   ```
   jar -xvf ear_file lib/jpa_file
   ```

   dove:

   - *ear_file* è `com.ibm.wmqfte.databaselogger.jee.oracle.ear` o `com.ibm.wmqfte.databaselogger.jee.ear` a seconda che si stia utilizzando Db2 o Oracle.
   - *jpa_file* è `com.ibm.wmqfte.web.jpa.oracle.jar` o `com.ibm.wmqfte.web.jpa.jar` a seconda che si stia utilizzando Db2 o Oracle.
2. Estrarre il file `persistence.xml` dal file JAR JPA utilizzando il seguente comando:

   ```
   jar -xvf lib/jpa_file META_INF/persistence.xml
   ```

   dove:

   - *jpa_file* è `com.ibm.wmqfte.web.jpa.oracle.jar` o `com.ibm.wmqfte.web.jpa.jar` a seconda che si stia utilizzando Db2 o Oracle.
3. Modificare il file `persistence.xml` per modificare la seguente riga:

   ```
   <property name="openjpa.jdbc.Schema" value="schema_name" />
   ```

   dove

   - *schema_name* è il nome schema che si desidera utilizzare.
4. Aggiornare il JAR JPA con il file `persistence.xml` modificato utilizzando il seguente comando:

   ```
   jar -uvf lib/jpa_file META_INF/persistence.xml
   ```

   dove:

   - *jpa_file* è `com.ibm.wmqfte.web.jpa.oracle.jar` o `com.ibm.wmqfte.web.jpa.jar` a seconda che si stia utilizzando Db2 o Oracle.
5. Aggiornare il file EAR con il file JAR JPA modificato utilizzando il seguente comando:

   ```
   jar -uvf ear_file lib/jpa_file
   ```

   dove:

   - *ear_file* è `com.ibm.wmqfte.databaselogger.jee.oracle.ear` o `com.ibm.wmqfte.databaselogger.jee.ear` a seconda che si stia utilizzando Db2 o Oracle.
   - *jpa_file* è `com.ibm.wmqfte.web.jpa.oracle.jar` o `com.ibm.wmqfte.web.jpa.jar` a seconda che si stia utilizzando Db2 o Oracle.

Operazioni successive

Utilizzare il file EAR modificato per installare il programma di registrazione database Java EE .

Attività correlate

“Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server 7.0” a pagina 736

Seguire queste istruzioni per installare e configurare il programma di registrazione database Java Platform, Enterprise Edition (Java EE) per Managed File Transfer con WebSphere Application Server 7.0.

“Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server Community Edition” a pagina 741
Seguire queste istruzioni per installare e configurare il programma di registrazione database Java Platform, Enterprise Edition (Java EE) per Managed File Transfer con WebSphere Application Server Community Edition.

Impostazione del percorso della libreria nativa in WebSphere Application Server 7.0
Se si distribuisce l'applicazione del programma di registrazione database Java Platform, Enterprise Edition (Java EE) su WebSphere Application Server 7.0e si desidera utilizzare le connessioni in modalità bind tra l'applicazione e IBM MQ, è necessario configurare il fornitore di messaggistica IBM MQ con l'ubicazione delle librerie native IBM MQ sul sistema.

Informazioni su questa attività
Se non si imposta il percorso della libreria nativa nel server delle applicazioni, si potrebbe ricevere il seguente messaggio di errore nel log di uscita del sistema WebSphere Application Server 7.0 :

```
A connection could not be made to WebSphere MQ for the following reason:
  CC=2;RC=2495;AMQ8568: The native JNI library 'mqjbnd' was not found. [3=mqjbnd]
```

Utilizzare la console di amministrazione WebSphere Application Server 7.0 per completare la seguente procedura:

Procedura
1. Nel pannello di navigazione, espandere **Risorse** > **JMS** > **Provider JMS**.
2. Selezionare il provider di messaggistica IBM MQ che si trova nell'ambito corretto per la factory di connessione o la specifica di attivazione che crea la connessione in modalità bind.

   Nota: Le informazioni sul percorso nativo nell'ambito `Server` vengono utilizzate in preferenza alle informazioni sul percorso nativo negli ambiti superiori e le informazioni sul percorso nativo nell'ambito `Node` vengono utilizzate in preferenza alle informazioni sul percorso nativo nell'ambito `Cell` .
3. In Proprietà generali, nel campo **Percorso libreria nativa** , immettere il nome completo della directory che contiene le librerie native IBM MQ .

   Ad esempio, su Linux immettere `/opt/mqm/java/lib`. Immettere un solo nome di directory.
4. Fare clic su **OK**.
5. Riavviare il server delle applicazioni per aggiornare la configurazione.
6. Richiesto: Riavviare il server delle applicazioni una seconda volta per caricare le librerie.

Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server 7.0
Seguire queste istruzioni per installare e configurare il programma di registrazione database Java Platform, Enterprise Edition (Java EE) per Managed File Transfer con WebSphere Application Server 7.0.

Prima di iniziare
Prima di installare l'applicazione programma di registrazione database JEE, seguire le istruzioni riportate negli argomenti “Preparazione all'installazione del programma di log del database Java EE per MFT” a pagina 733 e “Impostazione del percorso della libreria nativa in WebSphere Application Server 7.0” a pagina 736.

Informazioni su questa attività
Per ulteriori informazioni sul programma di registrazione database Java EE , consultare “Configurazione di un programma di registrazione MFT” a pagina 719.

Procedura

1. Impostare il provider JDBC XA:
   a) Seleziona **Resources** > **JDBC** > **JDBC Providers** dalla navigazione della console di amministrazione WebSphere Application Server 7.0 .
   b) Creare un provider JDBC utilizzando la procedura guidata della console, facendo clic su **Nuovo**.
   c) Nel passo 1 della procedura guidata, selezionare il database che si sta utilizzando dall'elenco **Tipo di database** e il tipo di fornitore associato dall'elenco **Tipo di fornitore** . Dall'elenco **Tipo di implementazione** , selezionare **Origine dati XA**. Fare clic su **Avanti**.
   d) Al passo 2 della procedura guidata, verificare che l'ubicazione della directory dei file jar del database richiesti sia impostata correttamente. Fare clic su **Avanti**.
   e) Fare clic su **Fine** nella pagina di riepilogo per creare il provider JDBC .
2. Creare alias di autenticazione. Si crea un alias per l'origine dati e un altro per IBM MQ:
   a) Seleziona **Sicurezza** > **Sicurezza globale** dalla navigazione della console di gestione WebSphere Application Server 7.0 .
   b) Nell'intestazione **Autenticazione** , espandere **JAAS (Java Authentication and Authorization Service)**.
   c) Fare clic su **J2C**. Viene aperta la pagina dell'alias di autenticazione.
   d) Creare un alias di autenticazione per l'origine dati:
      i) Fare clic su **Nuovo**.
      ii) Immettere i dettagli per **Alias**, **ID utente**, **Password**e **Descrizione**. I dettagli immessi nei campi **User ID** e **Password** devono corrispondere ai dettagli immessi quando è stato creato l'utente del database. Per ulteriori informazioni, fare riferimento a “Configurazione dell'accesso utente per il logger del database Java EE per MFT” a pagina 744.
      iii) Fare clic su **OK**.
   e) Creare un alias di autenticazione per IBM MQ:
      i) Fare clic su **Nuovo**.
      ii) Immettere i dettagli per **Alias**, **ID utente**, **Password**e **Descrizione**. i dettagli immessi nei campi **ID utente** e **Password** devono corrispondere alle impostazioni utente e password per l'installazione di IBM MQ .
      iii) Fare clic su **OK**.
3. Creare un'origine dati:
   a) Selezionare **Risorse** > **JDBC** > **Origini dati** dalla navigazione della console di gestione WebSphere Application Server 7.0 .
   b) Selezionare l'elenco a discesa **Ambito** e modificare l'ambito nel valore appropriato. Ad esempio, `Node=yourNode, Server=yourServer`.
   c) Creare un'origine dati utilizzando la procedura guidata della console, facendo clic su **Nuovo**.
   d) Al passo 1 della procedura guidata, nel campo **Nome origine dati** , immettere `wmqfte-database` e nel campo **Nome JNDI** , immettere `jdbc/wmqfte-database`. Fare clic su **Avanti**.
   e) Al passo 2 della procedura guidata, utilizzare l'elenco a discesa **Seleziona un provider JDBC** esistente per selezionare il provider JDBC creato nei passi precedenti. Fare clic su **Avanti**.
   f) **Db2:** Al passo 3 della procedura guidata, immettere 4nel campo **Tipo di driver** .
   g) **Db2:** immettere i dettagli nei campi **Nome database**, **Nome server**e **Numero porta** e fare clic su **Avanti**.

      Oracle: immettere l'URL di connessione nel campo **URL** e scegliere l'helper di archivio dati corretto nel campo **Nome classe helper archivio dati** .

Oracle RAC: quando ci si connette a un Oracle Real Application Cluster, l'URL di connessione deve includere le informazioni host necessarie per connettersi a tutte le istanze disponibili del database.

h) Al passo 4 della procedura guidata, selezionare il nome dell'alias di autenticazione dell'origine dati definito al passo 2d dall'elenco **Alias di autenticazione per il ripristino XA** . Selezionare lo stesso nome dagli elenchi **Alias di autenticazione gestito dal componente** e **Alias di autenticazione gestito dal contenitore** .

i) Fare clic su **Fine** nella pagina di riepilogo per creare l'origine dati.

4. Opzionale: Verificare la configurazione dell'origine dati:
   a) Selezionare **Risorse** > **JDBC** > **Origini dati** dalla navigazione della console di gestione WebSphere Application Server 7.0 .
   b) Fare clic su **Verifica connessione** .
5. Crea un argomento.
   a) Dalla navigazione nella console di amministrazione WebSphere Application Server 7.0 , fare clic su **Risorse** > **JMS** > **Argomenti**.
   b) Selezionare l'elenco a discesa **Ambito** e modificare l'ambito nel valore appropriato. Ad esempio, `Node=yourNode, Server=yourServer`.
   c) Fare clic su **Nuovo**.
   d) Fare clic sul provider di messaggistica **IBM MQ**.
   e) Sul pannello **Amministrazione** della pagina delle proprietà per l'argomento, scegliere valori univoci per i campi **Nome** e **Nome JNDI** , a cui si farà riferimento successivamente nella configurazione.
   f) Nel pannello **IBM MQ** , immettere `SYSTEM.FTE/Log/#` nel campo **Nome argomento** .
6. Creare una specifica di attivazione:
   a) Dalla navigazione della console di gestione WebSphere Application Server 7.0 , fare clic su **Risorse** > **JMS** > **Specifiche di attivazione**.
   b) Selezionare l'elenco a discesa **Ambito** e modificare l'ambito nel valore appropriato. Ad esempio, `Node=yourNode, Server=yourServer`.
   c) Fare clic su **Nuovo**.
   d) Fare clic sul provider di messaggistica **IBM MQ**.
   e) Nel passo 1 della procedura guidata, scegliere valori univoci per i campi **Nome** e **Nome JNDI** , a cui si farà nuovamente riferimento in seguito nella configurazione.
   f) Nel passo 1.1, immettere il nome JNDI per l'argomento impostato al punto 5 nel campo **Nome JNDI destinazione** .
   g) Dall'elenco **Tipo di destinazione** , selezionare **Argomento**.
   h) Nel passo 1.2 della procedura guidata, selezionare **Sottoscrizione durevole**. Immettere `SYSTEM.FTE.DATABASELOGGER.AUTO` nel campo **Nome sottoscrizione** .
   i) Nel passo 2 della procedura guidata, selezionare **Immettere tutte le informazioni richieste in questa procedura guidata**.
   j) Nel passo 2.1, immettere il nome del gestore code nel campo **Nome del gestore code o del gruppo di condivisione code** .
   k) Nel passo 2.2, selezionare il metodo di trasporto scelto dall'elenco **Trasporto** . Se si seleziona **Bind**, non sono richieste altre informazioni. Se si seleziona **Client** o **Bind, quindi client**, immettere i dettagli per **Nome host**, **Porta**e **Canale di connessione server**.
   l) Opzionale: Fare clic su **Verifica connessione** per verificare che il gestore code sia presente. Tuttavia, è possibile ricevere `NOT_AUTHORIZED` fino a quando non si fa riferimento all'alias di autenticazione nel passo 6n.
   m) Fare clic su **Salva**.

n) Fare clic sul nome della specifica di attivazione creata. Nella sezione **Proprietà generali** della scheda **Configurazione** , scorrere fino al pannello **Avanzate** e immettere un nome univoco per identificare la connessione IBM MQ nel campo **ID client** . È necessario completare questo passo o la propria connessione viene rifiutata da IBM MQ con il codice di errore `JMSCC0101` .

o) Se si sceglie **Client** come metodo di trasporto, scorrere fino al pannello **Impostazioni di sicurezza** e selezionare l'alias di autenticazione definito al passo 8 dall'elenco **Alias di autenticazione** .

p) Fare clic su **Applica**.

q) Nella sezione **Ulteriori proprietà** della scheda **Configurazione** , fare clic su **Proprietà avanzate**. Nella sezione **Consumatore connessione** del pannello **Proprietà avanzate** , immettere 1 nel campo **Numero massimo di sessioni server** .

Nota: Assicurarsi di completare questa operazione prima di proseguire. In caso contrario, il programma di registrazione potrebbe non funzionare correttamente.

r) Nella sezione **Ulteriori proprietà** della scheda **Configurazione** , fare clic su **Proprietà avanzate**. Impostare il valore di **Arresta endpoint se la consegna del messaggio non riesce** su un minimo di 1.

Se il valore della proprietà _numberOfFailedAttemptsBeforeReject è impostato su più di 1 (per ulteriori informazioni, vedere 9j), impostare **Arresta endpoint se la consegna del messaggio non riesce** almeno sul valore della proprietà _numberOfFailedAttemptsBeforeReject . Ciò impedisce all'endpoint di arrestarsi quando viene ricevuto un messaggio che non può essere elaborato (ad esempio, un messaggio di log di trasferimento non corretto). Per ulteriori informazioni, consultare MFT Gestione e rifiuto degli errori del programma di registrazione.

7. Creare un factory di connessione code.

a) Dalla navigazione della console di gestione WebSphere Application Server 7.0 , fare clic su **Risorse** > **JMS** > **Factory di connessione code**.

b) Selezionare l'elenco a discesa **Ambito** e modificare l'ambito nel valore appropriato. Ad esempio, `Node=yourNode, Server=yourServer`.

c) Fare clic su **Nuovo**.

d) Fare clic sul provider di messaggistica **IBM MQ**.

e) Nel passo 1 della procedura guidata, scegliere valori univoci per i campi **Nome** e **Nome JNDI** , a cui si farà nuovamente riferimento in seguito nella configurazione.

f) Nel passo 2, selezionare **Immettere tutte le informazioni richieste in questa procedura guidata**.

g) Nel passo 2.1, immettere il nome del gestore code nel campo **Nome del gestore code o del gruppo di condivisione code** .

h) Nel passo 2.2, selezionare il metodo di trasporto scelto dall'elenco **Trasporto** . Se si seleziona **Bind**, non sono richieste altre informazioni. Se si seleziona **Client** o **Bind, quindi client**, immettere i dettagli per **Nome host**, **Porta**e **Canale di connessione server**.

i) Opzionale: Fare clic su **Verifica connessione** per verificare che il gestore code sia presente. Tuttavia, è possibile ricevere `NOT_AUTHORIZED` fino a quando non si fa riferimento all'alias di autenticazione nel passaggio 7h.

j) Se è stato selezionato **Client** o **Bind e client** come metodo di trasporto, fare clic sul nome della factory di connessione code appena creata. Scorrere verso il basso il pannello **Impostazioni di protezione** della scheda **Configurazione** e selezionare l'alias di autenticazione definito nel passo 2e dagli elenchi **Alias di autenticazione per il ripristino XA** e **Alias di autenticazione gestito da contenitore** .

8. Creare una coda elementi respinti in WebSphere Application Server:

a) Dalla navigazione della console di gestione WebSphere Application Server 7.0 , fare clic su **Risorse** > **JMS** > **Code**.

b) Selezionare l'elenco a discesa **Ambito** e modificare l'ambito nel valore appropriato. Ad esempio, `Node=yourNode, Server=yourServer`.

c) Fare clic su **Nuovo**.

d) Fare clic sul provider di messaggistica **IBM MQ**.

e) Scegliere valori univoci per i campi **Nome** e **Nome JNDI** , a cui si farà nuovamente riferimento successivamente nella configurazione.

f) Immettere SYSTEM.FTE.LOG.RJCT.*logger_name* nel campo **Nome coda** . Assicurarsi di aver creato questa coda sul gestore code di coordinamento.

g) Immettere il proprio nome gestore code nel campo **Nome gestore code** .

h) Fare clic su **OK**.

9. Installare l'applicazione del programma di registrazione database JEE:

a) Dalla console di gestione WebSphere Application Server 7.0 , selezionare **Applicazioni** > **Nuova applicazione**.

b) Selezionare l'elenco a discesa **Ambito** e modificare l'ambito nel valore appropriato. Ad esempio, Node=yourNode, Server=yourServer.

c) Dall'elenco di opzioni, selezionare **Nuova applicazione enterprise**.

d) Nella pagina **Preparazione per l'installazione dell'applicazione** , selezionare il file com.ibm.wmqfte.databaselogger.jee.ear o il file com.ibm.wmqfte.databaselogger.jee.oracle.ear dalla directory *MQ_INSTALLATION_PATH*/mqft/web dell'installazione di Managed File Transfer Service e fare clic su **Avanti**.

e) Nella seguente schermata, selezionare **Dettagliato** per mostrare tutte le opzioni di installazione e i parametri e fare clic su **Avanti**.

f) Fare clic su **Avanti** attraverso i passi 1-4 della procedura guidata per accettare i valori predefiniti.

g) Nel passo 5 della procedura guidata, **Collegare i listener per i bean basati sui messaggi**, scorrere fino alla sezione **Collegamenti listener** . Fare clic su **Specifica di attivazione**.

Immettere i valori richiesti per i seguenti campi:

Nome JNDI della risorsa di destinazione
Il nome JNDI specificato durante la creazione di una specifica di attivazione nel passo 6d.

Nome JNDI di destinazione
Il nome JNDI specificato quando si crea un argomento nel passo 5d.

Fare clic su **Avanti**.

h) Nel passo 6 della procedura guidata, **Associa riferimenti risorsa alle risorse**, immettere i dettagli nel campo **Nome JNDI della risorsa di destinazione** . Questo nome è il nome JNDI specificato per il factory di connessione della coda di elementi respinti nel passaggio 7c. Fare clic su **Avanti**.

i) Nel passo 7 della procedura guidata, **Associa i riferimenti delle voci dell'ambiente delle risorse alle risorse**, immettere i dettagli nel campo **Nome JNDI risorsa di destinazione** . Questo è il nome JNDI della coda di elementi respinti creata nel passo 8d. Fare clic su **Avanti**.

j) Nel passo 8 della procedura guidata, **Associa voci di ambiente per i moduli EJB**, accettare il valore predefinito 1. Fare clic su **Avanti**.

Oracle RAC: quando ci si connette a Oracle Real Application Cluster, è necessario impostare il valore della proprietà _numberOfFailedAttemptsBeforeReject su **almeno** 2. Questa proprietà determina il numero di volte in cui il programma di registrazione tenta di elaborare un messaggio di controllo dopo un errore. In caso di failover del database, è probabile che si verifichi almeno un malfunzionamento. Per evitare di spostare inutilmente un messaggio nella coda di elementi respinti, l'aumento di questo valore consente di effettuare un secondo tentativo, che di solito ha esito positivo quando viene effettuata una connessione alla nuova istanza del database. Se durante il test si rileva che i messaggi vengono ancora spostati nella coda di elementi respinti durante il failover dell'istanza del database, aumentare ulteriormente questo valore: la tempistica del passaggio tra le istanze potrebbe causare più di un errore per lo stesso messaggio. Tuttavia, tenere presente che l'aumento di questo valore influisce su tutti i casi di errore (ad esempio, un messaggio in formato non corretto) e non solo sul failover del database, quindi aumentare il valore con attenzione per evitare tentativi non necessari.

k) Nel passo 9 della procedura guidata, **Metadata for modules**, fare clic su **Next**.

l) Nel passo 10 della procedura guidata, **Riepilogo**, fare clic su **Fine**.

10. È ora possibile avviare l'applicazione dalla console di gestione WebSphere Application Server 7.0 :

a) Selezionare **Applicazioni** > **Tipi di applicazioni** > **WebSphere WebSphere** dalla navigazione della console.

b) Selezionare la casella di controllo per l'applicazione enterprise **Logger** dalla tabella di raccolta e fare clic su **Avvia**.

Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server Community Edition

Seguire queste istruzioni per installare e configurare il programma di registrazione database Java Platform, Enterprise Edition (Java EE) per Managed File Transfer con WebSphere Application Server Community Edition.

Prima di iniziare

Prima di installare l'applicazione del programma di registrazione database Java EE , seguire le istruzioni nell'argomento “Preparazione all'installazione del programma di log del database Java EE per MFT” a pagina 733.

Informazioni su questa attività

Per ulteriori informazioni sul programma di registrazione database Java EE , consultare l'argomento “Configurazione di un programma di registrazione MFT” a pagina 719.

Procedura

1. Distribuire l'adattatore di risorse IBM MQ , `wmq.jmsra.rar`.

- Per distribuire l'adattatore di risorse IBM MQ per un programma di registrazione database Java EE utilizzando un gestore code di coordinamento QM_JUPITER, effettuare le seguenti operazioni. Questo esempio si applica quando l'istanza di WebSphere Application Server Community Edition è in esecuzione sullo stesso sistema del gestore code IBM MQ a cui si desidera connettersi.

a. Creare un file del piano che definisce una connessione al gestore code di coordinamento MFT . Il seguente file del piano di esempio definisce una connessione a un gestore code denominato QM_JUPITER e un riferimento a una coda denominata SYSTEM.FTE.LOG.RJCT.LOGGER1 su tale gestore code.

```
<?xml version="1.0" encoding="UTF-8"?>
<connector xmlns="http://geronimo.apache.org/xml/ns/j2ee/connector">
  <resourceadapter>
    <resourceadapter-instance>
      <resourceadapter-name>WMQ</resourceadapter-name>
      <workmanager>
        <gbean-link>DefaultWorkManager</gbean-link>
      </workmanager>
    </resourceadapter-instance>
    <outbound-resourceadapter>
      <connection-definition>
        <connectionfactory-interface>javax.jms.ConnectionFactory</connectionfactory-interface>
        <connectiondefinition-instance>
          <name>jms/WMQFTEJEEDBLoggerRejectQueueCF</name>
          <config-property-setting name="queueManager">QM_JUPITER</config-property-setting>
          <config-property-setting name="transportType">BINDINGS</config-property-setting>
          <connectionmanager>
            <xa-transaction>
              <transaction-caching/>
            </xa-transaction>
            <single-pool>
              <max-size>10</max-size>
              <min-size>1</min-size>
              <blocking-timeout-milliseconds>5000</blocking-timeout-milliseconds>
              <idle-timeout-minutes>2</idle-timeout-minutes>
              <match-all />
            </single-pool>
```

```
          </connectionmanager>
        </connectiondefinition-instance>
      </connection-definition>
    </outbound-resourceadapter>
  </resourceadapter>
  <adminobject>
    <adminobject-interface>javax.jms.Queue</adminobject-interface>
    <adminobject-class>com.ibm.mq.connector.outbound.MQQueueProxy</adminobject-class>
    <adminobject-instance>
      <message-destination-name>jms/WMQFTEJEEDBLoggerRejectQueue</message-destination-name>
      <config-property-setting name="baseQueueManagerName">QM_JUPITER</config-property-setting>
      <config-property-setting name="baseQueueName">SYSTEM.FTE.LOG.RJCT.LOGGER1</config-property-setting>
    </adminobject-instance>
  </adminobject>
</connector>
```

Per utilizzare questo file del piano nell'ambiente, modificare QM_JUPITER nel nome del gestore code di coordinamento.

b. Aprire la console di gestione WebSphere Application Server CE.

c. Dall'elenco **Azioni console comuni** nella **pagina di benvenuto**, fare clic su **Distribuisci nuove applicazioni** > **Distribuisci nuovo**.

d. Nel campo **Archivia** , immettere *mq_install_root*/java/lib/jca/wmq.jmsra.rar

e. Nel campo **Piano** , immettere il percorso del file del piano creato nel Passo 1a.

- Se l'istanza di WebSphere Application Server Community Edition è in esecuzione su un sistema differente rispetto al gestore code IBM MQ a cui si desidera connettersi, effettuare le seguenti operazioni per distribuire l'adattatore di risorse IBM MQ .

  a. Creare un file del piano che definisce una connessione al gestore code di coordinamento WMQFTE. Il seguente file del piano di esempio definisce una connessione a un gestore code, QM_SATURN, che si trova su un sistema differente per l'installazione di WebSphere Application Server Community Edition e un riferimento a una coda denominata SYSTEM.FTE.LOG.RJCT.LOGGER1 su tale gestore code. Il nome host di QM_SATURN è `saturn.example.com`. La porta di QM_SATURN è 1415. Il canale di QM_SATURN è SYSTEM.DEF.SVRCONN.

     Poiché il server delle applicazioni e il gestore code si trovano su sistemi differenti, è necessario utilizzare una connessione in modalità client al gestore code. Il seguente file del piano imposta il valore dell'elemento `<config-property-setting>` che ha il nome `transportType` su CLIENT.

```
<?xml version="1.0" encoding="UTF-8"?>
<connector xmlns="http://geronimo.apache.org/xml/ns/j2ee/connector">
  <resourceadapter>
    <resourceadapter-instance>
      <resourceadapter-name>WMQ</resourceadapter-name>
      <workmanager>
        <gbean-link>DefaultWorkManager</gbean-link>
      </workmanager>
    </resourceadapter-instance>
    <outbound-resourceadapter>
      <connection-definition>
        <connectionfactory-interface>javax.jms.ConnectionFactory</connectionfactory-interface>
        <connectiondefinition-instance>
          <name>jms/WMQFTEJEEDBLoggerRejectQueueCF</name>
          <config-property-setting name="queueManager">QM_SATURN</config-property-setting>
          <config-property-setting name="transportType">CLIENT</config-property-setting>
          <config-property-setting name="channel">SYSTEM.DEF.SVRCONN</config-property-setting>
          <config-property-setting name="hostName">saturn.example.com</config-property-setting>
          <config-property-setting name="port">1415</config-property-setting>
          <connectionmanager>
            <xa-transaction>
              <transaction-caching/>
            </xa-transaction>
            <single-pool>
              <max-size>10</max-size>
              <min-size>1</min-size>
              <blocking-timeout-milliseconds>5000</blocking-timeout-milliseconds>
              <idle-timeout-minutes>2</idle-timeout-minutes>
              <match-all />
            </single-pool>
```

```
          </connectionmanager>
        </connectiondefinition-instance>
      </connection-definition>
    </outbound-resourceadapter>
  </resourceadapter>
  <adminobject>
    <adminobject-interface>javax.jms.Queue</adminobject-interface>
    <adminobject-class>com.ibm.mq.connector.outbound.MQQueueProxy</adminobject-class>
    <adminobject-instance>
      <message-destination-name>jms/WMQFTEJEEDBLoggerRejectQueue</message-destination-name>
      <config-property-setting name="baseQueueManagerName">QM_SATURN</config-property-setting>
      <config-property-setting name="baseQueueName">SYSTEM.FTE.LOG.RJCT.LOGGER1</config-property-setting>
    </adminobject-instance>
  </adminobject>
</connector>
```

Per utilizzare questo file di piano nell'ambiente, modificare QM_SATURN nel nome del gestore code di coordinazione. Modificare il valore del nome host, della porta e del canale con i valori per il proprio gestore code di coordinamento.

b. Copiare il file *mq_install_root*/java/lib/jca/wmq.jmsra.rar dal sistema in cui è installato IBM MQ al sistema in cui è installato WebSphere Application Server CE.

c. Aprire la console di gestione WebSphere Application Server CE.

d. Dall'elenco **Azioni console comuni** nella **pagina di benvenuto**, fare clic su **Distribuisci nuove applicazioni** > **Distribuisci nuovo**.

e. Nel campo **Archivio** , immettere il percorso della copia del file wmq.jmsra.rar ottenuto.

f. Nel campo **Piano** , immettere il percorso del file del piano creato.

2. È necessario definire un connettore del database in modo che l'applicazione del programma di registrazione database Java EE abbia accesso al database richiesto dall'ambiente WebSphere Application Server Community Edition .

   Effettuare le operazioni riportate di seguito dalla console di amministrazione di WebSphere Application Server Community Edition :

   a) A seconda del livello di WebSphere Application Server Community Edition che si sta utilizzando, da **Navigazione console** , selezionare **Servizi** > **Pool di database**oppure selezionare **Risorse** > **Origini dati**.

   b) Creare un pool di database utilizzando la procedura guidata del pool di database Geronimo. Nel campo **Nome del pool di database** , immettere jdbc/wmqfte-database.

   c) Per il **tipo di database** , selezionare DB2 XA o Oracle Thin, come appropriato per il database.

   d) Fare clic su **Avanti**.

   e) Nel campo **jar driver** , selezionare il jar appropriato per il database.

   f) Nel campo **Nome database** , immettere il nome del database a cui ci si sta collegando per le informazioni sullo stato del trasferimento.

   g) Nel campo **Nome utente** , immettere il nome utente per la connessione e l'autenticazione con il database.

   h) Nei campi **Password** e **Conferma password** , immettere la password per l'autenticazione con il database.

   i) Nel campo **Numero di porta** , immettere il numero di porta che si sta utilizzando se non è la porta predefinita.

   j) Assicurarsi che il valore per **Tipo driver** sia 4.

   k) Selezionare XA dall'elenco **Tipo di transazione** .

   l) Fai clic su **Distribuisci**.

3. Aggiornare il file Managed File Transfer Java EE database logger application openejb-jar.xml per il proprio ambiente. Utilizzare un programma di utilità jar SDK Java per completare la seguente procedura:

   a) Estrarre il file jar EJB dal file EAR fornito eseguendo il seguente comando:

```
jar -xf ear_file_name com.ibm.wmqfte.databaselogger.jee.ejb.jar
```

dove *ear_file_name* è `com.ibm.wmqfte.databaselogger.jee.ear` o `com.ibm.wmqfte.databaselogger.jee.oracle.ear` a seconda se si utilizza Db2 o Oracle. Il file EAR si trova nella directory *MQ_INSTALLATION_PATH*`/mqft/web` dell'installazione del server IBM WebSphere MQ File Transfer Edition .

b) Estrarre il file `META-INF/openejb-jar.xml` dal file jar EJB precedentemente estratto, `com.ibm.wmqfte.databaselogger.jee.ejb.jar`, eseguendo il seguente comando:

```
jar -xf com.ibm.wmqfte.databaselogger.jee.ejb.jar META-INF/openejb-jar.xml
```

c) Utilizzare un editor di testo per modificare il file `META-INF/openejb-jar.xml` estratto. Modificare i seguenti valori `activation-config-property` in modo che corrispondano al proprio ambiente:

queueManager
Il nome del gestore code IBM MQ che viene utilizzato dal logger del database Java EE .

hostName
Il nome host da utilizzare per connettersi al gestore code IBM MQ specificato. Questo valore non è richiesto se ci si connette al gestore code in modalità bind.

transportType
Indica se connettersi al gestore code IBM MQ specificato in modalità client o bind.

porta
Non richiesto se è stato specificato un **`transportType`** di bind. La porta da utilizzare per connettersi al gestore code IBM MQ specificato.

canale
Non richiesto se è stato specificato un **`transportType`** di bind. Il canale del server da utilizzare per connettersi al gestore code IBM MQ specificato.

d) Aggiornare il file jar EJB con il file `META-INF/openejb-jar.xml` modificato, eseguendo il seguente comando:

```
jar -uf com.ibm.wmqfte.databaselogger.jee.ejb.jar META-INF/openejb-jar.xml
```

e) Aggiornare il file ear fornito con il file jar EJB aggiornato, eseguendo il comando riportato di seguito:

```
jar -uf ear_file_name com.ibm.wmqfte.databaselogger.jee.ejb.jar
```

dove *ear_file_name* è `com.ibm.wmqfte.databaselogger.jee.ear` o `com.ibm.wmqfte.databaselogger.jee.oracle.ear` a seconda del database.

4. Per distribuire il file EAR al server delle applicazioni, completare la seguente procedura dalla console di amministrazione di WebSphere Application Server Community Edition .
   a) Selezionare: **Applicazioni** > **Distribuisci nuovo** dal menu **Navigazione console** .
   b) Nel campo **Archivio** , specificare il file EAR: `com.ibm.wmqfte.databaselogger.jee.ear` o `com.ibm.wmqfte.databaselogger.jee.oracle.ear` in base al proprio database.
   c) Lasciare vuoto il campo **Piano** .
   d) Assicurarsi che la casella **Avvia applicazione dopo l'installazione** sia selezionata.
   e) Fai clic su **Installa**. L'applicazione del programma di registrazione database JEE è installata e avviata.

Configurazione dell'accesso utente per il logger del database Java EE per MFT

Quando si configura il programma di registrazione database Java Platform, Enterprise Edition (Java EE) per Managed File Transfer, sono necessari gli account utente per accedere a IBM MQ, al database e

al sistema operativo. Il numero di utenti del sistema operativo richiesto dipende dal numero di sistemi utilizzati per ospitare questi componenti.

Informazioni su questa attività

Il numero e il tipo di account utente necessari per eseguire il programma di registrazione database Java EE dipende dal numero di sistemi utilizzati. Gli account utente sono necessari per accedere ai seguenti tre ambienti:

- Sistema operativo locale
- IBM MQ
- Database

È possibile installare il programma di registrazione database JEE, IBM MQ e il proprio database su un singolo sistema o su più sistemi. I componenti possono essere installati nelle seguenti topologie di esempio:

Java EE database logger, IBM MQ, e il database tutti sullo stesso sistema
: È possibile definire un singolo utente del sistema operativo da utilizzare con tutti e tre i componenti. Il programma di registrazione utilizza la modalità Bindings per connettersi a IBM MQ e una connessione nativa per connettersi al database.

Java EE programma di registrazione database e IBM MQ su un sistema, il database su un sistema separato
: Si creano due utenti per questa configurazione: un utente del sistema operativo sul sistema che esegue il programma di registrazione e un utente del sistema operativo con accesso remoto al database sul server database. Il programma di registrazione utilizza la modalità Bindings per connettersi a IBM MQ e una connessione client per accedere al database.

Java EE programma di registrazione database su un sistema, IBM MQ su un altro sistema, il database su un altro sistema
: Si creano tre utenti per questa configurazione: un utente del sistema operativo per avviare il server delle applicazioni, un utente IBM MQ per accedere alle code e agli argomenti utilizzati e un utente del server di database per accedere e inserire nelle tabelle del database. Il programma di registrazione utilizza la modalità Client per accedere a IBM MQ e una connessione client per accedere al database.

Come esempio, il resto di queste istruzioni presuppone che l'utente sia denominato `ftelog`, ma è possibile utilizzare qualsiasi nome utente, nuovo o esistente. Configurare le autorizzazioni utente come segue:

Procedura

1. Verificare che l'utente del sistema operativo disponga di un proprio gruppo e che non appartenga ad alcun gruppo con ampie autorizzazioni sul gestore code di coordinamento. L'utente non deve essere nel gruppo mqm. Su alcune piattaforme, al gruppo di staff viene automaticamente fornito l'accesso al gestore code; l'utente del programma di registrazione non deve far parte del gruppo di staff. È possibile visualizzare i record di autorizzazioni per il gestore code stesso e per gli oggetti in esso contenuti utilizzando IBM MQ Explorer. Fare clic con il pulsante destro del mouse sull'oggetto e selezionare **Autorizzazioni oggetto> Gestisci record di autorizzazione**. Nella riga di comando, è possibile utilizzare i comandi dspmqaut (visualizza autorità) o dmpmqaut (dump autorità).
2. Utilizzare la finestra **Gestisci record di autorizzazioni** in IBM MQ Explorer o il comando setmqaut (concessione o revoca dell'autorità) per aggiungere autorizzazioni per il proprio gruppo di utenti IBM MQ (in UNIX, IBM MQ le autorizzazioni sono associate solo a gruppi, non a singoli utenti). Le autorità richieste sono le seguenti:
   - CONNECT e INQUIRE sul gestore code (le librerie IBM MQ Java richiedono l'autorizzazione INQUIRE per funzionare).
   - Autorizzazione SUBSCRIBE su SYSTEM.FTE .
   - Autorizzazione PUT su SYSTEM.FTE.LOG.RJCT.*nome_programma di registrazione* .

I nomi delle code di comando e di rifiuto forniti sono i nomi predefiniti. Se sono stati scelti nomi di coda differenti quando sono state configurate le code del programma di registrazione, aggiungere le autorizzazioni a tali nomi di coda.

3. Eseguire la configurazione dell'utente del database specifica per il database che si sta utilizzando.
   - Se il database è Db2, effettuare le seguenti operazioni:

     Nota: Esistono diversi meccanismi per la gestione degli utenti del database con Db2. Queste istruzioni si applicano allo schema predefinito in base agli utenti del sistema operativo.

     – Assicurarsi che l'utente `ftelog` non si trovi in alcun gruppo di gestione Db2 (ad esempio, db2iadm1, db2fadm1o dasadm1).
     – Fornire all'utente l'autorizzazione per la connessione al database e l'autorizzazione per selezionare, inserire e aggiornare le tabelle create come parte del Passo 2: creare le tabelle di database richieste.
   - Se il database è Oracle, effettuare le seguenti operazioni:
     – Assicurarsi che l'utente `ftelog` non sia in alcun gruppo di amministrazione Oracle (ad esempio, ora_dba su Windows o dba su UNIX).
     – Fornire all'utente l'autorizzazione a collegarsi al database e l'autorizzazione a selezionare, inserire e aggiornare le tabelle create come parte del Passo 2: creare le tabelle di database richieste.

Migrazione di un programma di registrazione database Java EE

Per migrare un programma di registrazione database Java EE su WebSphere Application Server 7.0 da IBM WebSphere MQ File Transfer Edition 7.0 a IBM WebSphere MQ 7.5 o successivo, completare la seguente procedura:

Procedura

1. Aprire la console di WebSphere Application Server.
2. Fare clic su **Applicazioni** > **Tipi di applicazione** > **Applicazioni enterprise**. Individuare l'applicazione del programma di registrazione database IBM WebSphere MQ File Transfer Edition nell'elenco di applicazioni. Se l'applicazione del programma di registrazione database non è già stata arrestata, selezionare l'applicazione e fare clic su **Arresta**.
3. Prendere nota delle impostazioni di configurazione precedentemente configurate per il programma di registrazione database JEE. Queste saranno necessarie più avanti nel passo “7” a pagina 747.
   a) Se in origine sono state apportate modifiche dalle impostazioni predefinite per i moduli EJB durante l'installazione del programma di registrazione database (per ulteriori informazioni, fare riferimento al passo 9), fare clic su **Applicazioni enterprise** > **WebSphere MQ File Transfer Edition** > **Voci di ambiente per moduli EJB** e prendere nota delle impostazioni nel riquadro.
   b) Fare clic su **Applicazioni enterprise** > **WebSphere MQ File Transfer Edition** > **Bind del listener Message Driven Bean** e prendere nota della specifica di attivazione utilizzata, del **Nome JNDI della risorsa di destinazione** e del **Nome JNDI di destinazione**.
   c) Fare clic su **Applicazioni enterprise** > **WebSphere MQ File Transfer Edition** > **Riferimenti risorse** e prendere nota dei dettagli della produzione connessioni code rifiutate.
   d) Fare clic su **Applicazioni enterprise** > **WebSphere MQ File Transfer Edition** > **Riferimenti voce ambiente di risorse** e prendere nota dei dettagli della coda di elementi respinti.
4. Disinstallare l'applicazione del programma di registrazione database IBM WebSphere MQ File Transfer Edition facendo clic su **Applicazioni** > **Tipi di applicazioni** > **Applicazioni enterprise**. Selezionare l'applicazione del programma di registrazione database e fare clic su **Disinstalla**.
5. Facoltativo: se si stanno utilizzando più installazioni per migrare a IBM WebSphere MQ 7.5o versioni successive e il percorso della libreria nativa è diverso, modificare il percorso facendo clic su **Risorse** > **Provider JMS** > **WebSphere MQ**

Ad esempio, se il percorso della libreria nativa era: `C:\Program Files\IBM\WebSphere MQ\java\lib`, modificare il percorso in: `C:\Program Files\IBM\`*`New MQ Installation Location`*`\java\lib`

6. Facoltativo: se si utilizzano più installazioni per migrare a IBM WebSphere MQ 7.5 o versioni successive, è necessario associare il gestore code alla nuova installazione utilizzando il comando setmqm.
7. Reinstallare l'applicazione del programma di registrazione database utilizzando le informazioni in “Installazione del programma di registrazione database Java EE per MFT con WebSphere Application Server 7.0” a pagina 736 e le informazioni registrate in precedenza nel passo “3” a pagina 746.
8. Avviare il nuovo programma di registrazione database facendo clic su **Applicazioni** > **Tipi di applicazioni** > **Applicazioni enterprise**. Selezionare l'applicazione del programma di registrazione database e fare clic su **Avvia**.
9. Per verificare la migrazione, controllare il database per assicurarsi che le voci vengano scritte.

Migrazione dal programma di registrazione database autonomo al programma di registrazione database di Java EE per MFT

È possibile eseguire la migrazione dal programma di registrazione database autonomo al programma di registrazione database Java EE . È necessario arrestare il programma di registrazione database autonomo e installare il programma di registrazione database JEE. Per evitare la perdita o la duplicazione delle voci di log, è necessario arrestare la pubblicazione dei messaggi nel sistema SYSTEM.FTE prima di arrestare il programma di registrazione database autonomo e riavviarlo dopo aver installato il programma di registrazione database Java EE . Eseguire il backup del database prima della migrazione.

Informazioni su questa attività

Procedura

1. Prima di interrompere il database, eseguire questo comando MQSC rispetto al proprio gestore code di coordinamento: `ALTER QM PSMODE(COMPAT)`

   Questo arresta la pubblicazione dei messaggi nel SISTEMA SYSTEM.FTE/Log . Attendere che il programma di registrazione abbia elaborato tutti i messaggi sulla relativa sottoscrizione. Per impostazione predefinita, questa sottoscrizione è denominata SYSTEM.FTE.LOGGER.AUTOAUTO.
2. Arrestare il programma di registrazione database utilizzando il comando **`fteStopLogger`** .
3. Eseguire il backup del database utilizzando gli strumenti forniti con il software del database.
4. Eliminare la sottoscrizione appartenente al programma di registrazione database autonomo.

   Per impostazione predefinita, questa sottoscrizione è denominata SYSTEM.FTE.LOGGER.AUTOAUTO.
5. Se lo schema del database è una versione precedente, è necessario migrare lo schema a ciascun livello successivo in ordine. Ad esempio, se lo schema del database è V7.0.1 e si sta eseguendo la migrazione a V7.0.4, è necessario migrare lo schema da V7.0.1 a V7.0.2, quindi da V7.0.2 a V7.0.3e quindi da V7.0.3 a V7.0.4. Migrare lo schema del database dalla versione *`old`* alla versione *new*, dove *`old`* e *new* sono le variabili che descrivono una versione dello schema, eseguendo una delle seguenti azioni per ciascuna versione dello schema da migrare:

   - z/OS Se il database è Db2 su z/OS e si sta eseguendo la migrazione tra schemi V7.0.2 e V7.0.3 o tra schemi V7.0.3 e V7.0.4 , è necessario creare un nuovo schema di database e copiare i dati esistenti in esso. Per ulteriori informazioni, consultare Migrating the database tables on Db2 on z/OS to MQ V8.0 or later.
   - Se il tuo database non è Db2 o hai creato il tuo database con una dimensione di pagina superiore a 8K, puoi migrare lo schema nello stesso modo come per le altre versioni, completando la seguente procedura.
   - Se si sta eseguendo la migrazione tra le tabelle del database in altre circostanze, completare la seguente procedura:

a. Scegliere il file appropriato per la piattaforma del database e che abbia un nome che includa la stringa *old-new*. Questo file si trova nella directory *MQ_INSTALLATION_PATH*/mqft/sql dell'installazione di Strumenti remoti e Documentation .

b. Se sono state apportate modifiche allo schema iniziale, esaminare il file di migrazione per assicurarsi che sia compatibile con il database modificato.

c. Eseguire il file SQL sul proprio database.

6. Installare il file EAR del programma di registrazione database Java EE .
7. Distribuire il programma di registrazione del database Java EE . Per ulteriori informazioni, consultare “Installazione del programma di registrazione database Java EE per MFT” a pagina 732.
8. Eseguire il seguente comando MQSC rispetto al gestore code di coordinamento: `ALTER QMGR PSMODE(ENABLED)`

   Ciò consente la pubblicazione dei messaggi nel SISTEMA SYSTEM.FTE/Log .

Risultati

Configurazione del bridge Connect:Direct

Configurare il bridge Connect:Direct per trasferire i file tra una rete Managed File Transfer e una rete Connect:Direct . I componenti del bridge Connect:Direct sono un nodo Connect:Direct e un agent Managed File Transfer dedicati alla comunicazione con tale nodo. A questo agent si fa riferimento come agent bridge Connect:Direct .

Prima di iniziare

L'agent e il nodo che costituiscono il bridge Connect:Direct devono essere sullo stesso sistema o avere accesso allo stesso file system, ad esempio tramite un montaggio NFS condiviso. Questo file system viene utilizzato per memorizzare temporaneamente i file durante i trasferimenti di file che coinvolgono il bridge Connect:Direct, in una directory definita dal parametro **cdTmpDir**. L'agent bridge Connect:Direct e il nodo bridge Connect:Direct devono essere in grado di raggiungere questa directory utilizzando lo stesso nome percorso. Ad esempio, se l'agent e il nodo si trovano su sistemi Windows separati, i sistemi devono utilizzare la stessa lettera di unità per il montaggio del file system condiviso. Le seguenti configurazioni consentono all'agent e al nodo di utilizzare lo stesso nome percorso:

- L'agent e il nodo si trovano sullo stesso sistema, che è in esecuzione in Windows o Linux per x86-64
- L'agent si trova su Linux per x86-64 e il nodo è su UNIX
- L'agent si trova su un sistema Windows e il nodo si trova su un altro sistema Windows

Le seguenti configurazioni non consentono all'agent e al nodo di utilizzare lo stesso nome percorso:

- L'agent si trova su Linux per x86-64 e il nodo è su Windows
- L'agent si trova su Windows e il nodo su UNIX

Considerare questa limitazione quando si pianifica l'installazione del bridge Connect:Direct.

Per ulteriori dettagli sulle versioni del sistema operativo supportate per il bridge Connect:Direct , consultare la pagina Web Requisiti di sistema per IBM MQ.

Informazioni su questa attività

Un agent bridge Connect:Direct è un agent Managed File Transfer dedicato alla comunicazione con un nodo Connect:Direct .

Per impostazione predefinita, l'agent bridge Connect:Direct utilizza il protocollo TCP / IP per connettersi al nodo Connect:Direct . Se si desidera una connessione sicura tra l'agent bridge Connect:Direct e il nodo Connect:Direct , è possibile utilizzare il protocollo SSL o il protocollo TLS.

Procedura

1. Scegliere i sistemi operativi per il nodo e l'agent bridge Connect:Direct :
   a) Scegliere un sistema su cui è in esecuzione Windows o Linux su x86-64 su cui installare l'agent bridge Connect:Direct .
   b) Scegliere un sistema operativo supportato da Connect:Direct per Windows o Connect:Direct per UNIX su cui installare il nodo bridge Connect:Direct .
2. Scegliere e configurare un nodo Connect:Direct :
   È necessario avere un nodo Connect:Direct installato prima di seguire queste istruzioni.
   a) Scegliere un nodo Connect:Direct con cui comunicare con l'agent Managed File Transfer .
   b) Controllare la mappa di rete per il nodo Connect:Direct scelto. Se la mappa di rete contiene voci per i nodi remoti in esecuzione su un sistema operativo Windows , è necessario assicurarsi che tali voci specifichino che i nodi sono in esecuzione su Windows.

      Windows Se il nodo Connect:Direct selezionato per il bridge Connect:Direct è in esecuzione su Windows, utilizzare Connect:Direct Requester per modificare la mappa di rete. Assicurarsi che il campo **Sistema operativo** per tutti i nodi remoti in esecuzione su Windows sia impostato su **Windows**.
3. Creare e configurare un agent bridge Connect:Direct :
   a) Creare un agent bridge Connect:Direct utilizzando il comando **fteCreateCDAgent** .
      - È necessario fornire un valore per il parametro **cdNode** . Questo parametro specifica il nome utilizzato dall'agent per il nodo Connect:Direct che fa parte del bridge Connect:Direct . Utilizzare il nome del nodo Connect:Direct scelto nella sezione precedente.
      - Fornire i parametri **cdNodeHost** e **cdNodePort** , che definiscono il nodo Connect:Direct con cui comunica l'agent.

        Se non si fornisce un valore per il parametro **cdNodeHost** , viene utilizzato il nome host o l'indirizzo IP del sistema locale. Se non si fornisce un valore per il parametro **cdNodePort** , viene utilizzato il valore 1363 .
      - Facoltativamente, utilizzare le informazioni in fteCreateAgent per stabilire se è necessario specificare un valore per il parametro **cdTmpDir** .
   b) Associare le credenziali utente utilizzate da Managed File Transfer alle credenziali utente su un nodo Connect:Direct . È possibile associare le credenziali utilizzando uno dei seguenti metodi:
      - Creare un file `ConnectDirectCredentials.xml` per definire le informazioni di associazione credenziali. Per ulteriori informazioni, consultare “Associazione delle credenziali per Connect:Direct utilizzando il file ConnectDirectCredentials.xml” a pagina 750.
      - Scrivere un'uscita utente per eseguire l'associazione credenziali per il bridge Connect:Direct . Per ulteriori informazioni, consultare “Associazione delle credenziali per Connect:Direct utilizzando le classi di uscita” a pagina 752.
4. Configurare il file `ConnectDirectNodeProperties.xml` per includere le informazioni sui nodi Connect:Direct remoti:
   È necessario aver creato un agent bridge Connect:Direct prima di seguire queste istruzioni.
   Modificare il modello `ConnectDirectNodeProperties.xml` nella directory di configurazione dell'agente bridge Connect:Direct . Per ogni nodo o gruppo di nodi Connect:Direct di cui si desidera definire le informazioni, effettuare le seguenti operazioni:
   a) All'interno dell'elemento nodeProperties , creare un elemento node .
   b) Aggiungere un attributo name all'elemento node . Specificare il valore di questo attributo come un modello che corrisponda al nome di uno o più nodi Connect:Direct remoti.
   c) Opzionale: Aggiungere un attributo pattern all'elemento node che specifica quale tipo di pattern è il valore nell'attributo name . I valori validi sono `regex` e `wildcard`. L'opzione predefinita è `wildcard`.

d) Aggiungere un attributo type all'elemento node che specifica il sistema operativo su cui vengono eseguiti i nodi Connect:Direct remoti specificati dall'attributo name .

I valori validi sono:

- `Windows` - il nodo viene eseguito su Windows
- `UNIX` - il nodo viene eseguito su UNIX o Linux
- 

`z/OS`, `zos`, `os/390`o `os390` - il nodo viene eseguito su z/OS

Il valore di questo attributo non è sensibile al maiuscolo / minuscolo. I trasferimenti ai nodi remoti che si trovano su altri sistemi operativi non sono supportati dal bridge Connect:Direct.

5. Configurare una connessione protetta tra l'agent bridge Connect:Direct e il nodo Connect:Direct .

   Per un esempio di come eseguire questa operazione, consultare Configurazione di SSL o TLS tra l'agent bridge Connect:Direct e il nodo Connect:Direct.

Associazione delle credenziali per Connect:Direct

Associare le credenziali utente in Managed File Transfer con le credenziali utente su un nodo Connect:Direct utilizzando la funzione di associazione credenziali predefinita dell'agent bridge Connect:Direct o scrivendo la propria uscita utente. Managed File Transfer fornisce un'uscita utente di esempio che esegue l'associazione delle credenziali utente.

Associazione delle credenziali per Connect:Direct utilizzando il file ConnectDirectCredentials.xml

Associare le credenziali utente in Managed File Transfer alle credenziali utente sui nodi Connect:Direct utilizzando la funzione di associazione credenziali predefinita dell'agent bridge Connect:Direct . Managed File Transfer fornisce un file XML che è possibile modificare per includere le informazioni sulle credenziali.

Informazioni su questa attività

Dopo che un agent bridge Connect:Direct è stato creato utilizzando il comando **fteCreateCDAgent** , è necessario creare manualmente un file `ConnectDirectCredentials.xml` . Prima di poter utilizzare un agent bridge Connect:Direct , è necessario modificare questo file per includere le informazioni su host, utente e credenziali. Per ulteriori informazioni, vedi Formato del file delle credenzialiConnect:Direct. Per impostazione predefinita, questo file viene caricato dalla directory home dell'utente corrente, ad esempio `/home/fteuser/ConnectDirectCredentials.xml` . Per utilizzare un'altra posizione, specificarla utilizzando l'elemento `<credentialsFile>` nel file `ConnectDirectNodeProperties.xml` .

Procedura

1. Verificare che l'attributo `name` nell'elemento `<tns:pnode name="Connect:Direct node host" pattern="wildcard">` contenga il valore del nome del nodo Connect:Direct a cui si connette l'agent bridge Connect:Direct . Questo valore deve essere lo stesso valore specificato per il parametro **fteCreateCDAgent -cdNode** .

   Il valore dell'attributo `pattern` può essere `wildcard` o `regex`. Se questo attributo non viene specificato, il valore predefinito è `wildcard`.

2. Inserire le informazioni sulle credenziali e sull'ID utente nel file come elementi child di `<tns:pnode>`.

   È possibile inserire una o più istanze del seguente elemento `<tns:user>` nel file:

```
<tns:user name="name"
          pattern="pattern"
          ignorecase="ignorecase"
          cdUserId="cdUserId"
          cdPassword="cdPassword"
          pnodeUserId="pnodeUserId"
          pnodePassword="pnodePassword">
</tns:user>
```

dove:

- *name* è un modello che corrisponde all'ID utente MQMD associato alla richiesta di trasferimento MFT .
- *pattern* specifica se il modello specificato per l'attributo name è un'espressione jolly o un'espressione regolare Java . Il valore dell'attributo pattern può essere wildcard o regex. Se questo attributo non viene specificato, il valore predefinito è wildcard.
- *ignorecase* specifica se considerare il modello specificato dall'attributo name come sensibile al maiuscolo / minuscolo. Se questo attributo non viene specificato, il valore predefinito è true.
- *cdUserId* è l'ID utente utilizzato dall'agent bridge Connect:Direct per connettersi al nodo Connect:Direct specificato dall'elemento name di <tns:pnode> . Se possibile, assicurarsi che *cdUserId* sia un ID utente amministratore Connect:Direct . Se *cdUserId* non può essere un amministratore Connect:Direct , assicurarsi che l'ID utente disponga delle seguenti autorizzazioni funzionali sul nodo bridge Connect:Direct :

  – Per un nodo Windows impostare le seguenti autorizzazioni. Questo esempio è formattato con ritorni a capo per facilitare la leggibilità:

```
View Processes in the  value: yes
 TCQ
Issue the copy         value: yes
 receive, copy send,
 run job, and run task
 Process statements
Issue the submit       value: yes
 Process statement
Monitor, submit,       value: all
 change,and delete all
 Processes
Access Process         value: all
 statistics
Use the trace tool or  value: yes
 issue traceon and
 traceoff commands
Override Process       value: yes
 options such as file
 attributes and remote
 node ID
```

  – Per un nodo UNIX impostare i parametri seguenti nel file userfile.cfg :

```
pstmt.copy             value: y
pstmt.upload           value: y
pstmt.download         value: y
pstmt.runjob           value: y
pstmt.runtask          value: y
cmd.submit             value: y
pstmt.submit           value: y
cmd.chgproc            value: y
cmd.delproc            value: y
cmd.flsproc            value: y
cmd.selproc            value: a
cmd.selstats           value: a
cmd.trace              value: y
snode.ovrd             value: y
```

- *cdPassword* è la password associata all'ID utente specificato dall'attributo cdUserId .
- Facoltativamente, è possibile specificare l'attributo pnodeUserId . Il valore di questo attributo è l'ID utente utilizzato dal nodo Connect:Direct specificato dall'attributo name dell'elemento <tns:pnode> per inoltrare il processo Connect:Direct . Se non si specifica l'attributo pnodeUserId , il nodo Connect:Direct utilizza l'ID utente specificato dall'attributo cdUserId per inoltrare il processo Connect:Direct .
- Facoltativamente, è possibile specificare l'attributo pnodePassword. Il valore di questo attributo è la parola d'ordine associata all'id utente specificato dall'attributo pnodeUserId .

Se nessun elemento utente corrisponde all'ID utente MQMD, il trasferimento ha esito negativo.

3. Opzionale: È possibile includere uno o più elementi <tns:snode> come elementi child dell'elemento <tns:user> . L'elemento <tns:snode> specifica le credenziali utilizzate dal nodo Connect:Direct che fa parte del bridge Connect:Direct . Queste credenziali sono l'ID utente e la password che il nodo bridge Connect:Direct utilizza per connettersi al nodo Connect:Direct che è l'origine o la destinazione del trasferimento file.

   Inserire uno o più dei seguenti elementi nel file:

```
<tns:snode name="name"
           pattern="pattern"
           userId="userId"
           password="password"/>
```

   dove:

   - *name* è un modello che corrisponde al nome del nodo Connect:Direct che è l'origine o la destinazione del trasferimento file.
   - *pattern* specifica se il modello specificato per l'attributo name è un'espressione jolly o un'espressione regolare Java . Il valore dell'attributo pattern può essere wildcard o regex. Se questo attributo non viene specificato, il valore predefinito è wildcard.
   - *userId* è l'ID utente utilizzato dal nodo Connect:Direct specificato dall'attributo name dell'elemento <tns:pnode> per connettersi a un nodo Connect:Direct che corrisponde al modello specificato dall'attributo name di <tns:snode>.
   - *password* è la password associata all'ID utente specificato dall'attributo userId .

   Se nessun elemento <tns:snode> corrisponde al nodo secondario del trasferimento file, il trasferimento non avrà esito negativo. Il trasferimento è stato avviato e non è stato specificato alcun ID utente e password da utilizzare con snode.

Risultati

Durante la ricerca di una corrispondenza di modello per i nomi utente o i nomi nodo Connect:Direct , l'agent bridge Connect:Direct esegue la ricerca dall'inizio del file alla fine del file. La prima corrispondenza trovata è quella utilizzata.

Attività correlate

“Configurazione del bridge Connect:Direct” a pagina 748

Configurare il bridge Connect:Direct per trasferire i file tra una rete Managed File Transfer e una rete Connect:Direct . I componenti del bridge Connect:Direct sono un nodo Connect:Direct e un agent Managed File Transfer dedicati alla comunicazione con tale nodo. A questo agent si fa riferimento come agent bridge Connect:Direct .

Riferimenti correlati

Formato file delle credenziali Connect:Direct

fteCreateCDAgent: crea un agent bridge Connect:Direct

Associazione delle credenziali per Connect:Direct utilizzando le classi di uscita

Se non si desidera utilizzare la funzione di associazione credenziali predefinita dell'agent bridge Connect:Direct , è possibile associare le credenziali utente in Managed File Transfer alle credenziali utente su un nodo Connect:Direct scrivendo la propria uscita utente. La configurazione delle proprie uscite utente di associazione credenziali disabilita la funzione di associazione credenziali predefinita.

Informazioni su questa attività

Le uscite utente create per associare le credenziali Connect:Direct devono implementare l'interfaccia com.ibm.wmqfte.exitroutine.api.ConnectDirectCredentialExit. Per ulteriori informazioni, vedi CDCredentialExit.java interface.

Windows Configurazione degli agenti MFT con MSCS

L'impostazione Managed File Transfer (MFT) agent Microsoft Cluster Service (MSCS) è supportata, se la piattaforma è una supportata da MFT ed esegue una delle versioni di Windows.

Informazioni su questa attività

Questa attività descrive due scenari che possono essere seguiti per ottenere il failover di un agent MFT :

- Scenario 1: configurazione dell'agent come risorsa MSCS.
- Scenario 2: configurazione del gestore code dell'agent e dell'agent come risorse MSCS.

Procedura

Scenario 1: configurazione dell'agent come risorsa MSCS

- Per configurare l'agent come risorsa MSCS, completare la seguente procedura:
  a) Installare Managed File Transfer localmente su ogni macchina nel cluster.

     Consultare Installazione di Managed File Transfer.

  b) Creare l'agente sulla macchina primaria nel cluster.

     L'agente deve essere configurato per connettersi al gestore code dell'agente utilizzando il trasporto CLIENT. Assicurarsi di creare tutti gli oggetti sul gestore code per questo agente. Per informazioni su come eseguire questa operazione, consultare Impostazione dell'agente.

  c) Modificare l'agent in modo che venga eseguito come servizio Windows e configurarlo in modo che non venga avviato automaticamente quando Windows viene riavviato impostando il campo **Tipo di avvio** per il servizio agent nello strumento Windows Servizi su `Manuale`.

     Per ulteriori informazioni, vedi Avvio di un agent MFT come servizio Windows.

  d) Ripetere il passo “2” a pagina 753 e il passo “3” a pagina 753 dello scenario 1 sulla macchina secondaria.

     Ciò garantisce che la struttura del file per i log, le proprietà e così via, esista sull'altra macchina nel cluster. Notare che non è necessario creare gli oggetti del gestore code come nel passo “2” a pagina 753.

  e) Sulla macchina primaria, aggiungere l'agent come 'Servizio generico ' sotto il controllo di MSCS.

     Per far ciò:

     a. Fare clic con il pulsante destro del mouse e selezionare **Ruolo -> Aggiungi risorsa -> 'Servizio generico'**.
     b. Dall'elenco dei servizi Windows , selezionare il servizio agent e completare la procedura guidata di configurazione facendo clic su **Avanti**.

     Il servizio agent è ora aggiunto come risorsa MSCS. Se si verifica un failover, il servizio agent verrà avviato sull'altra macchina.

Scenario 2: configurazione del gestore code dell'agent e dell'agent come risorse MSCS

- Per configurare il gestore code dell'agent e l'agent come risorse MSCS, completare la seguente procedura:
  a) Configurare il gestore code dell'agente da eseguire come risorsa MSCS.

     Per informazioni su come svolgere questa procedura, consultare “Inserimento di un gestore code sotto il controllo di MSCS” a pagina 463.

  b) Creare l'agente sulla macchina primaria nel cluster.

     L'agent deve essere configurato per connettersi al gestore code dell'agent utilizzando il trasporto BINDINGS. Assicurarsi di creare tutti gli oggetti sul gestore code per questo agente. Per informazioni su come eseguire questa operazione, consultare Impostazione dell'agente.

  c) Modificare l'agent in modo che venga eseguito come servizio Windows e configurarlo in modo che non venga avviato automaticamente quando Windows viene riavviato impostando il campo **Tipo di avvio** per il servizio agent nello strumento Windows Servizi su `Manuale`.

Per ulteriori informazioni, vedi Avvio di un agent MFT come servizio Windows.

d) Controllare che il gestore code dell'agent (sotto il controllo MSCS) sia in esecuzione sulla macchina secondaria.

   L'agent creato su questa macchina si connetterà al gestore code utilizzando il trasporto BINDINGS, pertanto deve essere disponibile quando l'agent viene creato.

e) Ripetere il passo “2” a pagina 753 e il passo “3” a pagina 753 dello scenario 2 sulla macchina secondaria.

   Ciò garantisce che la struttura del file per i log, le proprietà e così via, esista sull'altra macchina nel cluster. Notare che non è necessario creare gli oggetti del gestore code come nel passo “2” a pagina 753.

f) Aggiungere l'agent come 'Servizio generico ' nel controllo MSCS.

   Per far ciò:

   a. Fare clic con il pulsante destro del mouse e selezionare **Ruolo -> Aggiungi risorsa -> 'Servizio generico'**.

   b. Dall'elenco dei servizi Windows , selezionare il servizio agent e completare la procedura guidata di configurazione facendo clic su **Avanti**.

g) Modificare le proprietà della risorsa del servizio agent per aggiungere la risorsa del gestore code nell'elenco delle dipendenze.

   Ciò garantisce che la risorsa del gestore code venga avviata prima dell'avvio dell'agente.

h) Portare la risorsa del gestore code non in linea, quindi portare la risorsa agent in linea. Verificare se sia la risorsa del gestore code che l'agent sono avviati.

   Se si verifica un failover, il servizio agent e il gestore code agent verranno avviati sulla macchina secondaria.

V 9.1.4 Agent ad alta disponibilità in Managed File Transfer

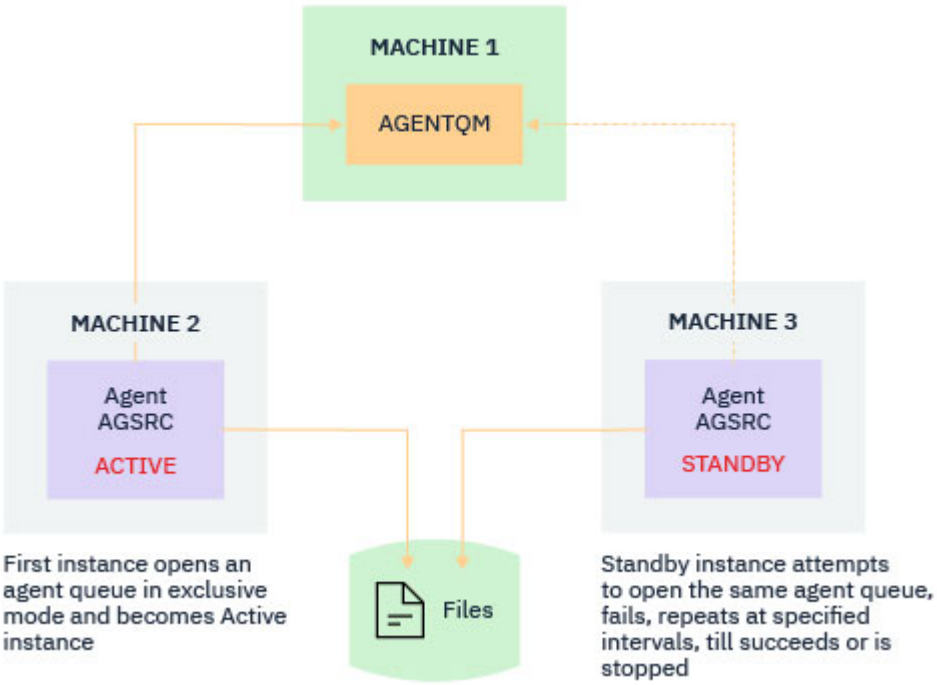
Da IBM MQ 9.1.4, è possibile configurare gli agent bridge o standard in MFT per l'esecuzione in una configurazione HA (High Availability). Una coppia di istanze agent con configurazioni identiche sono coinvolte nella configurazione HA, dove un'istanza è in esecuzione su una macchina mentre un'altra è in esecuzione su una macchina diversa. Entrambe le istanze sono configurate per connettersi allo stesso gestore code dell'agent.

Panoramica

Solo una, denominata *istanza attiva*, delle due istanze, sta elaborando i trasferimenti file, mentre l'altra istanza, denominata *istanza standby*, è in uno stato in cui può completare l'inizializzazione e prendere il controllo eseguendo i trasferimenti file, ma non elabora alcun trasferimento file.

Quando un'istanza attiva ha esito negativo o perde la connettività al gestore code, l'istanza in standby completa la sua inizializzazione, diventa attiva e avvia l'elaborazione dei trasferimenti file. Tutti i trasferimenti in corso quando l'istanza attiva non è riuscita vengono ripristinati dall'ultimo punto di controllo noto.

La seguente illustrazione mostra una configurazione comune degli agent attivi e



standby:

Note:

1. Un'istanza di un agente è in esecuzione su due macchine differenti, con una delle istanze come istanza attiva e l'altra come istanza standby.
2. Solo l'istanza attiva elabora i trasferimenti. L'istanza standby è in uno stato di inattività, in attesa che l'istanza attiva si disattivi.
3. La stessa serie di code agent è condivisa tra due istanze di un agent.
4. Entrambe le istanze dell'agent devono accedere allo stesso filesystem condiviso per eseguire i trasferimenti gestiti

Il meccanismo dell'istanza dell'agent attivo - standby funziona prendendo un blocco su una risorsa condivisa, come i gestori code a più istanze IBM MQ . L'istanza dell'agente che prende un blocco sulla risorsa condivisa diventa l'istanza attiva mentre l'altra istanza (che non riesce a prendere un blocco) diventa un'istanza standby.

La risorsa condivisa è una nuova coda, SYSTEM.FTE.HA.<agent name>. Questa coda viene creata automaticamente quando viene configurato un agente IBM MQ 9.1.4 .

Come funziona il processo

Per creare un agent HA, si crea un agent con parametri di configurazione identici su due macchine eseguendo il comando **fteCreateAgent** o **fteCreateBridgeAgent** utilizzando il parametro **-x** aggiuntivo insieme alla proprietà dell'agent **highlyAvailable** nel file agent.properties impostato su true.

Note:

- Entrambe le configurazioni devono puntare allo stesso gestore code dell'agente.
- Le code agent richieste devono essere create solo una volta sul gestore code agent.

Per ulteriori informazioni sulla proprietà dell'agent **highlyAvailable** , consultare il comando **fteCreateAgent** per ulteriori informazioni sul parametro **-x** e il file agent.properties .

Tenere presente che l'esecuzione di uno dei comandi crea un file MQSC contenente gli script richiesti per creare gli oggetti IBM MQ nel gestore code dell'agent e la coda <SYSTEM.FTE.HA.*agent name* , indipendentemente dal fatto che si specifichi o meno il parametro **-x** .

Durante la creazione di una configurazione dell'agent ad alta disponibilità, il comando **fteCreateAgent** o **fteCreateBridgeAgent** verifica l'esistenza di un'istanza dello stesso agent presente altrove sottoscrivendo l'argomento SYSTEM.FTE/Agents/*agent name* . Se viene trovata un'istanza dello stesso agent, il comando crea la configurazione richiesta sul file system ma non pubblica nuovamente la creazione dell'agent.

Quando un agent viene avviato in modalità HA:

1. L'agent tenta di aprire la coda SYSTEM.FTE.HA.*agent name* in modalità GET esclusiva.
2. Se l'agent apre correttamente la coda SYSTEM.FTE.HA.*agent name* , questa diventa l' *istanza attiva* di un agent e un ulteriore processo di avvio continua.
3. Se il tentativo di aprire la coda SYSTEM.FTE.HA.*agent name* in una modalità GET esclusiva ha esito negativo con il codice motivo MQRC_OBJECT_IN_USE, significa che esiste già un'istanza attiva dell'agent in esecuzione altrove. Di conseguenza, questa istanza diventa l' *istanza standby* dell'agente.

   L'istanza in standby tenta di aprire la coda SYSTEM.FTE.HA.<agent name> a intervalli specificati. Una proprietà agent aggiuntiva **standbyPollInterval** viene fornita per questo scopo nel file agent.properties .

   Con il valore predefinito, l'istanza in standby tenta di aprire la coda SYSTEM.FTE.HA.*agent name* ogni cinque secondi. Ciò si ripete fino a quando l'istanza riesce ad aprire la coda SYSTEM.FTE.HA.*agent name* o viene arrestata utilizzando il comando **fteStopAgent** .

Più istanze in standby

Tutte le istanze standby tentano di prendere la coda SYSTEM.FTE.HA.*agent name* in una modalità GET esclusiva e l'istanza che ha esito positivo, dopo che l'istanza attiva ha avuto esito negativo, diventa l'istanza attiva.

L'istanza attiva conserva le informazioni di tutte le istanze di standby note e pubblica le informazioni come parte della pubblicazione dello stato agent. Da IBM MQ 9.1.4, l'output del comando **fteShowAgentDetails** , la risposta GET REST API dell'agent e il plug-in IBM MQ Explorer MFT visualizzano informazioni su tutte le istanze in standby.

Per ulteriori informazioni, vedi gli output di esempio del comando **fteShowAgentDetails** e la risposta GET REST API dell'agent.

Consultare MFT Messaggi di stato dell'agente per esempi di informazioni sullo stato dell'agente in formato XML.

Requisito versione

Gli agent attivi e standby devono essere IBM MQ 9.1.4 o superiori.

Attenzione:

- Non è possibile configurare o avviare le versioni di IBM MQ precedenti a IBM MQ 9.1.4 in modalità alta disponibilità.
- Sia le istanze attive che quelle in standby devono eseguire la stessa versione del codice.

La versione delle istanze attive e standby viene convalidata per garantire che entrambe le istanze siano della stessa versione. Una coda dinamica temporanea viene utilizzata per la comunicazione tra le istanze. Due proprietà agent, **dynamicQueuePrefix** e **modelQueueName**, definite nel file agent.properties , generano il nome della coda dinamica temporanea.

V 9.1.4 Informazioni richieste per gli agent ad alta disponibilità in Managed File Transfer

Esistono vari tipi di informazioni che è necessario conoscere sugli agent standard o bridge MFT in esecuzione in una configurazione ad alta disponibilità. Queste informazioni includono i diversi metodi con cui viene avviato l'agent, come identificare l'istanza dell'agent nel file di log e le informazioni sullo stato per l'agent.

Avvio di un agent

Un'istanza di un agent è in esecuzione in una modalità non HA altrove

Se viene effettuato un tentativo di avviare un'altra istanza dell'agent non configurata come un agent HA, viene prima effettuato un controllo per verificare se è possibile acquisire un blocco sulla coda SYSTEM.FTE.HA.*agent name* .

Poiché l'altra istanza è stata avviata in modalità non HA, il vincolo sulla coda SYSTEM.FTE.HA.*agent name* verrà acquisito da questa istanza. L'agent continua l'inizializzazione, ma non riesce in un secondo momento perché la coda comandi viene aperta esclusivamente da un'altra istanza.

In questo caso, i messaggi mostrati nel seguente esempio vengono registrati sul file output0.log dell'agente e l'agente continua il suo tentativo di aprire la coda comandi ogni 30 secondi:

```
BFGMQ1045I: Coda di sistema dell'agent 'SYSTEM.FTE.COMMAND.SRC' è configurato come NOSHARE o
DEFSOPT (CONDIVISO).

BFGAG0035W: l'agente ha ricevuto il codice motivo MQI 2042 durante il tentativo di apertura della
coda
'SYSTEM.FTE.COMMAND.SRC'sul gestore code' MFTHAQM 'con nome connessione' localhost (1414) '
e canale 'MFT_HA_CHN'.  L'agent tenterà nuovamente l'operazione ogni 30 secondi.
```

Un'istanza di un agent è in esecuzione in una modalità HA altrove

Se viene effettuato un tentativo di avviare un'altra istanza dell'agent non configurata come un agent HA, viene prima effettuato un controllo per verificare se è possibile acquisire un blocco sulla coda SYSTEM.FTE.HA.*agent name* .

Poiché l'altra istanza è stata eseguita come istanza attiva, il tentativo di acquisire un blocco ha esito negativo. L'istanza non viene avviata e il seguente errore viene registrato nel file output0.log dell'agent:

```
BFGAG0194E: Un'istanza di questo agent è già in esecuzione altrove.
Pertanto, questa istanza non può continuare e verrà terminata.
```

Windows Avvio dell'agent come servizio Windows

Su Windows, è possibile avviare un agent come servizio Windows .

Durante l'avvio, Windows avvia l'agent MFT in modalità normale o HA. Se l'agent è configurato per essere eseguito in modalità HA, il servizio viene eseguito come istanza attiva o standby, a seconda di quale istanza acquisisce per prima il blocco.

Identificazione del tipo di istanza di un agente nel file di log

I messaggi informativi vengono scritti nel file output0.log dell'agente per indicare il tipo di istanza. Quando un'istanza agent viene avviata come istanza attiva, viene scritto il seguente messaggio:

```
BFGAG0193I: L'agent è stato inizializzato correttamente come istanza attiva.
```

Quando un'istanza dell'agent viene avviata come istanza standby, viene scritto il seguente messaggio:

```
BFGAG0193I: L'agent è stato inizializzato correttamente come un'istanza standby.
```

Aggiornamenti dello stato dell'agente

Poiché esistono due istanze dello stesso agent in esecuzione, è necessario disporre delle informazioni su entrambe le istanze nella pubblicazione dello stato dell'agent.

Si noti che l'istanza attiva è quella che pubblica lo stato di entrambe le istanze.

Istanza standby

Durante la pubblicazione dello stato dell'agent, l'istanza attiva controlla la durata della pubblicazione dell'istanza in standby.

Esistono due proprietà aggiuntive nel file `agent.properties` per questo scopo:

- **`standbyStatusExpiry`** è la scadenza per il messaggio di stato standby da inserire nella coda comandi dell'agent. Il messaggio scade se l'istanza attiva di un agente non elabora questo messaggio in tale periodo.

  Per impostazione predefinita, il valore di **`standbyStatusExipry`** è 30 secondi. Il messaggio è anche un messaggio con priorità bassa, 9, per consentire l'elaborazione con priorità delle richieste di trasferimento rispetto ai messaggi di stato standby.
- **`standbyStatusPublishInterval`** imposta la frequenza con cui l'istanza in standby pubblica il relativo stato.

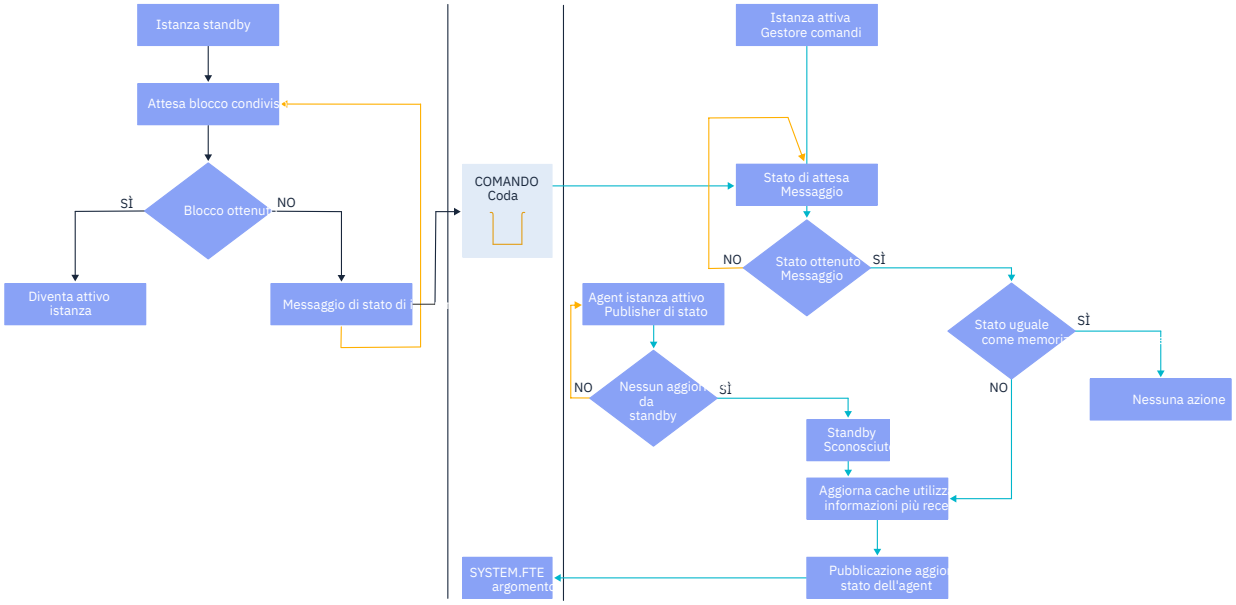
Istanza attiva

L'istanza attiva effettua le seguenti operazioni per elaborare gli aggiornamenti dello stato dall'istanza standby:

1. Richiama il messaggio dalla coda SYSTEM.FTE.COMMAND.<agent name> e delega l'elaborazione del messaggio a un thread di lavoro.
2. Il thread di lavoro richiama il contenuto dal corpo del messaggio, aggiorna l'oggetto di stato dell'agent con le informazioni sull'istanza in standby e notifica al publisher di stato agent di pubblicare lo stato.
3. Il publisher dello stato dell'agent pubblica lo stato.

   Notare che le ottimizzazioni vengono eseguite qui per memorizzare nella cache le informazioni sullo stato di standby. Quando viene effettuata una richiesta, il publisher dello stato dell'agent controlla il nuovo stato con lo stato memorizzato nella cache e pubblica solo se è presente una differenza.

Il seguente diagramma descrive il flusso seguito dalle istanze attive o standby per pubblicare lo stato di un agent:



V 9.1.4 Eliminazione di istanze, failover e manutenzione in agent altamente disponibili

Le istanze Managed File Transfer ad alta disponibilità possono essere eliminate, possono avere esito negativo in vari modi e potrebbero richiedere manutenzione.

Eliminazione dello stato dell'istanza in standby

Ci possono essere situazioni in cui l'istanza attiva è occupata con i trasferimenti e non è in grado di elaborare i messaggi di stato dell'istanza in standby, l'istanza in standby non è riuscita o non sta pubblicando i messaggi di stato per qualsiasi motivo.

In tali scenari, l'agente attivo che era consapevole della presenza di un'istanza standby attende il valore specificato dalla proprietà **standbyStatusDiscardTime** del file `agent.properties` prima di rimuovere l'istanza standby dal relativo elenco. Il valore predefinito per questa proprietà è 600 secondi, che è il doppio della proprietà **standbyStatusPublishInterval** .

Failover normale su un'istanza

È necessario utilizzare il comando **fteStopAgent** con l'opzione **-i** per eseguire un normale failover.

Ciò garantisce che l'istanza attiva venga arrestata immediatamente. Se si arresta un agent senza l'opzione **-i** , l'agent continua l'esecuzione fino a quando tutti i trasferimenti in corso non vengono completati dall'istanza attiva, quindi, il failover potrebbe richiedere molto tempo.

Eventuali trasferimenti in volo riprendono dall'ultimo punto di controllo noto.

Failover di un'istanza in altre situazioni

Se un'istanza attiva termina in un modo non normale o se l'intera macchina ha esito negativo, la connessione alla coda dell'agent viene interrotta e il gestore code chiude tutte le code aperte, inclusa la coda SYSTEM.FTE.HA.<agent name> e le connessioni.

A causa di ciò, l'istanza standby acquisisce il GET esclusivo e completa il resto dell'inizializzazione dell'agent.

Anche in questo caso, i trasferimenti in volo riprendono dagli ultimi punti di controllo noti.

In caso di interruzione di una connessione al gestore code

Modalità client

Un processo agent è composto da diversi thread. Oltre ai thread predefiniti, ad esempio, un thread che pubblica lo stato dell'agente a intervalli regolari, ogni richiesta di trasferimento viene gestita con una serie di thread che terminano dopo il completamento di un trasferimento.

Molti di questi thread si collegano al gestore code dell'agent e inviano e ricevono messaggi. È possibile che una di queste connessioni possa interrompersi a causa di un problema di rete o di un errore del gestore code. Quando un thread rileva un problema di connessione interrotta, il thread informa il thread principale di avviare il ripristino e termina.

Il thread principale avvia quindi un altro thread per attendere che venga stabilita una connessione al gestore code. Una volta riconnesso, viene effettuato un tentativo di acquisire il GET esclusivo per l'agente. Se l'operazione ha esito positivo, l'agent continua a completare il recupero e diventa l'istanza attiva. Se il tentativo di acquisire il GET esclusivo non riesce, l'istanza diventa standby.

Modalità bind

Durante la connessione in modalità bind, se un agent perde la connessione, il processo dell'agent termina. Il controller processi gestisce il riavvio dell'agent. Quando un agent viene riavviato, viene eseguito il tentativo di acquisire il GET esclusivo per se stesso.

Se l'agent ha esito positivo, diventa un'istanza attiva; in caso contrario, l'agent diventa un'istanza di standby.

Applicazione degli aggiornamenti del livello di manutenzione

La procedura per l'applicazione della manutenzione agli agent ad alta disponibilità è simile a quella documentata per i gestori code a più istanze. Per ulteriori informazioni, consultare Applicazione degli aggiornamenti del livello di manutenzione ai gestori code a più istanze in Windows, Applicazione degli aggiornamenti del livello di manutenzione ai gestori code a più istanze in AIX, Applicazione degli aggiornamenti del livello di manutenzione ai gestori code a più istanze in Solaris o Applicazione degli aggiornamenti del livello di manutenzione ai gestori code a più istanze in Linux.

È necessario arrestare l'agent in esecuzione sulla macchina su cui deve essere applicato il livello di manutenzione, prima di applicare la manutenzione. Se si sta aggiornando un'istanza attiva, per la continuità dei trasferimenti, è necessario eseguire il failover dell'istanza attiva su un'istanza in standby.

Una volta completato l'aggiornamento, è possibile avviare l'istanza dell'agent, eseguire il failover dell'istanza attiva corrente sull'istanza aggiornata e quindi aggiornare l'istanza standby.

Migrazione di agent da una versione precedente del prodotto

Gli agent migrati dalle versioni di IBM MQ precedenti a IBM MQ 9.1.4 vengono eseguiti come non altamente disponibili. È possibile eseguirli in modalità alta disponibilità seguendo la procedura in Migrazione di agent Managed File Transfer da una versione precedente.

V 9.1.0 Configurazione di IBM MQ Console e REST API

Il server mqweb che ospita IBM MQ Console e REST API viene fornito con una configurazione predefinita. Per poter utilizzare uno di questi componenti è necessario completare una serie di attività di configurazione, come la configurazione della sicurezza per consentire agli utenti di accedere. Questo argomento descrive tutte le opzioni di configurazione disponibili.

Procedura

- “Configurazione della sicurezza” a pagina 764
- “Configurazione del nome host HTTP” a pagina 764
- “Configurazione delle porte HTTPS e HTTP” a pagina 765
- “Configurazione del timeout di risposta” a pagina 766
- “Configurazione dell'avvio automatico” a pagina 767
- “Configurazione della registrazione nei log” a pagina 768
- “Configurazione del token LTPA” a pagina 770
- “Configurazione del gateway administrative REST API” a pagina 772
- “Configurazione di messaging REST API” a pagina 773
- “Configurazione di REST API per MFT” a pagina 775
- “Ottimizzazione della JVM del server mqweb” a pagina 777
- “Struttura del file del componente di installazione IBM MQ Console e REST API” a pagina 779
- “Configurazione della registrazione dell'utilizzo del server mqweb su z/OS” a pagina 781

Configurazione di base per il server mqweb

Prima di poter iniziare a utilizzare REST API o IBM MQ Console, è necessario installare i componenti corretti e configurare il server mqweb che ospita REST API o IBM MQ Console.

Informazioni su questa attività

La procedura per questa attività si concentra su una configurazione di base per il server mqweb in modo da poter iniziare rapidamente con REST API e IBM MQ Console. La procedura per la configurazione della sicurezza descrive come impostare un registro utente di base, ma esistono altre opzioni per la configurazione di utenti e ruoli. Per ulteriori informazioni sulla configurazione della sicurezza per il server mqweb, consultare IBM MQ Console e REST API security.

Nota: Per completare questa procedura, è necessario avere accesso al file `mqwebuser.xml` :

- z/OS Su z/OS, è necessario essere un utente con accesso in scrittura al file `mqwebuser.xml` .
- Multi Su tutti i sistemi operativi, è necessario essere un utente privilegiato per accedere al file `mqwebuser.xml` .

Procedura

1. Installare il componente IBM MQ Console e REST API :
   - AIX Su AIX, installare il fileset `mqm.web.rte` . Per ulteriori informazioni sull'installazione dei sottopacchetti su AIX, vedere Attività di installazione diAIX.
   - IBM i Su IBM i, installare il componente WEB. Per utilizzare questa funzione, è necessario installare anche 5724L26 IBM MQ Java Messaging and Web Services e 5770JV1 Java SE 8 prerequisites. Per ulteriori informazioni sull'installazione delle funzioni su IBM i, vedere Attività di installazione diIBM i.
   - Linux Su Linux, installare il componente `MQSeriesWeb` . Per ulteriori informazioni relative all'installazione dei componenti su Linux, consultare Attività di installazione diLinux.
   - Solaris Su Solaris, installare il componente `web` . Per ulteriori informazioni relative all'installazione dei componenti su Solaris, consultare Attività di installazione diSolaris.
   - Windows Su Windows, installare la funzione `Web Administration` . Per ulteriori informazioni sull'installazione delle funzioni su Windows, vedere Attività di installazione diWindows.
   - z/OS Su z/OS, installare la funzione `IBM MQ for z/OS Unix System Services Web Components` . Per ulteriori informazioni sull'installazione di componenti e funzioni su z/OS, consultare Attività di installazione diz/OS.
2. z/OS
   Su z/OS, creare il server mqweb che ospita IBM MQ Console e REST API eseguendo lo script **`crtmqweb`** .

   Questo script crea la directory utente WebSphere Liberty contenente la configurazione del server mqweb e i file di log. Per ulteriori informazioni sull'esecuzione dello script **`crtmqweb`** , consultare “Creazione del server mqweb” a pagina 889.
3. z/OS
   Su z/OS, creare una procedura catalogata per avviare il server mqweb.

   Per ulteriori informazioni, consultare “Creazione di una procedura per il server mqweb” a pagina 891.
4. Sostituire il file di configurazione esistente, `mqwebuser.xml` , con il file di esempio del registro di base configurato per offrire la sicurezza di base. Copiare il file `basic_registry.xml` dalla directory *`MQ_INSTALLATION_PATH`*`/web/mq/samp/configuration` nella directory appropriata per il proprio sistema e ridenominare il file in `mqwebuser.xml`:
   - Linux UNIX Su UNIX e Linux: `var/mqm/web/installations/`*`installationName`*`/servers/mqweb`

- Windows Su Windows: *MQ_DATA_PATH*\web\installations*installationName*\servers\mqweb

  Dove *MQ_DATA_PATH* è il percorso dati IBM MQ , questo percorso è il percorso dati selezionato durante l'installazione di IBM MQ. Per impostazione predefinita, questo è C:\ProgramData\IBM\MQ.

- z/OS Su z/OS: *WLP_user_directory*/servers/mqweb

  Dove *WLP_user_directory* è la directory specificata quando lo script **crtmqweb** è stato eseguito per creare la definizione del server mqweb.

Il file di esempio basic_registry.xml configura quattro utenti:

MQADMIN
Un utente di gestione che è un membro del ruolo MQWebAdmin .

mqreader
Un utente di gestione di sola lettura che è un membro del ruolo RO MQWebAdmin.

mftadmin
Un utente amministrativo che è un membro del ruolo MFTWebAdmin .

mftreader
Un utente amministrativo di sola lettura membro del ruolo RO MFTWebAdmin.

Tutti gli utenti sono anche membri del ruolo MQWebUser .

Per ulteriori informazioni sui ruoli disponibili, consultare Ruoli su IBM MQ Console e REST API

5. Opzionale: Modificare il file mqwebuser.xml per aggiungere ulteriori utenti e gruppi. Assegnare a tali utenti e gruppi i ruoli appropriati per essere autorizzati ad utilizzare REST API o IBM MQ Console. È inoltre possibile modificare le password per gli utenti definiti per impostazione predefinita e codificare le nuove password. Per ulteriori informazioni, vedi Configurazione di utenti e ruoli.

   Nota:

   - z/OS Su z/OS, se si aggiungono utenti al ruolo MQWebUser , è necessario concedere anche all'ID utente dell'attività avviata mqweb l'accesso alternativo agli ID utente con il ruolo MQWebUser . Ad esempio:

     ```
     RDEFINE MQADMIN hlq.ALTERNATE.USER.userId UACC(NONE)
     PERMIT hlq.ALTERNATE.USER.userId CLASS(MQADMIN) ACCESS(UPDATE) ID(mqwebUserId)
     ```

   - Multi z/OS Per completare la procedura per iniziare con messaging REST API, devi aggiungere un utente al file mqwebuser.xml . Questo utente deve avere lo stesso nome di un utente IBM MQ esistente sul sistema. Seguendo lo stesso formato degli altri utenti nel file XML, aggiungere ID utente e password dopo la riga seguente nel file xml: <user name="mftreader" password="mftreader" />.

6. z/OS
   Su z/OS, impostare la variabile di ambiente WLP_USER_DIR in modo che la variabile punti alla configurazione del server mqweb, immettendo il seguente comando:

   ```
   export WLP_USER_DIR=WLP_user_directory
   ```

   dove *WLP_user_directory* è il nome della directory passata a crtmqweb. Ad esempio:

   ```
   export WLP_USER_DIR=/var/mqm/web/installation1
   ```

   Per ulteriori informazioni, consultare “Creazione del server mqweb” a pagina 889.

7. Per default, REST API e IBM MQ Console sono disponibili solo dallo stesso host del server mqweb. Abilitare le connessioni remote al server mqweb immettendo il seguente comando:

   ```
   setmqweb properties -k httpHost -v hostname
   ```

Dove *hostname* specifica l'indirizzo IP, il nome host DNS (domain name server) con suffisso nome dominio o il nome host DNS del server in cui è installato IBM MQ . Utilizzare un asterisco, *, tra virgolette, per specificare tutte le interfacce di rete disponibili, come mostrato nel seguente esempio:

```
setmqweb properties -k httpHost -v "*"
```

8. Opzionale: Per impostazione predefinita, administrative REST API per MFT non è abilitato. Se si desidera utilizzare questa funzione, è necessario abilitarla e configurare un gestore code di coordinamento:
   a) Abilitare administrative REST API per MFT immettendo il seguente comando:

   ```
   setmqweb properties -k mqRestMftEnabled -v true
   ```

   b) Configurare quale gestore code è il gestore code di coordinamento immettendo il seguente comando:

   ```
   setmqweb properties -k mqRestMftCoordinationQmgr -v qmgrName
   ```

   Dove *qmgrName* è il nome del gestore code di coordinamento.

   c) CD
   Per abilitare chiamate POST, configurare quale gestore code è il gestore code comandi immettendo il seguente comando:

   ```
   setmqweb properties -k mqRestMftCommandQmgr -v qmgrName
   ```

   Dove *qmgrName* è il nome del gestore code comandi.

   Nota: Questo passo si applica da IBM MQ 9.1.2.
9. Avviare il server mqweb che supporta REST API e IBM MQ Console:
   - ULW Su UNIX, Linux, and Windows, come utente privilegiato, immettere il seguente comando:

     ```
     strmqweb
     ```

   - IBM i Su IBM i, come utente privilegiato, immettere il seguente comando in Qshell:

     ```
     /QIBM/ProdData/mqm/bin/strmqweb
     ```

   - z/OS Su z/OS, avviare la procedura creata in “Creazione di una procedura per il server mqweb” a pagina 891.

     I seguenti messaggi vengono emessi per STDOUT DD per indicare che il server mqweb è stato avviato correttamente.

     ```
     [AUDIT   ] MQWB2019I: MQ Console level: 9.2.4 - V924-CD924-L211028
     [AUDIT   ] MQWB0023I: MQ REST API level: 9.2.4 - V924-CD924-L211028
     [AUDIT   ] CWWKZ0001I: Application com.ibm.mq.rest started in 1.763 seconds.
     [AUDIT   ] CWWKZ0001I: Application com.ibm.mq.console started in 2.615 seconds.
     [AUDIT   ] CWWKF0011I: The mqweb server is ready to run a smarter planet. The mqweb
     server started in 10.016 seconds.
     ```

   È possibile arrestare il server mqweb in qualsiasi momento arrestando l'attività avviata del server mqweb suz/OSo utilizzando il comando **endmqweb** . Tuttavia, se il server mqweb non è in esecuzione, non è possibile utilizzare REST API o IBM MQ Console.
10. z/OS
    Opzionale: Su z/OS, se si desidera consentire ai prodotti di automazione del sistema di eseguire il trap dei messaggi MQWB2019I e MQWB0023I emessi all'avvio di MQ Console e REST API , configurare il server mqweb per scrivere tali messaggi nella console MVS . Per configurare il server mqweb in modo che scriva i messaggi MQWB2019I e MQWB0023I nella console MVS , modificare il file `mqwebuser.xml` creato nel passo “4” a pagina 761e aggiungere la riga seguente al file:

```
<zosLogging enableLogToMVS="true" wtoMessage="MQWB2019I,MQWB0023I"/>
```

Per ulteriori informazioni sulla configurazione della registrazione z/OS nel server mqweb, consultare z/OS Logging (zosLogging).

Operazioni successive

1. Configurare le impostazioni del server mqweb, compresa l'abilitazione delle connessioni HTTP e la modifica del numero di porta. Per ulteriori informazioni, consultare “Configurazione di IBM MQ Console e REST API” a pagina 760.
2. Facoltativamente, configurare REST API:
   a. Configurare la condivisione di risorse tra origini per REST API. Per impostazione predefinita, non puoi accedere a REST API dalle risorse web che non sono ospitate sullo stesso dominio di REST API. In altre parole, le richieste tra origini non sono abilitate. È possibile configurare CORS (Cross Origin Resource Sharing) per consentire richieste tra origini da URL specificati. Per ulteriori informazioni, consultare Configurazione di CORS per REST API.
   b. Configurare REST API per MFT. Per ulteriori informazioni, consultare “Configurazione di REST API per MFT” a pagina 775.
3. Utilizzare REST API o IBM MQ Console:
   - Introduzione a administrative REST API
   - Introduzione a messaging REST API
   - Introduzione a IBM MQ Console

V 9.1.0 Configurazione della sicurezza

È possibile configurare la protezione per IBM MQ Console e REST API modificando il file `mqwebuser.xml` . È possibile configurare e autenticare gli utenti configurando un registro utenti di base o un registro LDAP o uno qualsiasi degli altri tipi di registro forniti con WebSphere Liberty. È quindi possibile autorizzare tali utenti assegnando un ruolo a utenti e gruppi.

Informazioni su questa attività

Per configurare la sicurezza per IBM MQ Console, e REST API, è necessario configurare utenti e gruppi. Questi utenti e gruppi possono quindi essere autorizzati a utilizzare IBM MQ Console, REST APIo entrambi. Per ulteriori informazioni sulla configurazione di utenti e gruppi e sull'autenticazione e l'autorizzazione degli utenti, consultare IBM MQ Console e REST API security.

Quando gli utenti eseguono l'autenticazione con IBM MQ Console, viene generato un token LTPA. Questo token consente all'utente di utilizzare IBM MQ Console senza eseguire nuovamente l'autenticazione fino alla scadenza del token.

Se si utilizza l'autenticazione basata sul token con REST API, viene generato un token LTPA differente quando l'utente accede utilizzando la risorsa `/login` REST API con il metodo HTTP POST. È possibile configurare quando questo token scade e se può essere utilizzato per entrambe le connessioni HTTP e HTTPS. Per ulteriori informazioni, consultare “Configurazione del token LTPA” a pagina 770.

Procedura

- IBM MQ Console e REST API sicurezza
- “Configurazione del token LTPA” a pagina 770

V 9.1.0 Configurazione del nome host HTTP

Per impostazione predefinita, il server mqweb che ospita IBM MQ Console e REST API è configurato per consentire solo connessioni locali. Ovvero, è possibile accedere a IBM MQ Console e REST API solo sul

sistema su cui sono installati IBM MQ Console e REST API . È possibile configurare il nome host per consentire le connessioni remote utilizzando il comando **setmqweb** .

Prima di iniziare

Per completare questa attività, è necessario essere un utente con determinati privilegi in modo da poter utilizzare i comandi **dspmqweb** e **setmqweb**:

- z/OS Su z/OS, è necessario disporre dell'autorità per eseguire i comandi **dspmqweb** e **setmqweb** e l'accesso in scrittura al file `mqwebuser.xml`.
- Multi Su tutti gli altri sistemi operativi, è necessario essere un utente privilegiato.

Attenzione: z/OS V 9.1.0

Prima di immettere i comandi **setmqweb** o **dspmqweb** in z/OS, è necessario impostare la variabile di ambiente WLP_USER_DIR, in modo che la variabile punti alla configurazione del server mqweb.

Per eseguire questa operazione, immettere il seguente comando:

```
export WLP_USER_DIR=WLP_user_directory
```

dove *WLP_user_directory* è il nome della directory passata a `crtmqweb`. Ad esempio:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Per ulteriori informazioni, consultare Creazione del server mqweb.

Procedura

- Visualizzare la configurazione corrente del nome host HTTP utilizzando il seguente comando:

  ```
  dspmqweb properties -a
  ```

  Il campo `httpHost` mostra il nome host HTTP. Per ulteriori informazioni, vedere dspmqweb.
- Impostare il nome host HTTP utilizzando il seguente comando:

  ```
  setmqweb properties -k httpHost -v hostName
  ```

  dove *hostName* specifica l'indirizzo IP, il nome host DNS (domain name server) con suffisso nome dominio o il nome host DNS del server in cui è installato IBM MQ . Utilizzare un asterisco tra virgolette per specificare tutte le interfacce di rete disponibili. Utilizzare il valore `localhost` per consentire solo connessioni locali.
- Annullare l'impostazione del nome host HTTP utilizzando il seguente comando:

  ```
  setmqweb properties -k httpHost -d
  ```

V 9.1.0 Configurazione delle porte HTTPS e HTTP

Per impostazione predefinita, il server mqweb che ospita IBM MQ Console e REST API utilizza la porta HTTPS 9443. La porta associata alle connessioni HTTP non è abilitata. È possibile abilitare la porta HTTP, configurare una porta HTTPS diversa o disabilitare la porta HTTPS o HTTP. È possibile configurare le porte utilizzando il comando **setmqweb** .

Prima di iniziare

Se si abilita la porta HTTP e si utilizza l'autenticazione basata su token, è necessario abilitare lo stesso token LTPA da utilizzare per le connessioni HTTP e HTTPS. Per ulteriori informazioni, consultare “Configurazione del token LTPA” a pagina 770.

Per completare questa attività, è necessario essere un utente con determinati privilegi in modo da poter utilizzare i comandi **dspmqweb** e **setmqweb**:

- z/OS Su z/OS, è necessario disporre dell'autorità per eseguire i comandi **dspmqweb** e **setmqweb** e l'accesso in scrittura al file `mqwebuser.xml`.
- Multi Su tutti gli altri sistemi operativi, è necessario essere un utente privilegiato.

Attenzione: z/OS V 9.1.0

Prima di immettere i comandi **setmqweb** o **dspmqweb** in z/OS, è necessario impostare la variabile di ambiente WLP_USER_DIR, in modo che la variabile punti alla configurazione del server mqweb.

Per eseguire questa operazione, immettere il seguente comando:

```
export WLP_USER_DIR=WLP_user_directory
```

dove *WLP_user_directory* è il nome della directory passata a `crtmqweb`. Ad esempio:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Per ulteriori informazioni, consultare Creazione del server mqweb.

Procedura

- Visualizzare la configurazione corrente delle porte HTTPS e HTTP utilizzando il seguente comando:

  ```
  dspmqweb properties -a
  ```

  Il campo `httpPort` mostra la porta HTTP e il campo `httpsPort` mostra la porta HTTPS. Per ulteriori informazioni, vedere dspmqweb.
- Abilitare o configurare la porta HTTP: utilizzando il seguente comando:
  - Abilitare o impostare la porta HTTP utilizzando il seguente comando:

    ```
    setmqweb properties -k httpPort -v portNumber
    ```

    dove *portNumber* specifica la porta che si desidera utilizzare per le connessioni HTTP. È possibile disabilitare la porta utilizzando il valore `-1`.
  - Reimpostare il valore della porta HTTP sul valore predefinito `-1` utilizzando il seguente comando:

    ```
    setmqweb properties -k httpPort -d
    ```
- Configurare la porta HTTPS:
  - Impostare il numero di porta HTTPS utilizzando il seguente comando:

    ```
    setmqweb properties -k httpsPort -v portNumber
    ```

    dove *portNumber* specifica la porta che si desidera utilizzare per le connessioni HTTPS. È possibile disabilitare la porta utilizzando il valore `-1`.
  - Reimpostare il numero di porta HTTPS sul valore predefinito 9443 utilizzando il seguente comando:

    ```
    setmqweb properties -k httpsPort -d
    ```

V 9.1.0 Configurazione del timeout di risposta

Per impostazione predefinita, IBM MQ Console e REST API sono in timeout se il tempo impiegato per inviare una risposta a un client è superiore a 30 secondi. È possibile configurare IBM MQ Console e REST API per utilizzare un valore di timeout differente utilizzando il comando **setmqweb** .

Prima di iniziare

Per completare questa attività, è necessario essere un utente con determinati privilegi in modo da poter utilizzare i comandi **dspmqweb** e **setmqweb**:

- z/OS Su z/OS, è necessario disporre dell'autorità per eseguire i comandi **dspmqweb** e **setmqweb** e l'accesso in scrittura al file `mqwebuser.xml`.
- Multi Su tutti gli altri sistemi operativi, è necessario essere un utente privilegiato.

Attenzione: z/OS V 9.1.0

Prima di immettere i comandi **setmqweb** o **dspmqweb** in z/OS, è necessario impostare la variabile di ambiente WLP_USER_DIR, in modo che la variabile punti alla configurazione del server mqweb.

Per eseguire questa operazione, immettere il seguente comando:

```
export WLP_USER_DIR=WLP_user_directory
```

dove *WLP_user_directory* è il nome della directory passata a `crtmqweb`. Ad esempio:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Per ulteriori informazioni, consultare Creazione del server mqweb.

Procedura

- Visualizzare la configurazione corrente del timeout della richiesta utilizzando il seguente comando:

  ```
  dspmqweb properties -a
  ```

  Il campo `mqRestRequestTimeout` mostra il valore corrente per il timeout di risposta. Per ulteriori informazioni, vedere dspmqweb.
- Impostare il timeout della richiesta utilizzando il comando seguente:

  ```
  setmqweb properties -k mqRestRequestTimeout -v timeout
  ```

  dove *timeout* specifica il tempo, in secondi, prima del timeout.
- Reimpostare il timeout della richiesta sul valore predefinito di 30 secondi utilizzando il seguente comando:

  ```
  setmqweb properties -k mqRestRequestTimeout -d
  ```

V 9.1.0 Configurazione dell'avvio automatico

Per impostazione predefinita, il IBM MQ Console viene avviato automaticamente all'avvio del server mqweb. È possibile configurare se IBM MQ Console e REST API vengono avviati automaticamente utilizzando il comando **setmqweb** .

Prima di iniziare

Per completare questa attività, è necessario essere un utente con determinati privilegi in modo da poter utilizzare i comandi **dspmqweb** e **setmqweb**:

- z/OS Su z/OS, è necessario disporre dell'autorità per eseguire i comandi **dspmqweb** e **setmqweb** e l'accesso in scrittura al file `mqwebuser.xml`.
- Multi Su tutti gli altri sistemi operativi, è necessario essere un utente privilegiato.

Attenzione: z/OS V 9.1.0

Prima di immettere i comandi **setmqweb** o **dspmqweb** in z/OS, è necessario impostare la variabile di ambiente WLP_USER_DIR, in modo che la variabile punti alla configurazione del server mqweb.

Per eseguire questa operazione, immettere il seguente comando:

```
export WLP_USER_DIR=WLP_user_directory
```

dove *WLP_user_directory* è il nome della directory passata a crtmqweb. Ad esempio:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Per ulteriori informazioni, consultare Creazione del server mqweb.

Procedura

- Visualizzare la configurazione corrente dell'avvio automatico utilizzando il seguente comando:

  ```
  dspmqweb properties -a
  ```

  Il campo mqRestAutostart mostra se REST API viene avviato automaticamente e il campo mqConsoleAutostart mostra se IBM MQ Console viene avviato automaticamente. Per ulteriori informazioni, vedere dspmqweb.
- Configurare se IBM MQ Console viene avviato automaticamente utilizzando il seguente comando:

  ```
  setmqweb properties -k mqConsoleAutostart -v start
  ```

  dove *start* è il valore true se si desidera che IBM MQ Console venga avviato automaticamente o false in caso contrario.
- Configurare se REST API viene avviato automaticamente utilizzando il seguente comando:

  ```
  setmqweb properties -k mqRestAutostart -v start
  ```

  dove *start* è il valore true se si desidera che REST API venga avviato automaticamente o false in caso contrario.

V 9.1.0 Configurazione della registrazione nei log

È possibile configurare i livelli di log, la dimensione massima del file di log e il numero massimo di file di log utilizzati dal server mqweb che ospita IBM MQ Console e REST API. Puoi configurare la registrazione utilizzando il comando **setmqweb** .

Prima di iniziare

Per completare questa attività, è necessario essere un utente con determinati privilegi in modo da poter utilizzare i comandi **dspmqweb** e **setmqweb**:

- z/OS Su z/OS, è necessario disporre dell'autorità per eseguire i comandi **dspmqweb** e **setmqweb** e l'accesso in scrittura al file mqwebuser.xml.
- Multi Su tutti gli altri sistemi operativi, è necessario essere un utente privilegiato.

Informazioni su questa attività

I file di log per il server mqweb si trovano in una delle directory seguenti:

- ULW Su UNIX, Linux, and Windows: *MQ_DATA_PATH*/web/installations/*installationName*/servers/mqweb/logs
- z/OS Su z/OS: *WLP_user_directory*/servers/mqweb/logs

  dove *WLP_user_directory* è la directory specificata quando è stato eseguito lo script V 9.1.0 **crtmqweb** per creare la definizione del server mqweb.

I file di traccia della messaggistica per il server mqweb si trovano in una delle seguenti directory:

- ULW Su UNIX, Linux, and Windows: *MQ_DATA_PATH*/web/installations/*installationName*/servers/mqweb
- z/OS Su z/OS: *WLP_user_directory*/servers/mqweb

dove *WLP_user_directory* è la directory specificata quando è stato eseguito lo script V 9.1.0 **crtmqweb** per creare la definizione del server mqweb.

Per ulteriori informazioni sull'abilitazione della traccia per IBM MQ Console e REST API, consultare Traccia di IBM MQ Console e REST API.

Procedura

- Visualizzare la configurazione corrente della registrazione REST API utilizzando il seguente comando:

  ```
  dspmqweb properties -a
  ```

  Il campo `maxTraceFileSize` mostra le dimensioni massime del file di traccia, il campo `maxTraceFiles` mostra il numero massimo di file di traccia e il campo `traceSpec` mostra il livello di traccia utilizzato. Inoltre, il campo `maxMsgTraceFileSize` mostra la dimensione massima del file di traccia di messaggistica e il campo `maxMsgTraceFiles` mostra il numero massimo di file di traccia di messaggistica. Per ulteriori informazioni, vedere dspmqweb.
- Configurare la dimensione massima del file di log:
  - Impostare la dimensione massima del file di log utilizzando il comando seguente:

    ```
    setmqweb properties -k maxTraceFileSize -v size
    ```

    dove *size* specifica la dimensione, in MB, che ogni file di log può raggiungere per IBM MQ Console.
  - Ripristinare la dimensione massima del file di log sul valore predefinito di 20 MB utilizzando il seguente comando:

    ```
    setmqweb properties -k maxTraceFileSize -d
    ```
- Configurare il numero massimo di file da utilizzare per la registrazione:
  - Impostare il numero massimo di file da utilizzare per la registrazione utilizzando il seguente comando:

    ```
    setmqweb properties -k maxTraceFiles -v max
    ```

    dove *max* specifica il numero massimo di file per IBM MQ Console.
  - Reimpostare il numero massimo di file da utilizzare per la registrazione sul valore predefinito 2 utilizzando il seguente comando:

    ```
    setmqweb properties -k maxTraceFiles -d
    ```
- Configurare la dimensione massima della traccia di messaggistica:
  - Impostare la dimensione massima della traccia di messaggistica utilizzando il seguente comando:

    ```
    setmqweb properties -k maxMsgTraceFileSize -v size
    ```

    dove *size* specifica la dimensione, in MB, che ogni file di log può raggiungere.
  - Reimpostare la dimensione massima del file di log sul valore predefinito di 200 MB utilizzando il seguente comando:

    ```
    setmqweb properties -k maxMsgTraceFileSize -d
    ```
- Configurare il numero massimo di file di traccia di messaggistica da utilizzare:
  - Impostare il numero massimo di file da utilizzare per la traccia di messaggistica utilizzando il seguente comando:

    ```
    setmqweb properties -k maxMsgTraceFiles -v max
    ```

    dove *max* specifica il numero massimo di file.
  - Reimpostare il numero massimo di file da utilizzare per la traccia di messaggistica sul valore predefinito 5 utilizzando il seguente comando:

    ```
    setmqweb properties -k maxMsgTraceFiles -d
    ```
- Configurare il livello di registrazione utilizzato:

- Impostare il livello di registrazione utilizzato utilizzando il seguente comando:

  ```
  setmqweb properties -k traceSpec -v level
  ```

  dove *livello* è uno dei valori elencati in Tabella 52 a pagina 770. La tabella descrive i livelli di registrazione in aumento del livello di dettaglio. Quando si abilita un livello di registrazione, si abilita anche ciascun livello prima di esso. Ad esempio, se si abilita il livello di registrazione ***=warning** , si abilitano anche i livelli di registrazione ***=severe**e ***=fatal** .

  Modificare questo valore quando IBM Service lo richiede.
- Reimpostare il livello di registrazione utilizzato sul valore predefinito di ***=info** utilizzando il seguente comando:

  ```
  setmqweb properties -k traceSpec -d
  ```

Tabella 52. Livelli di registrazione validi

Valore	**Livello di registrazione applicato**
* =disattivo	La registrazione è disattivata.
* =irreversibile	L'attività non può continuare e il componente, l'applicazione e il server non possono funzionare.
* =grave	L'attività non può continuare ma il componente, l'applicazione e il server possono ancora funzionare. Questo livello può anche indicare un errore irreversibile imminente.
* =avvertenza	Errore potenziale o imminente. Questo livello può anche indicare un errore progressivo (ad esempio, la potenziale perdita di risorse).
* =controllo	Evento significativo che influisce sullo stato del server o sulle risorse
* =info	Informazioni generali che delineano l'andamento complessivo delle attività
* =config	Modifica della configurazione o stato
* =dettaglio	Informazioni generali sull'avanzamento dell'attività secondaria
* =fine	Informazioni di traccia - Traccia generale + valori di entrata, uscita e ritorno del metodo
* =più fine	Informazioni di traccia - Traccia dettagliata
* =migliore	Informazioni di traccia - Una traccia più dettagliata che include tutti i dettagli necessari per il debug dei problemi
* =tutti	Tutti gli eventi vengono registrati

Configurazione del token LTPA

I token LTPA possono essere utilizzati per evitare che un utente fornisca credenziali nome utente e password su ogni richiesta al server mqweb. È possibile configurare il nome del cookie del token LTPA, l'intervallo di scadenza per i token di autenticazione LTPA e configurare se i token LTPA possono essere utilizzati dalle connessioni HTTP, utilizzando il comando **setmqweb** .

Prima di iniziare

Per completare questa attività, è necessario essere un utente con determinati privilegi in modo da poter utilizzare i comandi **dspmqweb** e **setmqweb**:

- z/OS Su z/OS, è necessario disporre dell'autorità per eseguire i comandi **dspmqweb** e **setmqweb** e l'accesso in scrittura al file `mqwebuser.xml`.
- Multi Su tutti gli altri sistemi operativi, è necessario essere un utente privilegiato.

Nota: Se si utilizza sia l'autenticazione IBM MQ Console, sia l'autenticazione token con REST API, l'intervallo di scadenza viene condiviso.

Attenzione: z/OS V 9.1.0

Prima di immettere i comandi **setmqweb** o **dspmqweb** in z/OS, è necessario impostare la variabile di ambiente WLP_USER_DIR, in modo che la variabile punti alla configurazione del server mqweb.

Per eseguire questa operazione, immettere il seguente comando:

```
export WLP_USER_DIR=WLP_user_directory
```

dove *WLP_user_directory* è il nome della directory passata a `crtmqweb`. Ad esempio:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Per ulteriori informazioni, consultare Creazione del server mqweb.

Informazioni su questa attività

Quando gli utenti accedono a IBM MQ Console, viene generato un token LTPA. Se si utilizza l'autenticazione basata su token con REST API, un token LTPA viene generato quando l'utente accede utilizzando la risorsa `/login` REST API con il metodo HTTP POST. Questo token viene restituito in un cookie. Il token viene utilizzato per autenticare l'utente senza che all'utente venga richiesto di collegarsi di nuovo con il relativo ID utente e password, fino alla scadenza del token. L'intervallo di scadenza predefinito è 120 minuti.

Il nome del cookie che include il token LTPA varia in base alla piattaforma:

- MQ Appliance Su IBM MQ Appliance, il token LTPA è `LtpaToken2`. Questo valore non può essere modificato.
- ULW z/OS Per impostazione predefinita, su tutte le altre piattaforme, il nome del cookie che include il token LTPA inizia con `LtpaToken2`e include un suffisso che può cambiare quando viene riavviato il server mqweb. Questo nome cookie casuale consente l'esecuzione di più di un server mqweb sullo stesso sistema. Tuttavia, se si desidera che il nome cookie rimanga un valore congruente, è possibile specificare il nome che il cookie ha utilizzando il comando **setmqweb** .

ULW z/OS IBM i Se si abilitano entrambe le porte HTTP e HTTPS, un token LTPA emesso per una richiesta HTTPS può essere riutilizzato per una richiesta HTTP. Questo comportamento è disabilitato per impostazione predefinita, ma è possibile abilitarlo utilizzando il comando **setmqweb** .

Procedura

- Visualizzare la scadenza corrente del token LTPA, il nome del cookie del token LTPA e se il token LTPA può essere utilizzato per le richieste HTTP utilizzando il seguente comando:

  ```
  dspmqweb properties -a
  ```

  – Il campo `ltpaCookieName` mostra il nome del cookie del token LTPA. Se non è stato impostato un nome cookie, il valore di questa proprietà è `LtpaToken2_${env.MQWEB_LTPA_SUFFIX}` on UNIX, Linux, and Windows o `LtpaToken2_${httpsPort}` on z/OS, . La variabile dopo il prefisso `LtpaToken2_` viene utilizzata dal server mqweb per generare un nome univoco per il cookie. Non

è possibile impostare questa variabile, ma è possibile modificare `ltpaCookieName` in un valore di propria scelta.
  - Il campo `ltpaExpiration` mostra la scadenza del token LTPA.
  - Il campo `secureLtpa` è impostato su `false` se i token LTPA possono essere utilizzati dalle richieste HTTP.

  Per ulteriori informazioni, vedere dspmqweb.
- Configurare la scadenza del token LTPA:
  - Impostare la scadenza del token LTPA immettendo il seguente comando:

    ```
    setmqweb properties -k ltpaExpiration -v time
    ```

    dove *time* specifica l'ora, in minuti, prima della scadenza del token LTPA e della disconnessione dell'utente.
  - Reimpostare la scadenza del token LTPA sul valore predefinito di 120 minuti immettendo il seguente comando:

    ```
    setmqweb properties -k ltpaExpiration -d
    ```
- ULW z/OS

  Configurare il nome cookie del token LTPA:
  - Impostare il nome del cookie del token LTPA immettendo il seguente comando:

    ```
    setmqweb properties -k ltpaCookieName -v name
    ```

    dove *name* specifica un nome univoco per il cookie del token LTPA.
  - Reimpostare il nome del cookie del token LTPA sul valore predefinito, dove un prefisso di `LtpaToken2_` è seguito da caratteri casuali, immettendo il seguente comando:

    ```
    setmqweb properties -k ltpaCookieName -d
    ```
- ULW z/OS

  Configurare se il token LTPA può essere utilizzato dalle connessioni HTTP immettendo il seguente comando:

  ```
  setmqweb properties -k secureLtpa -v secure
  ```

  dove *secure* specifica se il token LTPA può essere utilizzato sia da connessioni HTTP non sicure che da connessioni HTTPS sicure. Il valore `false` consente alle connessioni HTTP e HTTPS di utilizzare lo stesso token LTPA.

V 9.1.0 Configurazione del gateway administrative REST API

Per impostazione predefinita, il gateway administrative REST API è abilitato. Quando il gateway administrative REST API è abilitato, è possibile eseguire la gestione remota con il REST API utilizzando un gestore code gateway. È possibile configurare il gestore code utilizzato come gestore code del gateway predefinito oppure è possibile impedire la gestione remota disabilitando il gateway administrative REST API utilizzando il comando **setmqweb** .

Informazioni su questa attività

Per completare questa attività, è necessario essere un utente con determinati privilegi in modo da poter utilizzare i comandi **dspmqweb** e **setmqweb**:

- z/OS Su z/OS, è necessario disporre dell'autorità per eseguire i comandi **dspmqweb** e **setmqweb** e l'accesso in scrittura al file `mqwebuser.xml`.
- Multi Su tutti gli altri sistemi operativi, è necessario essere un utente privilegiato.

Il gestore code del gateway predefinito viene utilizzato quando si verificano entrambe le seguenti condizioni:

- Un gestore code non è stato specificato nell'intestazione `ibm-mq-rest-gateway-qmgr` di una richiesta REST.
- Il gestore code specificato nell'URL della risorsa REST API non è un gestore code locale.

Per ulteriori informazioni sulla gestione remota con REST API, consultare Gestione remota utilizzando REST API.

Attenzione: z/OS V 9.1.0

Prima di immettere i comandi **setmqweb** o **dspmqweb** in z/OS, è necessario impostare la variabile di ambiente WLP_USER_DIR, in modo che la variabile punti alla configurazione del server mqweb.

Per eseguire questa operazione, immettere il seguente comando:

```
export WLP_USER_DIR=WLP_user_directory
```

dove *WLP_user_directory* è il nome della directory passata a `crtmqweb`. Ad esempio:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Per ulteriori informazioni, consultare Creazione del server mqweb.

Procedura

- Visualizzare la configurazione corrente del gateway administrative REST API utilizzando il comando seguente:

  ```
  dspmqweb properties -a
  ```

  Il campo `mqRestGatewayEnabled` mostra se il gateway è abilitato e il campo `mqRestGatewayQmgr` mostra il nome del gestore code del gateway predefinito. Per ulteriori informazioni, vedere dspmqweb.
- Configurare se il gateway administrative REST API è abilitato utilizzando il seguente comando:

  ```
  setmqweb properties -k mqRestGatewayEnabled -v enabled
  ```

  dove *enabled* è il valore **true** per abilitare il gateway administrative REST API o **false** in caso contrario.
- Configurare il gestore code utilizzato come gestore code del gateway predefinito:
  - Impostare il gestore code del gateway predefinito utilizzando il seguente comando:

    ```
    setmqweb properties -k mqRestGatewayQmgr -v qmgrName
    ```

    dove *qmgrName* è il nome di un gestore code nella stessa installazione del server mqweb.
  - Annullare l'impostazione del gestore code gateway predefinito utilizzando il seguente comando:

    ```
    setmqweb properties -k mqRestGatewayQmgr -d
    ```

V 9.1.0 Configurazione di messaging REST API

Per impostazione predefinita, il server mqweb che ospita IBM MQ Console e REST API ha il messaging REST API abilitato. Le V 9.1.2 connessioni a IBM MQ da messaging REST API sono raggruppate in pool, con 20 connessioni disponibili per ciascun gestore code. Quando tutte le connessioni sono in utilizzo, messaging REST API crea una nuova connessione non in pool da utilizzare per la richiesta. È possibile modificare il numero massimo di connessioni in pool e il comportamento di messaging REST API quando tutte le connessione sono utilizzate utilizzando il comando **setmqweb properties** . È possibile anche configurare se la messaggistica è abilitata utilizzando il comando **setmqweb properties** .

Prima di iniziare

Per completare questa attività, è necessario essere un utente con determinati privilegi in modo da poter utilizzare i comandi **dspmqweb** e **setmqweb**:

- z/OS Su z/OS, è necessario disporre dell'autorità per eseguire i comandi **dspmqweb** e **setmqweb** e l'accesso in scrittura al file `mqwebuser.xml`.
- Multi Su tutti gli altri sistemi operativi, è necessario essere un utente privilegiato.

Per utilizzare messaging REST API , il chiamante deve essere autenticato sul server mqweb e deve essere un membro del ruolo `MQWebUser` . I ruoli `MQWebAdmin` e `MQWebAdminRO` non sono applicabili per messaging REST API. Il chiamante deve anche essere autorizzato ad accedere alle code utilizzate per la messaggistica tramite OAM oRACF. Per ulteriori informazioni sulla sicurezza di REST API, consultare Sicurezza di IBM MQ Console e REST API.

Attenzione: z/OS V 9.1.0

Prima di immettere i comandi **setmqweb** o **dspmqweb** in z/OS, è necessario impostare la variabile di ambiente WLP_USER_DIR, in modo che la variabile punti alla configurazione del server mqweb.

Per eseguire questa operazione, immettere il seguente comando:

```
export WLP_USER_DIR=WLP_user_directory
```

dove *WLP_user_directory* è il nome della directory passata a `crtmqweb`. Ad esempio:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Per ulteriori informazioni, consultare Creazione del server mqweb.

Informazioni su questa attività

È possibile configurare se la messaggistica è abilitata utilizzando il comando **setmqweb properties** .

V 9.1.2 Per ottimizzare le prestazioni di messaging REST API, le connessioni ai gestori code IBM MQ vengono raggruppate in pool. In altre parole, invece di ogni richiesta REST che crea, utilizza e distrugge la connessione, ogni richiesta REST utilizza una connessione da un pool di connessione. Per impostazione predefinita, sono disponibili 20 connessioni per ciascun pool di gestori code e sono disponibili tre opzioni per la gestione delle richieste quando tutte le connessioni sono in uso:

- messaging REST API può creare una nuova connessione non in pool da utilizzare per la richiesta. Questo è il comportamento predefinito.
- messaging REST API può restituire un errore.
- messaging REST API può attendere che una connessione in pool diventi disponibile. Questa attesa è un'attesa indefinita.

È possibile modificare il numero massimo di connessioni in pool e il comportamento predefinito di messaging REST API quando tutte le connessioni vengono utilizzate utilizzando il comando **setmqweb properties** .

Procedura

- Visualizzare la configurazione corrente di HTTP messaging REST API utilizzando il seguente comando:

  ```
  dspmqweb properties -a
  ```

  Il campo `mqRestMessagingEnabled` mostra se il messaging REST API è abilitato. Il valore è `True` se messaging REST API è abilitato o `False` in caso contrario. Per ulteriori informazioni, vedere dspmqweb.
- Configurare messaging REST API utilizzando il seguente comando:

  ```
  setmqweb properties -k mqRestMessagingEnabled -v enabled
  ```

  dove *enabled* è il valore `true` se si desidera che messaging REST API sia abilitato o `false` in caso contrario.

- V 9.1.2
  Configurare il pool di connessioni per messaging REST API:
  - Configurare la dimensione massima del lotto connessioni per ciascun lotto gestori code utilizzando il seguente comando:

    ```
    setmqweb properties -k mqRestMessagingMaxPoolSize -v size
    ```

    dove *size* specifica la dimensione del pool.

    Nota: Se è stato impostato un valore elevato per *mqRestMessagingMaxPoolSize* e si sta connettendo a un numero elevato di gestori code, si consiglia di aumentare la dimensione massima dell'heap del server mqweb.

    Per ulteriori informazioni, consultare Ottimizzazione della JVM del server mqweb .
  - Configurare il funzionamento di messaging REST API quando tutte le connessioni nel lotto sono in uso utilizzando il seguente comando:

    ```
    setmqweb properties -k mqRestMessagingFullPoolBehavior -v action
    ```

    dove *action* specifica l'azione da intraprendere. *action* può essere uno dei seguenti valori:

    blocco
    Quando tutte le connessioni nel pool sono in uso, attendere che una connessione diventi disponibile.

    errore
    Quando tutte le connessioni nel pool sono in uso, restituire un errore.

    in eccesso
    Quando tutte le connessioni nel pool sono in uso, creare una connessione non in pool da utilizzare ed eliminare la connessione dopo che è stata utilizzata.

V 9.1.0 Configurazione di REST API per MFT

LTS Per impostazione predefinita, il server mqweb che ospita i servizi IBM MQ Console e REST non ha MFT abilitato. È possibile configurare se REST API per MFT è abilitato, impostare il gestore code di coordinamento e specificare il timeout di riconnessione MFT utilizzando il comando **setmqweb properties** . V 9.1.2 Per un comando di creazione REST API come **Create transfer** è necessario aggiungere `mqRestMftCommandQmgr`. CD V 9.1.4 Per impostazione predefinita, il server mqweb che ospita i servizi IBM MQ Console e REST non dispone di MFT abilitato.

Prima di iniziare

V 9.1.4 Ti serve:

- Per esercitare i servizi REST di MFT , devi abilitare il servizio REST MFT impostando **mqRestMftEnabled** su *true* e impostare anche il nome del gestore code comandi su `mqRestMftCoordinationQmgr`:

  ```
  setmqweb properties -k mqRestMftEnabled -v true
  setmqweb properties -k mqRestMftCoordinationQmgr -v <coordinationQmgrName>
  ```

- Per inoltrare qualsiasi richiesta di creazione, ad esempio per creare il trasferimento o il monitoraggio delle risorse, è necessario impostare `mqRestMftCommandQmgr`

  ```
  setmqweb properties -k mqRestMftCommandQmgr -v <commandQmgrName>
  ```

- Riavviare il server mqweb per applicare i valori appena impostati immettendo il comando **endmqweb** seguito dal comando **strmqweb** .

- Verificare lo stato del server Web immettendo il comando **dspmqweb** .

Per completare questa attività, è necessario essere un utente con determinati privilegi in modo da poter utilizzare i comandi **dspmqweb** e **setmqweb**:

- z/OS Su z/OS, è necessario disporre dell'autorità per eseguire i comandi **dspmqweb** e **setmqweb** e l'accesso in scrittura al file `mqwebuser.xml`.
- Multi Su tutti gli altri sistemi operativi, è necessario essere un utente privilegiato.

Per utilizzare REST API per MFT, il chiamante deve essere autenticato sul server mqweb e deve essere membro di uno o più ruoli `MFTWebAdmino` `MFTWebAdminRO` .

Attenzione: z/OS V 9.1.0

Prima di immettere i comandi **setmqweb** o **dspmqweb** in z/OS, è necessario impostare la variabile di ambiente WLP_USER_DIR, in modo che la variabile punti alla configurazione del server mqweb.

Per eseguire questa operazione, immettere il seguente comando:

```
export WLP_USER_DIR=WLP_user_directory
```

dove *WLP_user_directory* è il nome della directory passata a `crtmqweb`. Ad esempio:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Per ulteriori informazioni, consultare Creazione del server mqweb.

Informazioni su questa attività

Quando si configura il timeout REST API per MFT , notare che il primo tentativo di ristabilire la connessione viene effettuato immediatamente dopo che la connessione al gestore code di coordinamento è stata interrotta. Se non riesce, c'è un intervallo di cinque minuti tra ogni tentativo di riconnessione. Pertanto, l'impostazione di un valore compreso tra 0 e 5 determina un solo tentativo di riconnessione.

Dopo il timeout della riconnessione, viene effettuato il successivo tentativo di riconnessione quando viene richiamata una delle risorse REST API per MFT . Se questo tentativo di riconnessione ha esito negativo, MFT tenta nuovamente di riconnettersi ogni cinque minuti fino a quando non è trascorso il timeout di riconnessione.

Procedura

- Visualizza la configurazione corrente di REST API per MFT utilizzando il seguente comando:

  `dspmqweb properties -a`

  Il campo `mqRestMftEnabled` mostra se REST API per MFT è abilitato. Il valore è `True` se messaging REST API è abilitato o `False` in caso contrario.

  Il campo `mqRestMftCoordinationQmgr` mostra il nome del gestore code di coordinamento.

  V 9.1.2 Il campo `mqRestMftCommandQmgr` mostra il nome del gestore code comandi.

  Il campo `mqRestMftReconnectTimeoutInMinutes` mostra il valore di timeout della riconnessione, fino a quando i servizi REST di trasferimento MFT non smettono di tentare la connessione al gestore code di coordinamento. Per ulteriori informazioni, vedere dspmqweb.
- Configurare se REST API per MFT è abilitato:
  a) Configurare se REST API per MFT è abilitato immettendo il seguente comando:

     `setmqweb properties -k mqRestMftEnabled -v value`

     dove *valore* è `true` se si desidera che REST API per MFT sia abilitato o `false` in caso contrario.
  b) Riavviare il server mqweb immettendo i seguenti comandi:

```
endmqweb
strmqweb
```

- Configurare il gestore code di coordinamento da cui vengono richiamati i dettagli di trasferimento:
  a) Configurare il gestore code di coordinamento utilizzando il seguente comando:

     `setmqweb properties -k mqRestMftCoordinationQmgr -v qmgrName`

     dove *qmgrName* è il nome del gestore code di coordinamento. Il gestore code di coordinamento deve trovarsi sulla macchina su cui è in esecuzione il server mqweb. Per default, questo nome del gestore code è vuoto. Se un valore non è impostato, il REST API per MFT non funziona.
  b) Riavviare il server mqweb immettendo i seguenti comandi:

```
endmqweb
strmqweb
```

- Configurare il timeout, in minuti, dopo il quale REST API per MFT interrompe il tentativo di connessione al gestore code di coordinamento:
  a) Configurare il timeout utilizzando uno dei seguenti comandi:
     – Impostare il timeout:

       `setmqweb properties -k mqRestMftReconnectTimeoutInMinutes -v time`

       dove *time* specifica il tempo, in minuti, prima che si verifichi il timeout.

       Se questo valore è impostato tra `0-5`, REST API per MFT tenta di riconnettersi al gestore code di coordinamento solo una volta. Se la connessione non riesce, non ci sono tentativi di ristabilire la connessione fino a quando non viene richiamato REST API .

       Se questo valore è impostato su `-1`, REST API per MFT tenta di riconnettersi fino a quando la connessione non viene eseguita correttamente.
     – Reimpostare il timeout sul valore predefinito di 30 minuti:

       `setmqweb properties -k mqRestMftReconnectTimeoutInMinutes -d`
  b) Riavviare il server mqweb immettendo i seguenti comandi:

```
endmqweb
strmqweb
```

- V 9.1.2 Configurare il gestore code comandi per una richiesta di creazione:
  a) Configurare il gestore code comandi utilizzando il comando seguente:

     `setmqweb properties -k mqRestMftCommandQmgr -v qmgrName`

     dove *qmgrName* è il nome del gestore code comandi. Il gestore code comandi deve trovarsi sulla macchina su cui è in esecuzione il server mqweb. Per default, questo nome del gestore code è vuoto. Se un valore non è impostato, il MFT REST API per un comando di creazione non funziona.
  b) Riavviare il server mqweb immettendo i seguenti comandi:

```
endmqweb
strmqweb
```

V 9.1.0 Ottimizzazione della JVM del server mqweb

Per impostazione predefinita, la JVM (Java virtual machine) del server mqweb utilizza valori predefiniti specifici della piattaforma per parametri di configurazione quali la dimensione minima e massima dell'heap e la dimensione della cache delle classi.

Informazioni su questa attività

Potrebbe essere necessario modificare i valori predefiniti per migliorare le prestazioni o per risolvere i problemi. Ad esempio, se `java.lang.OutOfMemoryError` viene generato dal server mqweb, è necessario aumentare la dimensione massima dell'heap. È inoltre necessario aumentare la dimensione dell'heap se si sta tentando di caricare un numero elevato di oggetti coda.

Se si verificano problemi con la visualizzazione delle informazioni di configurazione del dashboard in IBM MQ Console, è necessario impostare una variabile che determina la codifica file della configurazione.

È possibile modificare i valori predefiniti nel file `jvm.options` .

Procedura

1. Aprire il file `jvm.options`.

   Il file `jvm.options` può essere trovato in una delle seguenti directory:

   - 

Su UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - 

Su z/OS: *WLP_user_directory*`/servers/mqweb`

     dove *WLP_user_directory* è la directory specificata quando è stato eseguito lo script **crtmqweb** per creare la definizione del server mqweb.
2. Opzionale: Impostare la dimensione heap massima aggiungendo la seguente linea al file:

   ```
   -Xmx MaxSize m
   ```

   Dove *MaxSize* specifica la dimensione massima dell'heap, in MB.

   Ad esempio, la seguente riga imposta la dimensione heap massima su 1GB:

   ```
   -Xmx1024m
   ```
3. Opzionale: Impostare la dimensione heap minima aggiungendo la riga seguente al file:

   ```
   -Xms MinSize m
   ```

   Dove *MinSize* specifica la dimensione minima dell'heap, in MB. L'aumento della dimensione heap minima dal valore predefinito può ridurre il tempo impiegato per avviare il server mqweb.

   Ad esempio, la seguente riga imposta la dimensione heap minima su 512MB:

   ```
   -Xms512m
   ```
4. Opzionale: Impostare la dimensione della cache di classi aggiungendo la seguente riga al file:

   ```
   -Xscmx Size m
   ```

   Dove *Dimensione* specifica la dimensione della cache delle classi, in MB.

   Ad esempio, la seguente riga imposta la dimensione della cache di classi su 100MB: :

   ```
   -Xscmx100m
   ```

   La cache delle classi condivisa Java è utilizzata per memorizzare i dati come le classi caricate e il codice AOT (Ahead - Of - Time) compilato.

   La cache delle classi riduce significativamente il tempo impiegato per avviare il server mqweb. La prima volta che il server mqweb viene avviato, viene creata la cache delle classi e il server può impiegare un tempo significativo per l'avvio. I riavvii successivi del server saranno molto più rapidi poiché le classi possono essere caricate dalla cache di classi condivisa.

   L'aumento della dimensione della cache delle classi rispetto al valore predefinito può ridurre il tempo impiegato per avviare il server mqweb.

z/OS La cache delle classi viene ricreata quando il server mqweb viene avviato su un altro sistema z/OS . Pertanto, l'avvio del server mqweb su un altro sistema z/OS in un sysplex può richiedere molto più tempo rispetto al riavvio del server sullo stesso sistema.

Notare che le modifiche a questo valore diventano effettive solo quando viene creata la cache delle classi. La cache delle classi viene creata quando il server mqweb viene avviato per la prima volta o dopo che la cache delle classi è stata eliminata utilizzando il programma di utilità della cache delle classi Java .

5. Opzionale: Impostare la codifica del file utilizzata per le informazioni di configurazione del dashboard utente in IBM MQ Console aggiungendo la riga seguente al file:

```
-Dfile.encoding=UTF-8
```

6. Riavviare il server mqweb.

z/OS Su z/OS, arrestare e riavviare l'attività avviata del server mqweb.

Multi Su tutte le altre piatteforme, immettere i seguenti comandi sulla riga comandi:

```
endmqweb
strmqweb
```

Struttura del file del componente di installazione IBM MQ Console e REST API

Ci sono due serie di strutture di directory associate al componente di installazione IBM MQ Console e REST API . Una struttura di directory contiene file che è possibile modificare. L'altra struttura di directory contiene file che non possono essere modificati.

File modificabili

I file modificabili dall'utente sono disposti come parte dell'installazione iniziale del componente di installazione IBM MQ Console e REST API . Poiché questi file possono essere modificati, non vengono modificati quando viene applicata la manutenzione.

L'ubicazione dei file modificabili dall'utente dipende dal tipo di sistema operativo:

- ULW Su UNIX, Linux, and Windows: *MQ_DATA_PATH*/web/installations/*installationName*/
- IBM i Su IBM i: *MQ_DATA_PATH*/web/installations/Installation1/
- z/OS Su z/OS: *WLP_user_directory*

  dove *WLP_user_directory* è la directory specificata quando è stato eseguito lo script V 9.1.0 **crtmqweb** per creare la definizione del server mqweb.

In questa directory di primo livello, sono presenti le seguenti directory e file:

Directory e file	Descrizione
angular.persistence/	Directory in cui è memorizzata la configurazione del dashboard IBM MQ Console .
servers/	Directory dei server del profilo WebSphere Liberty .
servers/mqweb	Directory che contiene la struttura di directory del server mqweb.
servers/mqweb/logs	Directory che contiene i log per il server mqweb.

Directory e file	Descrizione
`servers/mqweb/logs/console.log`	Log dello stato del server di base e dei messaggi operativi.
`servers/mqweb/logs/ffdc`	Directory di output FFDC (First Failure Data Capture).
`servers/mqweb/logs/messages.log`	Log dei messaggi di runtime dal server mqweb, inclusi IBM MQ Console e REST API. I messaggi più vecchi vengono memorizzati in file denominati `messages_`*`timestamp`*`.log`.
`servers/mqweb/logs/trace.log`	Log di traccia dal server mqweb, inclusi IBM MQ Console e REST API. La traccia precedente è memorizzata in file denominati `trace_`*`timestamp`*`.log`. Questi file esistono solo se la traccia è abilitata.
`servers/mqweb/logs/state`	Stato specifico del server.
`servers/mqweb/server.xml`	File di configurazione del server principale. Questo file è di sola lettura. Modificare il file `mqwebuser.xml` per sovrascrivere la configurazione predefinita.
`servers/mqweb/mqwebuser.xml`	File di configurazione per IBM MQ Console e REST API. Le impostazioni configurate in questo file sovrascrivono la configurazione predefinita. È necessario essere un utente privilegiato per modificare questo file.
`servers/mqweb/resources`	Directory che contiene varie risorse del server come i keystore.
`servers/mqweb/workarea`	Directory creata dal server come funziona. Questa directory viene creata dopo la prima esecuzione del server.

File non modificabili

I file non modificabili sono stabiliti come parte dell'installazione iniziale del componente di installazione IBM MQ Console e REST API . Questi file vengono aggiornati quando viene applicata la manutenzione.

L'ubicazione dei file modificabili dall'utente dipende dal tipo di sistema operativo:

- ULW Su UNIX, Linux, and Windows: *`MQ_INSTALLATION_PATH`*`/web`
- IBM i Su IBM i: *`MQ_INSTALLATION_PATH`*`/web`
- z/OS Su z/OS: *`installation_directory`*`/web/`

  dove *directory_installazione* è il percorso di installazione di IBM MQ UNIX System Services Components.

I seguenti file e struttura di directory sono presenti in questa ubicazione:

Directory e file	Descrizione
`bin/`	Directory che contiene i comandi Liberty. È necessario essere un utente privilegiato per eseguire gli script in questa directory.

Directory e file	Descrizione
mq/	Struttura di directory che contiene varie risorse IBM MQ .
mq/apps/	Directory che contiene le applicazioni IBM MQ Console e REST API .
mq/etc/	
mq/etc/mqweb.xml	File di configurazione di sola lettura per il server mqweb. Modificare il file mqwebuser.xml per apportare modifiche alla configurazione.
mq/libs	Directory che contiene le librerie condivise per l'utilizzo da parte di IBM MQ Console e REST API.
mq/samp	Directory che contiene esempi.
mq/samp/configuration	Directory che contiene file di configurazione di esempio che possono essere copiati nel file mqwebuser.xml .

z/OS V 9.1.0 Configurazione della registrazione dell'utilizzo del server mqweb su z/OS

Per determinare l'utilizzo del prodotto, il sistema z/OS registra la quantità di tempo processore utilizzato dal server mqweb che ospita IBM MQ Console e REST API. Potrebbe essere necessario configurare il server mqweb per registrare l'utilizzo rispetto all'ID prodotto corretto.

Prima di iniziare

Per completare questa procedura, è necessario disporre dell'autorizzazione per smontare e montare i file system e arrestare e riavviare l'attività avviata del server mqweb.

Informazioni su questa attività

Per default, l'utilizzo del server mqweb viene registrato come un prodotto IBM MQ for z/OS autonomo, con ID prodotto 5655-MQ9. Se si dispone della licenza per utilizzare IBM MQ for z/OS Value Unit Edition (VUE)o IBM MQ Advanced for z/OS Value Unit Edition, è necessario seguire questa procedura per modificare l'ID prodotto rispetto al quale viene registrato l'utilizzo del server mqweb.

In tutti i seguenti passi, sostituire quanto segue:

- WLP_USER_DIR con il nome della directory utente Liberty inizialmente passata a **crtmqweb**, nota anche come 'USERDIR ' nella procedura JCL del server mqweb.
- PathPrefix con il nome del percorso di installazione dei componenti USS (UNIX System Services) IBM MQ for z/OS .

Procedura

1. In USS, creare una nuova directory 'mqweb_extension' nella directory WLP_USER_DIR.
   Ad esempio:

```
mkdir /var/mqm/web/installation1/mqweb_extension
```

2. Creare un file ASCII denominato mqweb.properties nella directory WLP_USER_DIR/mqweb_extension .
3. Modificare il file mqweb.properties per includere la riga:

```
com.ibm.websphere.productInstall= WLP_USER_DIR/mqweb_extension
```

Inoltre, aggiungere una delle seguenti tre righe, che fa riferimento al PID del prodotto da registrare:

```
com.ibm.websphere.productId=com.ibm.mqo
com.ibm.websphere.productId=com.ibm.mqvueo
com.ibm.websphere.productId=com.ibm.mqadv
```

4. In USS, creare la cartella `WLP_USER_DIR/mqweb_extension/lib/features/`.

   Ad esempio, utilizzare il comando USS

```
mkdir -p WLP_USER_DIR/mqweb_extension/lib/features/
```

5. In USS, creare la cartella `WLP_USER_DIR/mqweb_extension/lib/versions/`.

   Ad esempio, utilizzare il comando USS

```
mkdir -p WLP_USER_DIR/mqweb_extension/lib/versions/
```

6. Copiare uno dei seguenti file da `PathPrefix/web/mq/etc` a `WLP_USER_DIR/mqweb_extension/lib/versions`.

   Il file che è necessario copiare dipende dal tipo di prodotto che si desidera configurare per la registrazione dell'utilizzo.

   mq.properties
   L'utilizzo del server mqweb viene registrato come prodotto IBM MQ for z/OS autonomo, con ID prodotto 5655-MQ9.

   mqVue.properties
   L'utilizzo del server mqweb viene registrato come prodotto IBM MQ for z/OS Value Unit Edition (VUE) autonomo, con ID prodotto 5655-VU9.

   mqAdvancedVue.properties
   L'uso del server mqweb viene registrato come parte del prodotto IBM MQ Advanced for z/OS Value Unit Edition , con l'ID prodotto 5655-AV1.

7. Se l'utilizzo del server mqweb da registrare è per l'ID prodotto 5655-VU9 o per l'ID 5655-AV1, modificare il file delle proprietà nella directory `WLP_USER_DIR/mqweb_extension/lib/versions` .

   Eseguire questa operazione sostituendo la linea

```
com.ibm.websphere.productReplaces=com.ibm.websphere.appserver.zos
```

con riga

```
com.ibm.websphere.productReplaces=com.ibm.mq
```

8. Nella directory `WLP_USER_DIR/servers/mqweb`, modificare file `server.env` e aggiungere la seguente riga:

```
WLP_PRODUCT_EXT_DIR=WLP_USER_DIR/mqweb_extension
```

9. Modificare la proprietà e le autorizzazioni delle directory e dei file nella directory utente Liberty, in modo che appartengano all'ID utente e al gruppo con cui viene eseguito il server mqweb.

   Utilizzare i comandi:

```
chown -R userid:group WLP_USER_DIR
chmod -R 770 WLP_USER_DIR
```

10. Se il server mqweb è in esecuzione, arrestare il server utilizzando il comando MVS **STOP** sull'attività avviata del server mqweb.
11. Montare il file system dei componenti di IBM MQ for z/OS UNIX System Services per l'accesso in lettura e scrittura, utilizzando il comando **MOUNT** TSO/E con il parametro **MODE(RDWR)** .
12. Eliminare tutti i seguenti file dalla directory *PathPrefix*`/web/lib/versions` :

- `mq.properties`
- `mqVue.properties`
- `mqAdvancedVue.properties`

13. Copiare `PathPrefix/web/mq/etc/mq.properties` nella cartella `PathPrefix/web/lib/versions`.

    Questo file delle proprietà predefinito potrebbe essere sovrascritto in base al prodotto registrato, ma è obbligatorio.
14. Montare il file system IBM MQ for z/OS UNIX System Services Components per l'accesso in sola lettura utilizzando il comando TSO/E **MOUNT** con il parametro **MODE(READ)** .
15. Avviare il server mqweb utilizzando il comando MVS **START** *procname* , dove *procname* è il nome della procedura di attività avviata del server mqweb.
16. In `messages.log`, nella directory `WLP_USER_DIR/servers/mqweb/logs`, il messaggio CWWKB0108I verifica il prodotto registrato.

    Ad esempio:

```
CWWKB0108I: IBM CORP product MQM MVS/ESA version V9 R1.0 successfully registered with z/OS.
```

MQ Adv. Linux MQ Adv. VUE V 9.1.4 Definizione di una connessione Aspera gateway su Linux

IBM Aspera fasp.io Gateway fornisce un tunnel TCP/IP veloce che può aumentare in modo significativo la velocità di trasmissione di rete per IBM MQ. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux.

Informazioni su questa attività

Aspera gateway può essere utilizzato per migliorare le prestazioni dei canali del gestore code. È particolarmente efficace se la rete ha una latenza elevata o tende a perdere pacchetti ed è generalmente utilizzata per velocizzare la connessione tra gestori code in diversi data center.

Nota: Per una rete veloce che non perde pacchetti, si verifica una diminuzione delle prestazioni quando si utilizza Aspera gateway, quindi è importante controllare le prestazioni della rete prima e dopo la definizione di una connessione Aspera gateway .

Definire un Aspera gateway ad ogni estremità della connessione di rete IP, quindi utilizzare TCP/IP per connettere i canali del gestore code a ciascun gateway. Un gestore code non deve essere in esecuzione sulla stessa macchina del Aspera gateway che utilizza e più gestori code possono utilizzare lo stesso gateway. Le uniche restrizioni sono le seguenti:

Per utilizzare Aspera gateway, è necessario disporre di una o più delle seguenti titolarità:

- IBM MQ Advanced for Multiplatforms
- IBM MQ Appliance
- V 9.1.5 IBM MQ Advanced for z/OS VUE

È possibile distribuire Aspera gateway su una qualsiasi delle seguenti piattaforme Linux (Red Hat o Ubuntu):

- Linux for x86-64
- V 9.1.5 Linux on POWER Systems - Little Endian
- V 9.1.5 Linux for IBM Z

L'utilizzo di Aspera gateway è limitato ai messaggi IBM MQ a meno che il gateway non sia autorizzato separatamente.

I gestori code che utilizzano Aspera gateway possono essere in esecuzione su qualsiasi piattaforma autorizzata supportata per le release Continuous Delivery (CD). Per un elenco completo delle piattaforme CD , consultare Icone di release e piattaforma nella documentazione del prodotto.

Per ogni gestore code che non si trova sulla stessa macchina del Aspera gateway che utilizza, verificare di disporre di una connessione di rete veloce tra il gestore code e Aspera gateway.

Si utilizza un file `toml` per creare una definizione di gateway che definisce le porte in entrata e in uscita utilizzate dal gateway. Un file `toml` di esempio viene fornito con Aspera gateway. La definizione del gateway in entrata definisce la connessione dal gestore code locale al gateway e dal gateway locale a quello remoto. La definizione gateway in entrata definisce la connessione dal gateway remoto al gateway locale e dal gateway locale al gestore code locale.

La seguente procedura fornisce una guida di base per l'attività e l'esecuzione. Per informazioni più dettagliate, consultare la documentazione diIBM Aspera fasp.io Gateway V1.0.0.

Procedura

1. Ottieni l'immagine di installazione Aspera gateway .

   Se la tua azienda ha la titolarità IBM MQ Advanced for Multiplatforms o IBM MQ Appliance , puoi scaricare il Aspera gateway da Passport Advantage, come "IBM MQ V9.1.x Continuous Delivery Release for IBM Aspera fasp.io eAssembly ". Per scaricare questo eAssembly, andare a Download IBM MQ 9.1 , quindi fare clic sulla scheda per l'ultima release di fornitura continua. eAssembly contiene le immagini di installazione per tutte le piattaforme Linux su cui è disponibile il gateway.

   V 9.1.5 Se la propria azienda dispone della titolarità IBM MQ Advanced for z/OS VUE , è possibile ottenere Aspera gateway dal componente Connector Pack che fa parte dell'installazione SMP/E. Per ulteriori informazioni, consultare la directory del programma IBM MQ Advanced for z/OS VUE (IBM MQ for z/OS Program Directory PDF files). Quando Connector Pack è installato, crea una directory fasp in Unix System Services che contiene un file `.zip` . Il file `.zip` contiene le immagini di installazione per tutte le piattaforme Linux su cui è disponibile il gateway. Si noti che Aspera gateway non può essere eseguito nativamente su z/OS.
2. Copiare l'immagine di installazione Aspera gateway sulle due macchine che eseguiranno il gateway, quindi estrarre e installare il gateway.

   Installare utilizzando RPM Package Manager (RPM):

   ```
   rpm -ivh ibm-fasp.io-gateway-1.0.0_qa_48-1.x86_64.rpm
   ```

   Per installare utilizzando RPM su Ubuntu, hai due opzioni:

   - Aggiungere l'attributo `--force-debian` al comando di installazione di Aspera gateway , come descritto in Installazione di un client IBM MQ su Linux utilizzando rpm.
   - Utilizzare il comando apt - get:

     ```
     sudo apt-get install ./ibm-fasp.io-gateway_1.0.0_amd64.deb
     ```
3. Configurare ciascun gateway.

   Modificare i file `gateway.toml` e `logging.toml` nella directory `/etc/fasp.io` creata dall'installazione. Utilizzare il file `gateway.toml` per definire le porte in entrata e in uscita utilizzate dal gateway e il file `logging.toml` per definire il livello di registrazione richiesto. In questo argomento viene fornito un esempio di modifica dei file `gateway.toml` .
4. Ad ogni estremità della connessione di rete, modificare la definizione di canale per connettersi alla porta su cui è in ascolto il gateway locale.
5. Avviare ciascun servizio gateway.
   Da un prompt dei comandi, eseguire questo comando:

   ```
   systemctl start fasp.io-gateway
   ```
6. Riavviare i canali.

I gestori code stanno ora comunicando attraverso una connessione Aspera gateway .

Esempio

Questo esempio definisce una connessione Aspera gateway su due computer su cui è in esecuzione Linux. La configurazione è la seguente:

- L'indirizzo IP della macchina gateway locale è 9.20.193.107. L'indirizzo IP della macchina gateway remota è 9.20.192.115.
- Il gestore code locale è in esecuzione su una macchina con indirizzo IP 9.20.121.5. Il gestore code remoto è in esecuzione su una macchina con indirizzo IP 9.20.121.25. Entrambi i gestori code sono in ascolto sulla porta 1414.
- Il canale del gestore code sul gestore code locale viene modificato per connettersi al Aspera gateway locale utilizzando **conname** 9.20.193.107(1500). Il canale del gestore code sul gestore code remoto è stato modificato per connettersi al Aspera gateway remoto utilizzando **conname** 9.20.192.115(1500).

1. Definire una connessione Aspera gateway sulla macchina gateway locale:
   - Installare Aspera gateway:

     ```
     rpm -ivh ibm-fasp.io-gateway-1.0.0_qa_48-1.x86_64.rpm
     ```

   - Modificare il file `gateway.toml` nella directory `/etc/fasp.io` creata dall'installazione. Modificarlo per impostare le definizioni del gateway locale.

     ```
     [[bridge]]
         name = "Outbound"
         [bridge.local]
                protocol = "tcp"
                    host = "9.20.193.107"
                    port = 1500

         [bridge.forward]
                protocol = "fasp"
                    host = "9.20.192.115"
                    port = 1600

     [[bridge]]
         name = "Inbound"
         [bridge.local]
                protocol = "fasp"
                    host = "9.20.193.107"
                    port = 1600

         [bridge.forward]
                protocol = "tcp"
                    host = "9.20.121.5"
                    port = 1414
     ```

2. Ripetere il passo precedente per definire una connessione Aspera gateway sulla macchina gateway remota. Modificare il file `gateway.toml` nella directory `/etc/fasp.io` creata dall'installazione. Modificarlo per impostare le definizioni del gateway remoto:

   ```
   [[bridge]]
       name = "Outbound"
       [bridge.local]
              protocol = "tcp"
                  host = "9.20.192.115"
                  port = 1500

       [bridge.forward]
              protocol = "fasp"
                  host = "9.20.193.107"
                  port = 1600

   [[bridge]]
       name = "Inbound"
       [bridge.local]
              protocol = "fasp"
                  host = "9.20.192.115"
                  port = 1600
   ```

```
    [bridge.forward]
           protocol = "tcp"
               host = "9.20.121.25"
               port = 1414
```

3. Ad ogni estremità della connessione, modificare la definizione di canale per connettersi alla porta su cui è in ascolto il gateway locale.
   - Modificare il canale del gestore code sul gestore code locale per connettersi al Aspera gateway locale utilizzando **conname** 9.20.193.107(1500).
   - Modificare il canale del gestore code sul gestore code remoto per connettersi al Aspera gateway remoto utilizzando **conname** 9.20.192.115(1500).
4. Avviare il gateway locale immettendo il seguente comando sulla macchina del gateway locale:

```
systemctl start fasp.io-gateway
```

5. Avviare il gateway remoto eseguendo il seguente comando sulla macchina del gateway remoto:

```
systemctl start fasp.io-gateway
```

6. Riavviare i canali.

Operazioni successive

Aspera gateway trasmette i dati che riceve, senza interpretarli in alcun modo. Ciò significa che è possibile configurare TLS tra i canali del gestore code che utilizzano Aspera gateway, poiché la connessione gateway non è a conoscenza dell'handshake TLS. Ciò significa anche che i gestori code su qualsiasi piattaforma IBM MQ supportata possono utilizzare Aspera gateway.

Per utilizzare un gestore code a più istanze con un gateway, configurare le definizioni gateway per ogni istanza del gestore code.

Nota: Aspera gateway è stato testato solo con i canali del del gestore code. Non è stato testato con i canali client. Questo perché l'uso previsto per Aspera gateway è quello di connettere gestori code remoti su una rete lenta, mentre le applicazioni client in genere si connettono ai gestori code in un datacenter locale su una rete veloce.

Riferimenti correlati

Aspera gateway guida di orientamento

“Il tipo di comunicazione da utilizzare” a pagina 15
Piattaforme differenti supportano protocolli di comunicazione differenti. La scelta del protocollo di trasmissione dipende dalla combinazione di IBM MQ MQI client e delle piattaforme server.

IBM Aspera fasp.io Gateway V1.0.0 - Documentazione

Multi V 9.1.0 Configurazione IBM MQ per l'utilizzo con il IBM Cloud Private servizio di misurazione

Configurazione di IBM MQ per l'utilizzo con il servizio di misurazione IBM Cloud Private per notificare e visualizzare le informazioni di avvio e utilizzo del gestore code.

Prima di iniziare

Prima di configurare i tuoi gestori code IBM MQ per utilizzare un servizio IBM Cloud Private , devi avere un account IBM Cloud (formerly Bluemix) . Per creare il tuo account, consulta Registrati per IBM Cloud.

Informazioni su questa attività

Utilizzando il servizio di misurazioneIBM Cloud Private, puoi connettere i tuoi prodotti IBM in loco alla tua istanza del servizio in IBM Cloud Private e visualizzare tutti i prodotti registrati nella tua organizzazione in un singolo dashboard.

È possibile configurare e collegare i gestori code AIX, Linuxe Windows alla propria istanza del servizio di misurazione e visualizzare le informazioni di avvio e utilizzo. Tuttavia, su piattaforme diverse dagli ambienti Linux Container, i dati non possono essere utilizzati a supporto delle licenze di prezzo basate sui contenitori orari.

V 9.1.1 Per registrare i dati di utilizzo per un tipo di licenza VPC mensile, invece della metrica di licenza oraria predefinita, imposta la variabile di ambiente AMQ_LICENSING_METRIC=VPCMonthlyPeak. Ciò fa sì che il gestore code carichi i dati relativi ai tipi di licenze VPC mensili, invece del comportamento predefinito di caricamento dei dati relativi alle licenze orarie basate sul contenitore.

Utilizzare i seguenti attributi con la stanza `ReportingService` (precedentemente `BluemixRegistration`) nel file `qm.ini` :

APIKeyFile
Ubicazione del file di testo con il valore dell'istanza del servizio di misurazione **APIKey** .

CapacityReporting
Scrive periodicamente i messaggi di log di errori nei log AMQERR nel seguente formato:

```
4/22/2018 01:44:29 PM - Process(1274.1) User(bld-adm) Program(amqmgr0)
Host(8b3b83f2bc7d) Installation(Docker)
VRMF(9.1.0.0)
Time(2018-04-22T13:44:29.295Z)
ArithInsert1(300)
CommentInsert1(8.5)
CommentInsert2(IBM MQ Advanced)
```

Le informazioni prodotte dall'attributo **CapacityReporting** vengono inserite in un messaggio AMQ5064, che fornisce una migliore comprensione di quanto IBM MQ l'azienda sta utilizzando:

AMQ5064
Questo gestore code è stato in esecuzione per 300 secondi. Attualmente è in esecuzione con 8.5 core. Il tipo di licenza è IBM MQ Advanced.

Gravità
0: Informazioni

Spiegazione
Questo è un messaggio informativo per la traccia dell'utilizzo.

Risposta
Nessuna.

V 9.1.1 **LicensingGroup**
Il gruppo di fatturazione a cui appartiene il gestore code. Ciò influenza il modo in cui i dati vengono raggruppati nei report generati dal servizio di misurazione.

ServiceURL
L'indirizzo di servizio IBM Cloud Private .

ServiceProxy
L'URL e la porta per il proxy HTTP che possono essere utilizzati se i gestori code non hanno accesso diretto alla rete su cui è in esecuzione il servizio di misurazione.

È possibile visualizzare gli host su cui sono installati i propri prodotti, le versioni del prodotto utilizzate e le piattaforme su cui sono in esecuzione. Dalle metriche di utilizzo di alto livello che vengono visualizzate per ogni prodotto, puoi avere una panoramica di quanto sono pesanti i carichi di lavoro. Per IBM MQ, puoi vedere quali gestori code sono più utilizzati e quali hanno carichi di lavoro più leggeri.

Quando un gestore code è configurato per connettersi a un'istanza del servizio di misurazione, le seguenti informazioni sono riportate a IBM Cloud Private:

- IBM MQ Nome gestore code
- IBM MQ Identificativo gestore code
- Directory root di installazione IBM MQ

- Componenti installati IBM MQ (nome e versione)
- Nome host
- Nome sistema operativo host
- Versione sistema operativo host
- Informazioni sull'utilizzo del VPC (Virtual Processor Core) per il gestore code IBM MQ

Puoi monitorare le metriche di utilizzo del tuo VPC del gestore code nel tuo pannello di controllo dell'istanza del servizio di misurazione.

Procedura

- Configurare un gestore code da utilizzare con l'istanza del servizio di misurazione su IBM Cloud Private.
- Connettersi al servizio di misurazione IBM Cloud Private tramite proxy HTTP.
- Risolvere i problemi di connessione al servizio di misurazione di IBM Cloud Private .

Concetti correlati

Metrica dei prezzi per VPC (Virtual Processor Core)

V 9.1.1 Multi Configurazione di un gestore code per l'utilizzo con l'istanza del servizio di misurazione su IBM Cloud Private

Imposta le informazioni di sicurezza e di registrazione IBM Cloud per il tuo gestore code e connettiti all'istanza del servizio di misurazione che hai già creato.

Informazioni su questa attività

Il dashboard dell'istanza del servizio di misurazioneIBM Cloud Private mostra i dati solo per i gestori code configurati per includere la sicurezza e le informazioni di registrazione IBM Cloud Private .

Procedura

1. Attieniti alla procedura documentata ICP per creare un ID servizio in:

   Creazione di un ID servizio utilizzando la CLI IBM Cloud Private.
2. Seguire la procedura documentata ICP per creare una chiave API all'indirizzo:

   API di gestione delle chiavi API.
3. Scarica i certificati TLS dal cluster ICP.

   Prendi nota dell'ubicazione in cui hai scaricato i certificati. È possibile aggiungere i certificati scaricati al keystore per il gestore code, nel passo “9” a pagina 789.
4. Creare un file di testo `apikeyfile.txt` e aggiungere il valore **`API key`** copiato nell'attività precedente.

   Nota l'ubicazione di `apikeyfile.txt` in modo da poter includere il relativo percorso nel passo 8. Questo file deve essere leggibile dall'utente del gestore code (*'mq*' su sistemi UNIX). Il file deve contenere solo il **`API key`** stesso, non un payload JSON, ad esempio `d9c11b45-4dda-4de4-c0b2-2e4e1004dc64`
5. Creare il gestore code, ad esempio *QM1*.

   Per ulteriori informazioni, fare riferimento a Creazione e gestione di gestori code su più piattaforme.
6. Avviare il gestore code *QM1*.

   Per ulteriori informazioni, consultare Avvio di un gestore code.
7. Ricordati di impostare il tuo ambiente della riga di comando IBM MQ prima di eseguire comandi IBM MQ .

   Eseguire il comando **`setmqenv`**.

AIX Su AIX:

```
. /usr/mqm/bin/setmqenv -s
```

Linux Su Linux:

```
. /opt/mqm/bin/setmqenv -s
```

Windows Su Windows:

```
"C:\Program Files\IBM\MQ\bin\setmqenv.cmd" -n installation name
```

8. Creare un truststore SSL per il gestore code *QM1*.

AIX Inizia a creare il truststore, su AIX:Amend for AIX

```
runmqckm -keydb -create -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
-expire 30 -stash
```

Linux Su Linux:

```
runmqckm -keydb -create -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
-expire 30 -stash
```

Windows Su Windows:

```
runmqckm -keydb -create -db "MQ data directory\qmgrs\QM1\ssl\key.kdb" -pw password -type
cms -expire 30 -stash
```

9. Aggiungere i certificati digitali scaricati nel passo “3” a pagina 788al truststore del gestore code.

AIX Su AIX:

```
runmqckm -cert -add -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
-label RootCA
-file Download_location/RootCA.crt -format ascii -trust enable

runmqckm -cert -add -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
-label ServerCert
-file Download_location/CERT.crt -format ascii -trust enable
```

Linux Su Linux:

```
runmqckm -cert -add -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
-label RootCA
-file Download_location/RootCA.crt -format ascii -trust enable

runmqckm -cert -add -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
-label ServerCert
-file Download_location/CERT.crt -format ascii -trust enable
```

Windows Su Windows:

```
runmqckm -cert -add -db "MQ data directory\qmgrs\QM1\ssl\key.kdb" -pw password -type cms
-label RootCA
-file "Download_location\RootCA.crt" -format ascii -trust enable

runmqckm -cert -add -db "C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl\key.kdb" -pw password -type
cms -label ServerCert
-file "Download_location\CERT.crt" -format ascii -trust enable
```

10. Aggiungere la nuova stanza `ReportingService` con il percorso `apikeyfile` al file `qm.ini` del gestore code:

```
ReportingService:
   APIKeyFile=APIKey file location/apikeyfile.txt
```

11. Aggiungere il valore **API host** al file qm.ini .

    La sezione della stanza ReportingService contiene ora il percorso ai valori apikeyfile e **API host** (**ServiceURL**):

```
ReportingService:
   APIKeyFile=APIKey file location/apikeyfile.txt
   ServiceURL=https://productinsights-api.ng.bluemix.net
```

    Salvare e uscire da qm.ini .

12. Riavviare il gestore code per rendere effettive le modifiche.

    Potrebbe essere richiesto di concedere l'autorizzazione per il processo del gestore code **amqzmur0** per accedere alla rete. L'accesso è richiesto per abilitare il gestore code a contattare il servizio di misurazione.

13. Visualizzare informazioni sul gestore code *QM1* nell'istanza del servizio di misurazione.

    Quando lo stato di creazione report è attivo, le informazioni di avvio e utilizzo per tutti i server di integrazione sul nodo di integrazione specificato vengono riportate al servizio di misurazione. Le informazioni di utilizzo vengono aggiornate ogni 15 minuti.

14. Opzionale: Arrestare la notifica di un gestore code al servizio di misurazione, rimuovendo la sezione ReportingService dal file qm.ini del gestore code e riavviare il gestore code.

15. Opzionale: Controllare le informazioni diagnostiche nel file di log del gestore code se il gestore code non riesce a riportare le informazioni di avvio o di utilizzo al servizio di misurazione.

    Modifica per AIX

    AIX Su AIX:

```
/var/mqm/qmgrs/QM1/errors/AMQERR0*.log
```

    Linux Su Linux:

```
/var/mqm/qmgrs/QM1/errors/AMQERR0*.log
```

    Windows Su Windows:

```
C:\ProgramData\IBM\MQ\errors\AMQERR0*.log
```

Risultati

Hai creato un'istanza del servizio di misurazione e configurato il gestore code per la connessione all'istanza. È possibile visualizzare le informazioni sul gestore code nel dashboard dell'istanza del servizio di misurazione.

V 9.1.1 Multi Connessione al servizio di misurazione IBM Cloud Private tramite un proxy HTTP

Se il tuo gestore code è in esecuzione su un sistema che non ha accesso diretto al tuo cluster ICP, puoi utilizzare un proxy HTTP fornito dalla tua organizzazione per connetterti alla tua istanza del servizio di misurazione in IBM Cloud Private.

Prima di iniziare

È stata configurata la protezione, è stato aggiunto **API key** e l'URL del servizio al file qm.ini del proprio gestore code.

Informazioni su questa attività

Utilizza questa attività per configurare il tuo gestore code per la connessione all'istanza del servizio di misurazione in IBM Cloud Private tramite un proxy HTTP fornito dalla tua organizzazione.

Procedura

- Aggiungere un attributo proxy del servizio alla stanza di registrazione IBM Cloud Private del proprio file `qm.ini` .

  È possibile impostare l'attributo **ServiceProxy** come segue:

  – Un URL che include il prefisso http:// e, facoltativamente, la porta. Se non si specifica la porta, viene utilizzato *1080* .

  ```
  ReportingService:
     ServiceProxy=http://myorgproxy.net:1080
  ```

  Nota: Il parametro **ServiceProxy** deve essere impostato su un URL http:// valido. Altri protocolli proxy, ad esempio, HTTPS e SOCKS non sono supportati.
- Riavviare il gestore code prima che le modifiche diventino effettive.

V 9.1.1 Multi Risoluzione dei problemi di connessione al servizio di misurazione

Avviso di risoluzione dei problemi per gli errori che potresti riscontrare durante la connessione del tuo gestore code a un'istanza del servizio di misurazione.

Il gestore code non può registrare o caricare le metriche di utilizzo nel servizio di misurazione configurato

Verificare che il gestore code abbia accesso alla rete. Il valore **APIKey** nel file della chiave API non è corretto. Assicurarsi che il componente GSKit sia installato.

Stanza `qm.ini` non valida

È stata trovata una stanza `qm.ini` non valida. Per ulteriori informazioni, consultare il log degli errori.

Parametro proxy servizio HTTP non valido

Il valore per l'attributo **ServiceProxy** per la sezione del gestore code `ReportingService` non è configurato correttamente. Il gestore code non si registra con il servizio. Il parametro **ServiceProxy** deve essere impostato su un URL http:// valido. Altri protocolli proxy, ad esempio, HTTPS e SOCKS non sono supportati.

Linux V 9.1.0 Configurazione di IBM MQ per l'utilizzo con gli argomenti push Salesforce e gli eventi della piattaforma

Utilizzare queste informazioni per impostare la sicurezza e le connessioni a Salesforce e alla rete IBM MQ configurando e quindi eseguendo IBM MQ Bridge to Salesforce.

Prima di iniziare

Nota: Il IBM MQ Bridge to Salesforce è obsoleto in tutte le release del 22 novembre 2022 (vedi Lettera di annuncio USA 222 - 431).

- IBM MQ Bridge to Salesforce è disponibile su Linux per x86-64 (64 bit). Il bridge non è supportato per la connessione ai gestori code in esecuzione su IBM WebSphere MQ 6.0 e versioni precedenti.

- V 9.1.2 IBM MQ 9.1.2 introduce ulteriori opzioni di configurazione. La modifica principale è che un gestore code può ora supportare più istanze bridge, dove sono state configurate in modo appropriato. Consultare “Opzioni di configurazione aggiuntive per IBM MQ Bridge to Salesforce” a pagina 798 per ulteriori informazioni.
- Installare il package **MQSeriesSFBridge** . Per ulteriori informazioni, consultare Installazione del server IBM MQ su Linux.

Informazioni su questa attività

Salesforce è una piattaforma di gestione delle relazioni con i clienti basata sul cloud. Se si utilizza Salesforce per gestire le interazioni e i dati del cliente, è possibile utilizzare IBM MQ Bridge to Salesforce per sottoscrivere gli argomenti di push Salesforce e gli eventi della piattaforma che possono essere pubblicati nel gestore code IBM MQ . Le applicazioni che si connettono a tale gestore code possono utilizzare i dati evento della piattaforma e dell'argomento push, in modo utile. È anche possibile utilizzare il bridge per creare messaggi di evento per gli eventi della piattaforma in Salesforce.

Per una panoramica di IBM MQ Bridge to Salesforce, consultare il diagramma nella Figura 1.

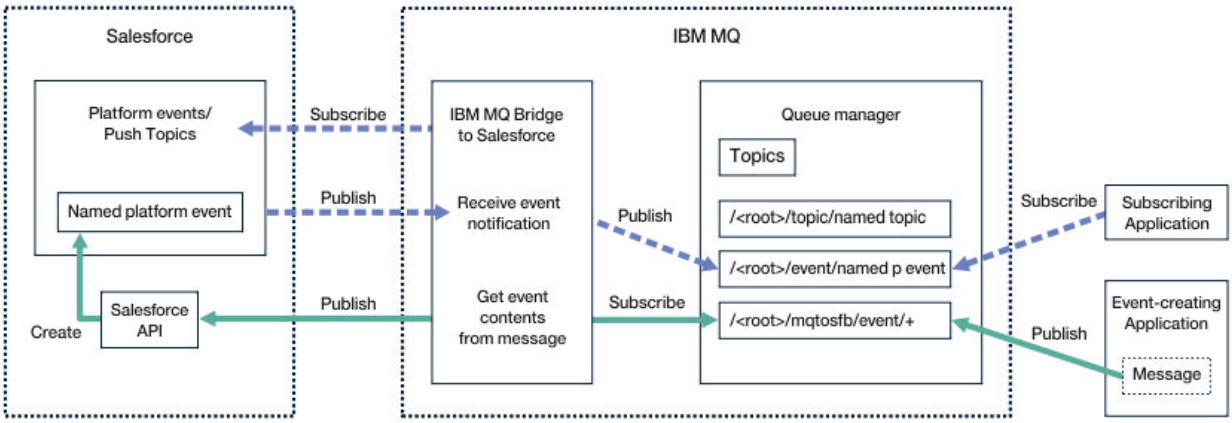


Figura 97. IBM MQ Bridge to Salesforce

Gli argomenti push sono query che definisci per utilizzare l'API `Force.com` Streaming per ricevere notifiche per le modifiche ai record in Salesforce. Per ulteriori informazioni sulla configurazione degli argomenti push e su come utilizzare l'API Streaming, vedi Introduzione all'API Streaming e Utilizzo di PushTopics.

Gli eventi della piattaforma sono messaggi di evento personalizzabili che possono essere definiti per determinare i dati di evento che la piattaforma `Force.com` produce o utilizza. Per ulteriori informazioni sugli eventi della piattaforma e la differenza tra gli eventi Salesforce , vedi Eventi della piattaforma di messaggistica aziendale e Qual è la differenza tra gli eventi Salesforce.

- Per creare la configurazione per la sottoscrizione agli argomenti di push e agli eventi della piattaforma, vedi “Configurazione di IBM MQ Bridge to Salesforce” a pagina 793.
- Per creare la configurazione per la creazione di messaggi di evento per eventi della piattaforma Salesforce , consultare “Creazione di messaggi di eventi per eventi della piattaforma Salesforce” a pagina 800.

È possibile monitorare i dati dal bridge in due modi, tramite IBM MQ Console e utilizzando il parametro **-p** con il comando **amqsrua** . Viene pubblicata una serie di dati per lo stato del bridge generale:

- Il numero totale di messaggi di argomento push elaborati in un intervallo (nella struttura ad albero `STATUS/PUSHTOPIC`).
- Numero di argomenti push visualizzati in questo intervallo.
- Il numero totale di eventi della piattaforma elaborati in un intervallo (nella struttura ad albero `STATUS/PLATFORM`).

- Numero di eventi della piattaforma visualizzati in questo intervallo.
- Numero totale di eventi della piattaforma IBM MQ creati elaborati in un intervallo (nella struttura ad albero STATUS/MQPE).
- Numero univoco di eventi di piattaforma creati da IBM MQ visualizzati in questo intervallo.
- Numero non riuscito di pubblicazioni di IBM MQ eventi di piattaforma creati visualizzati in questo intervallo.

Per ogni argomento Salesforce configurato, viene pubblicato un ulteriore messaggio. L'argomento IBM MQ utilizza il nome completo dell'argomento Salesforce e `/event` o `/topic` nel nome oggetto:

- Numero di messaggi elaborati in un intervallo.

Per configurare IBM MQ Console per monitorare i dati bridge, consultare i passi 9 e 10 in Configurazione di IBM MQ Bridge to Salesforce. Per informazioni sull'utilizzo del comando **amqsrua** , consultare Monitoraggio di IBM MQ Bridge to Salesforce.

Seguire i passi in queste attività per configurare ed eseguire IBM MQ Bridge to Salesforce:

Procedura

1. Configurae IBM MQ Bridge to Salesforce.
2. V 9.1.0
   Creare messaggi di evento per gli eventi della piattaforma Salesforce .
3. Eseguire IBM MQ Bridge to Salesforce.

Attività correlate

Traccia di IBM MQ Bridge to Salesforce

Riferimenti correlati

runmqsfb (eseguire IBM MQ Bridge to Salesforce)

Linux V 9.1.0 Configurazione di IBM MQ Bridge to Salesforce

Puoi configurare IBM MQ e immettere i parametri IBM MQ Bridge to Salesforce per creare il file di configurazione e collegare gli argomenti di push Salesforce e gli eventi della piattaforma al tuo gestore code IBM MQ .

Prima di iniziare

Prima di iniziare questa attività, assicurarsi di aver installato il package `MQSeriesSFBridge` nell'installazione di IBM MQ su una piattaforma x86-64 Linux .

Informazioni su questa attività

Questa attività ti guida attraverso la configurazione minima necessaria per creare il file di configurazione IBM MQ Bridge to Salesforce e collegarti correttamente a Salesforce e IBM MQ in modo da poter sottoscrivere gli argomenti di push Salesforce e gli eventi della piattaforma. Per ulteriori informazioni sul significato e sulle opzioni per tutti i parametri, consultare il comando runmqsfb . È necessario considerare i propri requisiti di sicurezza e personalizzare i parametri appropriati per la propria distribuzione.

Per creare la configurazione per la creazione di messaggi di evento per eventi della piattaforma Salesforce , consultare “Creazione di messaggi di eventi per eventi della piattaforma Salesforce” a pagina 800.

Sottoscrizione agli argomenti di push e agli eventi della piattaforma Salesforce

Quando IBM MQ Bridge to Salesforce stabilisce connessioni sia a Salesforce che a IBM MQ, crea sottoscrizioni agli argomenti di push Salesforce e agli eventi della piattaforma. Il nome dell'evento della piattaforma o dell'argomento push a cui il bridge desidera sottoscrivere deve essere incluso nel file di configurazione o aggiunto nella riga comandi prima che venga effettuata la connessione.

Uno degli attributi di configurazione è la root della struttura ad albero degli argomenti IBM MQ e gli eventi vengono pubblicati sotto questa root. Il bridge accede a questa root e aggiunge il nome dell'argomento Salesforce completo, ad esempio `/MQ/SF/ROOT/topic/EscalatedCases`. L'argomento di monitoraggio e le applicazioni che si collegano a IBM MQ potrebbero cercare gli argomenti di push in `/topic/EscalatedCases` e gli eventi della piattaforma in `/event/NewCustomer__e`.

Il messaggio pubblicato contiene le informazioni di controllo e la struttura dati che contiene i campi di dati richiesti. Per gli argomenti push, la struttura dati è un **sobject** e per gli eventi della piattaforma, la struttura è **payload**. Il bridge non può sottoscrivere un argomento o un evento se non sono definiti in Salesforce. Se il bridge rileva un errore quando tenta di sottoscrivere un argomento, il bridge si arresta.

Non è necessario definire un oggetto argomento in IBM MQ , ma devono esistere autorizzazioni appropriate, in base all'elemento parent più vicino nella struttura ad albero. Per impostazione predefinita, il messaggio ripubblicato contiene solo la struttura dati pertinente dal messaggio originale. Le informazioni di controllo vengono rimosse. Per gli eventi della piattaforma, la pubblicazione ha una struttura di payload. L'opzione di configurazione **Publish control data with the payload** nella serie di parametri **Comportamento del programma bridge** consente la ripubblicazione dell'intero messaggio, inclusi i dati di controllo. Per ulteriori informazioni, consultare Parametri di configurazione.

Ogni argomento push e evento della piattaforma ha un *ReplayID* associato alla pubblicazione da Salesforce. Il *ReplayID* può essere utilizzato per richiedere il punto di partenza per la pubblicazione quando viene stabilita la connessione al server. Salesforce conserva una cronologia per un massimo di 24 ore e consente al bridge di non perdere gli argomenti di push recenti e gli eventi della piattaforma anche se non è stato avviato al momento della loro generazione. Il ponte supporta due modalità QoS (quality of service):

Al massimo una volta
: Il ponte non utilizza *ReplayId* per il riavvio. Dopo il riavvio del bridge, vengono elaborati solo gli argomenti push e gli eventi della piattaforma appena generati. Le domande devono essere preparate per trattare le pubblicazioni mancanti. Il *ReplayId* è ancora tracciato dal bridge e forzato su una coda, in modo che il bridge possa essere riavviato con l'altra qualità del servizio e conoscere lo stato corrente.

Almeno una volta
: *ReplayId* viene tracciato dal bridge e forzato su una coda. Al riavvio del bridge, il *ReplayId* persistente viene utilizzato per richiedere il punto di partenza per le pubblicazioni dal server. A condizione che il divario non fosse superiore a 24 ore, vengono inviate le pubblicazioni più vecchie. Il *ReplayId* per un argomento non è forzato su ogni messaggio. Viene scritto in un messaggio persistente a intervalli regolari e quando il bridge viene arrestato. Le applicazioni devono essere preparate per visualizzare pubblicazioni duplicate.

ReplayId viene scritto come messaggio in una coda appena definita. È necessario definire questa coda, **SYSTEM.SALESFORCE.SYNCQ**, prima di avviare il bridge. Se **SYSTEM.SALESFORCE.SYNCQ** non esiste, il bridge non continua, indipendentemente dalla modalità QoS (quality of service). Viene fornito uno script MQSC per la creazione della coda con attributi rilevanti. La coda deve essere configurata con l'opzione `DEFSOPT (EXCL) NOSHARE` per garantire che solo una istanza del programma bridge possa aggiornare la coda **SYSTEM.SALESFORCE.SYNCQ** .

Per creare la configurazione per la creazione dei messaggi di eventi per gli eventi della piattaforma, consultare “Creazione di messaggi di eventi per eventi della piattaforma Salesforce” a pagina 800.

Procedura

1. Creare e avviare un gestore code.
   a) Creare un gestore code, ad esempio SQM1.

   ```
   crtmqm SQM1
   ```

   b) Avviare il gestore code.

   ```
   strmqm SQM1
   ```

2. **Nota:** Per utilizzare le credenziali Salesforce di accesso e di sicurezza esistenti e il certificato autofirmato, andare al passo “3” a pagina 795.

   Opzionale: Crea un token di sicurezza per il tuo account Salesforce .

   a) Esegui l'accesso al tuo account Salesforce.

   b) Crea o reimposta il tuo token di sicurezza seguendo la procedura nell'articolo della guida Salesforce help: Reimposta il tuo token di protezione.

3. Creare un certificato di protezione firmato dalla CA in Salesforce.

   a) Selezionare **Controlli di protezione** dal menu **Amministra** della **Force.com Home** page, quindi **Gestione chiavi e certificati**.

   Viene visualizzata la pagina **Gestione chiavi e certificati** .

   b) Fare clic su **Crea certificato firmato CA**.

   Viene visualizzata la pagina **Certificati** .

   c) Immettere un nome per il certificato nel campo **Etichetta** , premere Tab, quindi fare clic su **Salva**.

   Vengono visualizzate le informazioni sui dettagli chiave e certificato.

   d) Fare clic su **Torna all'elenco: Certificati e chiavi**.

   e) Fare clic su **Esporta nel keystore**.

   f) Immettere una password per il keystore, quindi fare clic su **Esporta**.

   g) Salvare il keystore esportato nel file system locale.

4. Utilizzare la GUI di IBM Key Management per aprire il keystore esportato da Salesforce e popolare i certificati del firmatario.

   a) Eseguire il comando **`strmqikm`** per aprire la GUI di IBM Key Management.

   Per ulteriori informazioni, consultare Utilizzo di runmqckm, runmqakm e strmqikm per gestire i certificati digitali.

   b) Fare clic su **Apri un file del database delle chiavi** e selezionare l'ubicazione del keystore Salesforce .

   c) Fare clic su **Apri**, assicurarsi di selezionare **JKS** dalle opzioni **Tipo di database delle chiavi** , quindi fare clic su **OK**.

   d) Immettere la password creata per il keystore nel passo 3f, quindi fare clic su **OK**.

   e) Selezionare **Certificati firmatario** dalle opzioni **Contenuto database di chiavi** .

   f) Fare clic su **Popola**.

   g) Selezionare la casella di spunta **Verisign Inc.** dall'elenco **Aggiungi certificati CA** , quindi fare clic su **OK**.

5. Opzionale: Genera la chiave consumer OAuth e il segreto creando una connessione dell'app per IBM MQ Bridge to Salesforce nell'account Salesforce .

   Hai bisogno dei codici **Chiave consumer** e **Segreto consumer** quando utilizzi IBM MQ Bridge to Salesforce negli ambienti di produzione.

   a) Selezionare **Crea**, quindi **App** dal menu **Crea** della pagina **Home Force.com** .

   Viene aperta la pagina App.

   b) Fare clic su **Nuovo** nella sezione **App connesse** .

   Viene aperta la pagina **Nuova App connessa** .

   c) Immetti un nome per il tuo IBM MQ Bridge to Salesforce in **Connected App Name**, ad esempio **MQBridgeToSalesforce**.

   d) Immetti il **Nome API**.

   Se passi al campo successivo, il **Nome applicazione connessa** viene copiato nel campo del nome **Nome API** .

   e) Immettere la propria **email di contatto**.

f) Selezionare l'opzione **Abilita impostazioni OAuth** nella sezione **API (Abilita impostazioni OAuth)** .

Vengono quindi presentate ulteriori opzioni in tale sezione.

g) Aggiungere l' **URL di callback**, ad esempio `https://www.ibm.com`.

h) Selezionare l'opzione **Accesso completo (completo)** dall'elenco **Ambiti OAuth disponibili** nella sottosezione **Ambiti OAuth selezionati** , quindi fare clic su **Aggiungi**, per aggiungere l'accesso completo all'elenco **Ambiti OAuth selezionati** .

i) Fare clic su **Salva**.

j) Fare clic su **Continua**.

k) Prendere nota dei codici **Chiave consumer** e **Segreto consumer** .

6. Creare la coda di sincronia richiesta sul gestore code.

```
cat /opt/mqm/mqsf/samp/mqsfbSyncQ.mqsc | runmqsc SQM1
```

La coda di sincronizzazione mantiene lo stato dell'evento tra i riavvii dell'applicazione o del gestore code. La grandezza della coda può essere ridotta in quanto è previsto un solo messaggio sulla coda. Solo un'istanza del bridge può essere eseguita per volta su questa coda, quindi le opzioni predefinite vengono impostate per l'accesso esclusivo.

7. Creare un file di configurazione con i parametri di connessione e sicurezza per IBM MQ, Salesforcee il funzionamento di IBM MQ Bridge to Salesforce .

```
runmqsfb -o new_config.cfg
```

I valori esistenti vengono visualizzati all'interno delle parentesi. Premere `Enter` per accettare i valori esistenti, premere `Space` quindi `Enter` per cancellare i valori e, immettere, quindi `Enter` per aggiungere nuovi valori.

a) Immettere i valori per la connessione al gestore code SQM1:

I valori minimi necessari per la connessione sono il nome gestore code, la root dell'argomento di base IBM MQ e il nome canale.

```
Connection to Queue Manager
---------------------------
Queue Manager or JNDI CF   : []SQM1
MQ Base Topic              : []/sf
MQ Channel                 : []A channel you have defined or for example
SYSTEM.DEF.SVRCONN
MQ Conname                 : []
MQ Publication Error Queue : [SYSTEM.SALESFORCE.ERRORQ]
MQ CCDT URL                : []
JNDI implementation class  : [com.sun.jndi.fscontext.RefFSContextFactory]
JNDI provider URL          : []
MQ Userid                  : []
MQ Password                : []
```

Nota: Il nome del canale non è richiesto se ci si connette localmente. Non è necessario fornire il nome del gestore code e l'argomento di base nel file di configurazione poiché possono essere inclusi sulla riga comandi in un secondo momento, quando si esegue il bridge.

b) Immettere i valori per la connessione a Salesforce:

I valori minimi necessari per la connessione sono ID utente, password, token di sicurezza e endpoint di collegamento Salesforce . Negli ambienti di produzione, è possibile aggiungere la chiave consumer e il segreto per la sicurezza OAuth.

```
Connection to Salesforce
------------------------
Salesforce Userid (reqd)   : []salesforce_login_email
Salesforce Password (reqd) : []salesforce_login_password
Security Token (reqd)      : []Security_Token
Login Endpoint             : [https://login.salesforce.com]
Consumer ID                : []
Consumer Secret Key        : []
```

c) Immettere i valori per gli archivi certificati per connessioni TLS:

I valori minimi necessari per connessioni TLS sono il percorso del keystore per i certificati TLS e la password del keystore. Se non viene fornito alcun percorso o password dell'archivio attendibile, i parametri keystore e password vengono utilizzati per l'archivio attendibile e la password. Se si utilizza TLS per la connessione al gestore code IBM MQ , è possibile utilizzare lo stesso keystore.

```
Certificate stores for TLS connections
--------------------------------------
Personal keystore for TLS certificates : []path_to_keystore, for example: /var/mqm/qmgrs/
SQM1/ssl/key.jks
Keystore password          : []keystore_password
Trusted store for signer certificates : []
Trusted store password     : []
Use TLS for MQ connection  : [N]
```

d) Immettere valori per configurare il comportamento di IBM MQ Bridge to Salesforce:

Non è necessario modificare o fornire nessuno di questi valori, ma se si conoscono i nomi degli argomenti push o degli eventi della piattaforma, aggiungerli qui. Possono anche essere aggiunti in un secondo momento, nella riga di comando, quando si è pronti a eseguire il bridge. È necessario specificare il file di log, nel file di configurazione o sulla riga comandi.

```
Behaviour of bridge program
---------------------------
PushTopic Names          : []
Platform Event Names     : []
MQ Monitoring Frequency  : [30]
At-least-once delivery? (Y/N) : [Y]
Subscribe to MQ publications for platform events? (Y/N) : [N]
Publish control data with the payload? (Y/N) : [N]
Delay before starting to process events : [0]
Runtime logfile for copy of stdout/stderr : []
```

8. Opzionale: Creare il servizio IBM MQ per controllare l'esecuzione del programma. Modificare il file `mqsfbService.mqsc` di esempio in modo che punti al file di configurazione appena creato e apportare eventuali altre modifiche ai parametri del comando.

```
cat modified mqsfbService.mqsc | runmqsc SQM1
```

9. Opzionale: Attieniti alle istruzioni in Introduzione a IBM MQ Console per configurare IBM MQ Console.
10. Opzionale: Configurare il IBM MQ Bridge to Salesforce per l'esecuzione come utente senza root.

    Per poter eseguire IBM MQ Bridge to Salesforce come un *utente senza root*, ad esempio all'interno di un *contenitore senza root*, le directory Java `userRoot` e `systemRoot` devono essere impostate correttamente per garantire l'accesso in lettura/scrittura per l'utente che esegue il processo bridge. A tale scopo, impostare le seguenti proprietà JVM:

```
export MQSFB_EXTRA_JAVA_OPTIONS="-
Djava.util.prefs.userRoot=directory_with_read_write_access"
```

```
export MQSFB_EXTRA_JAVA_OPTIONS="-
Djava.util.prefs.systemRoot=directory_with_read_write_access"
```

Risultati

Hai creato il file di configurazione che IBM MQ Bridge to Salesforce utilizza per sottoscrivere gli argomenti di push Salesforce e gli eventi della piattaforma e pubblicarli nella tua rete IBM MQ .

Operazioni successive

Eseguire le operazioni per “Esecuzione di IBM MQ Bridge to Salesforce” a pagina 806.

Attività correlate

Traccia di IBM MQ Bridge to Salesforce

Monitoraggio di IBM MQ Bridge to Salesforce

Riferimenti correlati

runmqsfb (eseguire IBM MQ Bridge to Salesforce)

Linux V 9.1.2 Opzioni di configurazione aggiuntive per IBM MQ Bridge to Salesforce

IBM MQ 9.1.2 introduce ulteriori opzioni di configurazione che consentono due classi principali di topologia aggiuntiva, gestendo il lavoro "in entrata" (eventi generati da Salesforce, pubblicati in applicazioni IBM MQ) e "in uscita" (applicazioniIBM MQ che pubblicano eventi inviati a Salesforce). Inoltre, vi è un cambiamento nel modo in cui la traccia e la registrazione funzionano.

Modifiche da IBM MQ 9.1.0 IBM MQ Bridge to Salesforce

Per impostazione predefinita, non ci sono modifiche al comportamento dal bridge IBM MQ 9.1.0 , a parte il file di log che ora inizia a ruotare. Per ulteriori informazioni, consultare “Rotazione dei log” a pagina 799.

La modifica principale è che un gestore code ora supporta più istanze bridge. Per abilitare questa funzione e il resto delle topologie aggiuntive, è necessario apportare alcune modifiche manuali alla configurazione.

Consultare runmqfsb per ulteriori informazioni sulle opzioni di configurazione aggiuntive e “Output di configurazione di esempio” a pagina 799 per un esempio delle informazioni di configurazione modificate.

Lavoro in ingresso separato

Più istanze del bridge possono gestire il lavoro in entrata da Salesforce a IBM MQ, ma devono lavorare su serie indipendenti di eventi e argomenti di push Salesforce . In caso contrario, vi sarebbe la possibilità di eventi ripetuti visti dalle applicazioni IBM MQ , poiché non esiste alcun protocollo cross - bridge per arrestare la duplicazione degli eventi. Ogni istanza utilizza la propria coda di sincronizzazione configurabile per contenere **ReplayId**.

Ciò è probabilmente utile quando:

- Argomenti Salesforce differenti hanno autorizzazioni di protezione differenti. Ogni istanza bridge ha una diversa serie di credenziali per accedere a Salesforce.
- Il carico di lavoro proveniente da Salesforce è troppo elevato per essere gestito da un singolo bridge. Pertanto, è possibile organizzare gli argomenti da partizionare con "A-M" che passa attraverso un ponte e "N-Z" attraverso un altro.

Lavoro in uscita condiviso

Il bridge supporta più istanze per supportare il lavoro in uscita inviato da IBM MQ a Salesforce. Se un'istanza del bridge ha esito negativo, le altre istanze sottoscritte agli stessi argomenti sullo stesso gestore code possono continuare l'elaborazione delle pubblicazioni.

Nota: Non sono necessarie modifiche alla configurazione dell'argomento IBM MQ .

Queste istanze collaborative devono essere configurate in modo che, al massimo, una delle istanze stia gestendo il lavoro in entrata da Salesforce, poiché tale istanza deve avere accesso esclusivo alla coda di sincronizzazione.

È probabile che ciò sia utile quando si hanno dubbi su:

- Carico di lavoro proveniente da IBM MQ. Poiché le richieste a Salesforce sono sincrone, il ponte non può elaborare nuovo lavoro mentre elabora ancora un messaggio. Avere più consumatori riduce questa situazione.
- Architettura di disponibilità. Ad esempio, è ora possibile eseguire più istanze in data center separati, con migliori opzioni di failover e ripristino di emergenza. L'esecuzione come client IBM MQ separa anche il bridge dall'ubicazione del gestore code.

Interazione di traccia e debug

L'indicatore di debug continua ad agire come prima. Ovvero, *-d1* fornisce informazioni di debug del bridge e *-d2* attiva la registrazione di debug per i componenti prerequisiti. Tuttavia, se è stata abilitata la traccia IBM MQ quando si avvia il bridge, il report di livello *-d2* viene attivato automaticamente.

Rotazione dei log

Il comportamento predefinito per il file di log cambia per avere tre file di log, ciascuno di dimensione 2 MB. È possibile sovrascrivere questi valori utilizzando ulteriori proprietà di configurazione. L'attributo di configurazione esistente o il parametro della riga comandi per il file di log, viene utilizzato come nome di base per i log, con un indice aggiunto.

Se il file di log configurato ha:

- Nessun tipo di file, l'indice viene aggiunto alla fine del nome file.

  Impostando il file di log su `abc`, si ottengono log denominati `abc.0`, `abc.1`e così via.
- Un tipo di file, l'indice viene inserito prima del tipo di file.

  Impostando il file di log su `abc.log`, si ottengono log denominati `abc.0.log`, `abc.1.log`e così via.

Note:

1. Poiché i bridge possono essere in esecuzione con autorizzazioni utente arbitrarie, non è possibile forzare una particolare directory, ad esempio, `/var/mqm/qmgrs/<qm>/errors`, per i log.
2. Le stesse informazioni continuano ad essere scritte negli stream *stdout* e *stderr* .
3. Ogni volta che un singolo file di log viene riaperto, le informazioni di configurazione di base vengono ristampate. Le informazioni saranno sempre disponibili, invece di essere stampate una sola volta all'avvio del programma.

Conservazione dei log

Le nuove topologie rendono più probabile la presenza di più istanze del bridge in esecuzione su uno specifico gestore code.

Per evitare che le istanze interferiscano tra loro e per evitare di sovrascrivere le precedenti esecuzioni del bridge, il bridge non verrà avviato se il log `.0` esiste già.

È necessaria una procedura di avvio che elimini le copie precedenti del log prima di avviare il bridge o aggiunga una data / ora al nome.

Attività correlate

“Configurazione di IBM MQ per l'utilizzo con gli argomenti push Salesforce e gli eventi della piattaforma” a pagina 791
Utilizzare queste informazioni per impostare la sicurezza e le connessioni a Salesforce e alla rete IBM MQ configurando e quindi eseguendo IBM MQ Bridge to Salesforce.

Riferimenti correlati

runmqfsb

Linux V 9.1.2 Output di configurazione di esempio

Un output di configurazione di esempio, che mostra le modifiche da IBM MQ 9.1.0 IBM MQ Bridge to Salesforce.

```
IBM MQ Bridge to Salesforce
5724-H72 (C) Copyright IBM Corp. 2017, 2024.
Level : <<unknown>>

Enter new values for the configuration attributes. The
current settings are shown.
Press ENTER to accept current values; use SPACE+ENTER
to clear values.
```

```
Connection to Queue Manager
---------------------------
Queue Manager or JNDI CF   : [V9000_A]
MQ Base Topic              : [/sf]
MQ Channel                 : []
MQ Conname                 : []
MQ Publication Error Queue : [SYSTEM.SALESFORCE.DEADQ]
MQ Replay Status Queue     : [SYSTEM.SALESFORCE.SYNCQ]
MQ CCDT URL                : []
JNDI implementation class  : [com.sun.jndi.fscontext.RefFSContextFactory]
JNDI provider URL          : []
MQ Userid                  : []
MQ Password                : []

Connection to Salesforce
------------------------
Salesforce Userid (reqd)   : [johndoe@<yourenterprise>.com]
Salesforce Password (reqd) : [********]
Security Token             : [********]
Login Endpoint             : [https://login.salesforce.com]
Consumer Key               : [3MVG9HxRZv05HarQhSy89qSKYNr1gDcv1wE3zN5kyFAa4Wxt]
Consumer Secret            : [********]

Certificate stores for TLS connections
--------------------------------------
Personal keystore for TLS certificates : [/var/mqm/ssl/key.jks]
Keystore password          : [********]
Trusted store for signer certificates : []
Trusted store password     : []
Use TLS for MQ connection  : [N]

Event processing
----------------
PushTopic Names            : []
Platform Event Names       : []
At-least-once delivery for Salesforce events? (Y/N) : [N]
At-least-once delivery for MQ publications? (Y/N) : [N]
Subscribe to MQ publications for platform events? (Y/N) : [Y]
Publish control data with the payload? (Y/N) : [Y]
Treat unknown Salesforce topic as warning (Y/N) : [N]

Behaviour of bridge program
---------------------------
Bridge unique identifier   : []
MQ Monitoring Frequency    : [30]
Delay before starting to process events : [0]
Continue to retry after maximum reconnection attempts (Y/N) : [N]
Runtime logfile for copy of stdout/stderr : [/tmp/runmqsfb.log]
Number of logfiles         : [3]
Maximum size of each logfile : [2097152]
Done.
```

Riferimenti correlati

runmqfsb

Linux V 9.1.0 Creazione di messaggi di eventi per eventi della piattaforma Salesforce

È possibile configurare IBM MQ ed immettere `IBM MQ Bridge to Salesforce parameters` per creare il file di configurazione ed utilizzare il bridge per creare messaggi di eventi per gli eventi della piattaforma Salesforce .

Prima di iniziare

- È stato installato il pacchetto **MQSeriesSFBridge** nell'installazione di IBM MQ su una piattaforma x86-64 Linux .

Informazioni su questa attività

Questa attività consente di eseguire la configurazione minima necessaria per creare il file di configurazione IBM MQ Bridge to Salesforce e connettersi correttamente a Salesforce e IBM MQ in modo

da creare messaggi di eventi per gli eventi della piattaforma Salesforce . Per ulteriori informazioni sul significato e sulle opzioni per tutti i parametri, consultare il comando runmqsfb . È necessario considerare i propri requisiti di sicurezza e personalizzare i parametri appropriati per la propria distribuzione.

Per creare la configurazione per la sottoscrizione agli argomenti di push e agli eventi della piattaforma, vedi "Configurazione di IBM MQ Bridge to Salesforce" a pagina 793.

Creazione di messaggi di eventi per eventi della piattaforma Salesforce

È possibile utilizzare un'applicazione IBM MQ per creare i messaggi inseriti in un argomento del gestore code `/root/mqtosfb/event/+`. Il bridge sottoscrive l'argomento, richiama il contenuto dai messaggi e lo utilizza per pubblicare i messaggi di eventi per un evento della piattaforma Salesforce . Per ulteriori informazioni sugli eventi della piattaforma, vedi Distribuzione di notifiche personalizzate con gli eventi della piattaforma nella documentazione dello sviluppatore Salesforce .

Per abilitare il bridge a creare messaggi di eventi, è necessario fornire due attributi aggiuntivi rispetto a quelli utilizzati per la sottoscrizione agli argomenti di push e agli eventi della piattaforma:

- Creare e aggiungere il nome di **MQ Publication Error Queue** negli attributi di configurazione bridge per **Connessione al gestore code**.
- Impostare l'opzione **Subscribe to MQ publications for platform events** su *Y*, negli attributi di configurazione bridge per definire il **Comportamento del programma bridge**.

È necessario creare un evento piattaforma in Salesforce e definire i campi del contenuto prima di poter utilizzare il ponte per creare i messaggi evento per tale evento piattaforma. Il nome dell'evento della piattaforma e il relativo contenuto determinano come è necessario formattare il messaggio IBM MQ elaborato dal bridge. Ad esempio, se il tuo Salesforce evento della piattaforma **Object name** è *MQPlatformEvent1* e i due campi definiti personalizzati sono campi di testo con **API name** *MyText__c* e *Name__c*, il tuo messaggio IBM MQ pubblicato nell'argomento `/root/mqtosfb/event/MQPlatformEvent1__`e deve essere un JSON formattato correttamente, come riportato di seguito:

```
{ "MyText__c" : "Some text here", "Name__c" : "Bob Smith" }
```

Il messaggio deve essere formattato in modo che IBM MQ Bridge to Salesforce sia in grado di riconoscerlo come corpo del messaggio formattato MQFMT_STRING.

Consultare il passo "7" a pagina 803 per creare l'evento della piattaforma in Salesforce oppure ignorare questo passo se si dispone già di un evento della piattaforma per cui si desidera creare messaggi di eventi. Devi formattare il tuo messaggio IBM MQ per corrispondere ai campi impostati nell'evento della piattaforma Salesforce . I campi all'interno dell'evento della piattaforma Salesforce possono essere indicati come facoltativi o obbligatori. Per ulteriori informazioni, vedi Campi evento della piattaforma nella documentazione per lo sviluppatore di Salesforce .

Quando il bridge è in esecuzione, sottoscrive l'argomento IBM MQ designato.

- Se si specifica la QoS (quality of service) **At-most-once** nella configurazione del bridge, la sottoscrizione che il bridge effettua non è durevole. Tutte le pubblicazioni effettuate dalle applicazioni IBM MQ mentre il bridge non è in esecuzione non vengono elaborate.
- Se si specifica la QoS (quality of service) **At-least-once** nella configurazione del bridge, la sottoscrizione che il bridge effettua è durevole. Ciò significa che il bridge può elaborare le pubblicazioni effettuate dalle applicazioni IBM MQ mentre il bridge non è in esecuzione. Le sottoscrizioni durevoli richiedono una sottoscrizione nota e un ID client. Il bridge utilizza *D_SUB_RUNMQSFB* come nome sottoscrizione e *runmqsfb_1* come ID client.

Se il bridge viene utilizzato per la sottoscrizione agli argomenti di push Salesforce e agli eventi della piattaforma e non per la creazione di messaggi di evento, tenta di eliminare la sottoscrizione durevole, nel caso in cui la configurazione venga modificata, e la sottoscrizione è ora orfana.

È possibile eliminare le sottoscrizioni durevoli create dal bridge nel modo seguente:

Utilizzare IBM MQ Explorer.

Aprire la **cartella sottoscrizioni** per il gestore code che il bridge sta utilizzando e cercare il nome della sottoscrizione che termina in *:D_SUB_RUNMQSFB* dove la stringa di argomenti è `/sf/mqtosfb/`

event+. Fare clic con il tasto destro del mouse sul nome della sottoscrizione e fare clic su Elimina. Se ricevi un errore che indica che la sottoscrizione è in uso, il tuo bridge potrebbe essere ancora in esecuzione. Arrestare il bridge e provare a eliminare nuovamente la sottoscrizione.

Utilizzare `runmqsc` per trovare ed eliminare la sottoscrizione.
Avviare l'interfaccia **`runmqsc`** ed eseguire `DISPLAY SUB (*)`. Ricercare il nome della sottoscrizione **SUB** che termina con *:D_SUB_RUNMQ*. Immettere il comando secondario delete e includere il **SUBID** della sottoscrizione che si desidera eliminare. Ad esempio, `DELETE SUB SUBID(414D5120514D312020202020202020205C589459987E8620)`

Arrestare, quindi avviare il bridge con la QoS (quality of service) `At-most-once` .
Se hai avviato il bridge con la **`At-least-once`** QoS (quality of service) `At-least-once delivery? (Y/N) :[Y]`, la sottoscrizione creata è durevole. Per eliminare la sottoscrizione, modificare la QoS (quality of service) in `At-least-once delivery? (Y/N) :[N]` nel file di configurazione e riavviare il bridge. La sottoscrizione durevole viene eliminata e viene creata una sottoscrizione non durevole.

Procedura

1. Creare e avviare un gestore code.
   a) Creare un gestore code, ad esempio PEQM1.

   ```
   crtmqm PEQM1
   ```

   b) Avviare il gestore code.

   ```
   strmqm PEQM1
   ```

2. **Nota:** Per utilizzare le credenziali di accesso e sicurezza Salesforce esistenti e il certificato autofirmato, andare al passo 4.

   Opzionale: Crea un token di sicurezza per il tuo account Salesforce .
   a) Esegui l'accesso al tuo account Salesforce.
   b) Crea o reimposta il tuo token di sicurezza seguendo la procedura nell'articolo della guida Salesforce help: Reimposta il tuo token di protezione.
3. Creare un certificato di sicurezza autofirmato in Salesforce.
   a) Selezionare **Controlli di protezione** dal menu **Amministra** della **Force.com Home** page, quindi **Gestione chiavi e certificati**.
   Viene visualizzata la pagina **Gestione chiavi e certificati** .
   b) Fare clic su **Crea certificato autofirmato**.
   Viene visualizzata la pagina **Certificati** .
   c) Immettere un nome per il certificato nel campo **Etichetta** , premere Tab, quindi fare clic su **Salva**.
   Vengono visualizzate le informazioni sui dettagli chiave e certificato.
   d) Fare clic su **Torna all'elenco: Certificati e chiavi**.
   e) Fare clic su **Esporta nel keystore**.
   f) Immettere una password per il keystore, quindi fare clic su **Esporta**.
   g) Salvare il keystore esportato nel file system locale.
4. Utilizzare la GUI di IBM Key Management per aprire il keystore esportato da Salesforce e popolare i certificati del firmatario.
   a) Eseguire il comando **`strmqikm`** per aprire la GUI di IBM Key Management. Per ulteriori informazioni, consultare Utilizzo di runmqckm, runmqakm e strmqikm per gestire i certificati digitali.
   b) Fare clic su **Apri un file del database delle chiavi** e selezionare l'ubicazione del keystore Salesforce .

c) Fare clic su **Apri**, assicurarsi di selezionare **JKS** dalle opzioni **Tipo di database delle chiavi** , quindi fare clic su **OK**.

d) Immettere la password creata per il keystore nel passo 3f, quindi fare clic su **OK**.

e) Selezionare **Certificati firmatario** dalle opzioni **Contenuto database di chiavi** .

f) Fare clic su **Popola**.

g) Selezionare la casella di spunta **Verisign Inc.** dall'elenco **Aggiungi certificati CA** , quindi fare clic su **OK**.

5. Opzionale: Genera la chiave consumer OAuth e il segreto creando una connessione dell'app per IBM MQ Bridge to Salesforce nell'account Salesforce .

   Hai bisogno dei codici **Chiave consumer** e **Segreto consumer** quando utilizzi IBM MQ Bridge to Salesforce negli ambienti di produzione.

   a) Selezionare **Crea**, quindi **App** dal menu **Crea** della pagina **Home Force.com** .

      Viene visualizzata la pagina **App** .

   b) Fare clic su **Nuovo** nella sezione **App connesse** .

      Viene aperta la pagina **Nuova App connessa** .

   c) Immetti un nome per il tuo IBM MQ Bridge to Salesforce in **Connected App Name**, ad esempio **MQBridgeToSalesforce**.

   d) Immetti il **Nome API**.

      Se passi al campo successivo, il **Nome applicazione connessa** viene copiato nel campo del nome **Nome API** .

   e) Immettere la propria **email di contatto**.

   f) Selezionare l'opzione **Abilita impostazioni OAuth** nella sezione **API (Abilita impostazioni OAuth)** .

      Vengono quindi presentate ulteriori opzioni in tale sezione.

   g) Aggiungere l' **URL di callback**, ad esempio `https://www.ibm.com`.

   h) Selezionare l'opzione **Accesso completo (completo)** dall'elenco **Ambiti OAuth disponibili** nella sottosezione **Ambiti OAuth selezionati** , quindi fare clic su **Aggiungi**, per aggiungere l'accesso completo all'elenco **Ambiti OAuth selezionati** .

   i) Fare clic su **Salva**.

   j) Fare clic su **Continua**.

   k) Prendere nota dei codici **Chiave consumer** e **Segreto consumer** .

6. Creare le code di sincronizzazione e di errore richieste sul gestore code.

```
cat /opt/mqm/mqsf/samp/mqsfbSyncQ.mqsc | runmqsc PEQM1
```

   La coda di sincronizzazione mantiene lo stato dell'evento tra i riavvii dell'applicazione o del gestore code. La grandezza della coda può essere ridotta in quanto è previsto un solo messaggio sulla coda. Solo un'istanza del bridge può essere eseguita per volta su questa coda, quindi le opzioni predefinite vengono impostate per l'accesso esclusivo. La coda di errori deve essere creata prima di poter utilizzare il bridge per creare messaggi di eventi per gli eventi della piattaforma. La coda di errore viene utilizzata per i messaggi che non possono essere elaborati correttamente da Salesforce. È necessario aggiungere il nome della coda di errori nella sezione del parametro di configurazione bridge **`Connection to Queue Manager`** come mostrato nel passo “8.a” a pagina 804.

7. Opzionale: Crea un oggetto evento della piattaforma nell'account Salesforce .

   a) Seleziona **Platform Events** dal menu **Develop** della tua **Force.com Home** page, quindi fai clic su **New Platform Event**.

      Viene aperta la pagina **Nuovo evento piattaforma** .

   b) Completare i campi **Etichetta** e **Etichetta plurale** .

   c) Fare clic su **Salva**.

Viene aperta la pagina **Dettagli definizione evento piattaforma** .

d) Definire i **Campi e relazioni personalizzati**.

Ad esempio, è possibile aggiungere due campi di testo con etichette *MyText* e *Name* e impostare le lunghezze dei campi **Tipo di dati** su *Testo (64)* e *Testo (32)* rispettivamente.

È stato creato un evento della piattaforma e definito **Custom Fields and Relationships** per esso. Utilizza il tuo evento della piattaforma *Platform Object name* o il *nome API* come argomento IBM MQ in cui puoi inserire i messaggi che vuoi che il bridge elabori. Ad esempio, è possibile utilizzare l'esempio **AMQSPUBA** per aggiungere il seguente messaggio formattato JSON all'argomento `/sf/mqtosfb/event/`*`Salesforce Platform Object Name/API name`* :

```
{ "MyText__c" : "Some text here", "Name__c" : "Bob Smith" }
```

È possibile eseguire l'esempio **AMQSPUBA** per creare messaggi dopo l'avvio del bridge. Dalla directory *`MQ installation location`*`/samp/bin` , immettere il seguente comando:

```
./amqspub /sf/mqtosfb/event/Salesforce Platform Object Name/API name PEQM1
```

Al prompt, immettere il messaggio in formato JSON.

8. Creare un file di configurazione con i parametri di connessione e sicurezza per IBM MQ, Salesforcee il funzionamento di IBM MQ Bridge to Salesforce .

```
runmqsfb -o new_config.cfg
```

I valori esistenti vengono visualizzati all'interno delle parentesi. Premere `Enter` per accettare i valori esistenti, premere `Space` quindi `Enter` per cancellare i valori e, immettere, quindi `Enter` per aggiungere nuovi valori.

a) Immettere i valori per la connessione al gestore code PEQM1:

I valori minimi necessari per la connessione sono il nome del gestore code, la root dell'argomento di base IBM MQ , il nome della coda di errori e il nome del canale.

```
Connection to Queue Manager
---------------------------
Queue Manager or JNDI CF   : []PEQM1
MQ Base Topic              : []/sf
MQ Channel                 : []A channel you have defined or for example
SYSTEM.DEF.SVRCONN
MQ Conname                 : []
MQ Publication Error Queue : [SYSTEM.SALESFORCE.ERRORQ]
MQ CCDT URL                : []
JNDI implementation class  : [com.sun.jndi.fscontext.RefFSContextFactory]
JNDI provider URL          : []
MQ Userid                  : []
MQ Password                : []
```

Nota: Se si sta effettuando la connessione in locale, il nome del canale non è richiesto. Non è necessario fornire il nome del gestore code e l'argomento di base nel file di configurazione poiché possono essere inclusi sulla riga comandi in un secondo momento, quando si esegue il bridge.

b) Immettere i valori per la connessione a Salesforce:

I valori minimi necessari per la connessione sono ID utente Salesforce , password, token di sicurezza e endpoint di collegamento. Negli ambienti di produzione, è possibile aggiungere la chiave consumer e il segreto per la sicurezza OAuth.

```
Connection to Salesforce
------------------------
Salesforce Userid (reqd)   : []salesforce_login_email
Salesforce Password (reqd) : []salesforce_login_password
Security Token (reqd)      : []Security_Token
Login Endpoint             : [https://login.salesforce.com]
Consumer ID                : []
Consumer Secret Key        : []
```

c) Immettere i valori per gli archivi certificati per connessioni TLS:

I valori minimi necessari per connessioni TLS sono il percorso del keystore per i certificati TLS e la password del keystore. Se non viene fornito alcun percorso o password dell'archivio attendibile, i parametri keystore e password vengono utilizzati per l'archivio attendibile e la password. Se si utilizza TLS per la connessione al gestore code IBM MQ , è possibile utilizzare lo stesso keystore.

```
Certificate stores for TLS connections
--------------------------------------
Personal keystore for TLS certificates : []path_to_keystore, for example: /var/mqm/qmgrs/
PEQM1/ssl/key.jks
Keystore password          : []keystore_password
Trusted store for signer certificates : []
Trusted store password     : []
Use TLS for MQ connection  : [N]
```

d) Immettere valori per configurare il comportamento di IBM MQ Bridge to Salesforce:

È necessario modificare l'opzione **Subscribe to MQ publications for platform events** dal valore predefinito *N*, a *Y* , per utilizzare il bridge per creare messaggi di eventi. È inoltre necessario specificare il file di log, nel file di configurazione o sulla riga comandi.

```
Behaviour of bridge program
---------------------------
PushTopic Names            : []
Platform Event Names       : []
MQ Monitoring Frequency    : [30]
At-least-once delivery? (Y/N) : [Y]
Subscribe to MQ publications for platform events? (Y/N) : [Y]
Publish control data with the payload? (Y/N) : [N]
Delay before starting to process events : [0]
Runtime logfile for copy of stdout/stderr : []
```

9. Opzionale: Creare il servizio IBM MQ per controllare l'esecuzione del programma. Modificare il file `mqsfbService.mqsc` di esempio in modo che punti al file di configurazione appena creato e apportare eventuali altre modifiche ai parametri del comando.

```
cat modified mqsfbService.mqsc | runmqsc PEQM1
```

10. Opzionale: Attieniti alle istruzioni in Introduzione a IBM MQ Console per configurare IBM MQ Console.
11. Opzionale: Aggiungere e configurare i widget nella propria istanza IBM MQ Console per visualizzare i dati Salesforce .
    a) Fare clic su **Aggiungi widget**.
    Viene aperto il nuovo widget.
    b) Selezionare **Grafici**
    c) Fare clic sull'icona **Configura widget** nella barra del titolo del nuovo widget.
    d) Opzionale: Immettere un **Titolo widget**.
    e) Seleziona **Salesforce Bridge** dal menu a discesa **Resource to monitor**, **Source** .
    f) Selezionare **Stato bridge**, dal menu a discesa **Classe risorsa**.
    g) Selezionare **MQ-created Platform Events**, dal menu a discesa **Tipo di risorsa**.
    h) Selezionare **Totale eventi piattaforma MQcreati**, dal menu a discesa **Elemento risorsa**.
    i) Fare clic su **Salva**.

È stato configurato il IBM MQ Console per mostrare il numero totale di IBM MQ eventi della piattaforma creati. Quando il bridge è in esecuzione e si inizia a inserire i messaggi nell'argomento `/sf/mqtosfb/event/`*`Salesforce Platform Object Name/API name`* , il widget mostra il numero totale di eventi di messaggi creati dal bridge.

V 9.1.0 Formato del messaggio e messaggi di errore per IBM MQ Bridge to Salesforce

Informazioni sulla formattazione dei messaggi elaborati da IBM MQ Bridge to Salesforce.

Un'applicazione inserisce un messaggio in un argomento specifico del gestore code, ad esempio */root/mqtosfb/event/MQPlatformEvent1__e*. Il bridge sottoscrive l'argomento, richiama il contenuto dai messaggi e lo utilizza per pubblicare i messaggi di eventi per un evento della piattaforma Salesforce .

È necessario creare un evento piattaforma in Salesforce e definire i campi del contenuto prima di poter utilizzare il ponte per creare i messaggi evento per tale evento piattaforma. Il nome dell'evento della piattaforma e il relativo contenuto determinano come è necessario formattare il messaggio IBM MQ elaborato dal bridge. Ad esempio, se il tuo Salesforce evento della piattaforma **Object name** è *MQPlatformEvent1* e i due campi definiti personalizzati sono campi di testo con **API name** *MyText__c* e *Name__c*, il tuo messaggio IBM MQ pubblicato nell'argomento */root/mqtosfb/event/MQPlatformEvent1__e* deve essere un JSON formattato correttamente, come riportato di seguito:

```
{ "MyText__c" : "Some text here", "Name__c" : "Bob Smith" }
```

I messaggi utilizzati e prodotti dal bridge sono messaggi di testo (MQSTR) in formato JSON. Il messaggio di input è un semplice JSON e i programmi possono utilizzare la concatenazione di stringhe per generarlo.

Messaggi di errore

Gli errori possono essere rilevati dal bridge, ad esempio se il messaggio non è in formato testo o da Salesforce, ad esempio se il nome evento della piattaforma non esiste. Se si verifica un errore durante l'elaborazione del messaggio di input, il messaggio viene spostato nella coda di errori del bridge insieme alle proprietà che descrivono l'errore. L'errore viene scritto anche nel flusso *stderr* per il bridge.

Gli errori generati da Salesforce sono JSON. Di seguito sono riportati alcuni errori causati da messaggi formattati in maniera non corretta:

Contenuto evento piattaforma non valido, stato 400 Testo

```
[{"message":"No such column 'Name__c' on sobject of type
MQPlatformEvent2__e","errorCode":"INVALID_FIELD"}
```

Nome evento piattaforma non valido, testo stato 404

```
{"errorCode":"NOT_FOUND","message":"The requested resource does not exist"}
```

JSON non corretto, testo stato 400

```
{"errorCode":"NOT_FOUND","message":"The requested resource does not exist"}
```

Il messaggio non è JSON, testo stato 400

```
[{"message":
  "Unexpected character ('h' (code 104)): expected a valid value (number, String, array,
object, 'true', 'false' or 'null') at [line:1, column:2]",
  "errorCode":"JSON_PARSER_ERROR"}
```

Non è un messaggio di testo (non inviato a Salesforce)

```
Error: Publication on topic ' /sf/mqtosfb/event/MQPlatformEvent1' does not contain a text
formatted message
```

Linux V 9.1.0 Esecuzione di IBM MQ Bridge to Salesforce

Eseguire IBM MQ Bridge to Salesforce per connettersi a Salesforce e IBM MQ. Quando è connesso, il bridge può creare sottoscrizioni agli argomenti Salesforce e ripubblicare i messaggi nell'argomento IBM MQ . Il ponte può anche creare messaggi di eventi per gli eventi della piattaforma Salesforce .

Prima di iniziare

È stata completata la procedura di configurazione nell'attività di :

- “Configurazione di IBM MQ Bridge to Salesforce” a pagina 793
- “Creazione di messaggi di eventi per eventi della piattaforma Salesforce” a pagina 800

.

Informazioni su questa attività

Utilizzare il file di configurazione creato nell'attività precedente per eseguire IBM MQ Bridge to Salesforce. Se non sono stati inclusi tutti i parametri richiesti nel file di configurazione, assicurarsi di includerli nella riga comandi.

Procedura

1. Definisci gli argomenti push o gli eventi della piattaforma in Salesforce per cui vuoi sottoscrivere o l'evento della piattaforma per cui vuoi creare i messaggi di eventi.
2. Avviare IBM MQ Bridge to Salesforce per connettersi a Salesforce e al gestore code. Se stai eseguendo il bridge per sottoscrivere gli eventi Salesforce , includi il nome dell'argomento push o dell'evento della piattaforma che hai definito nel passo 1.

   ```
   runmqsfb -f new_config.cfg -r logFile -p PushtopicName -e eventName
   ```

   Quando il bridge è connesso, vengono restituiti i seguenti messaggi:

   - Se stai utilizzando il bridge per sottoscrivere l'argomento push Salesforce e gli eventi della piattaforma:

     ```
     Successful connection to queue manager QM1
     Warning: Subscribing to MQ-created platform events is not enabled.
     Successful login to Salesforce at https://eu11.salesforce.com
     Ready to process events.
     ```

   - Se si sta utilizzando il bridge per creare messaggi di evento per gli eventi della piattaforma Salesforce :

     ```
     Successful connection to queue manager QM1
     Successful login to Salesforce at https://eu11.salesforce.com
     Successful subscription to '/sf/mqtosfb/event/+' for MQ-created platform events
     Ready to process events.
     ```

3. Opzionale: Risolvere i problemi relativi alla connessione al gestore code e a Salesforce se i messaggi restituiti dopo l'esecuzione del bridge indicano che una connessione non è stata eseguita correttamente.
   a) Immettere il comando in modo debug con l'opzione di debug 1.

      ```
      runmqsfb -f new_config.cfg -r logFile -p PushtopicName -e eventName -d 1
      ```

      Il bridge passa attraverso la configurazione della connessione e mostra i messaggi di elaborazione in modalità concisa.

   b) Immettere il comando in modo debug con l'opzione di debug 2.

      ```
      runmqsfb -f new_config.cfg -r logFile -p PushtopicName -e eventName -d 2
      ```

      Il bridge passa attraverso la connessione impostata e mostra i messaggi di elaborazione in modalità dettagliata. L'output completo viene scritto nel file di log.
4. Generare eventi utilizzando l'interfaccia Salesforce per modificare i record nel database.
5. Passare a IBM MQ Console per visualizzare le modifiche agli argomenti push nel widget configurato nell'attività precedente.

Operazioni successive

Utilizzare la variabile *MQSFB_EXTRA_JAVA_OPTIONS* per passare nelle propriet ... JVM, ad esempio, per abilitare la traccia IBM MQ . Per ulteriori informazioni, consultare Traccia di IBM MQ Bridge to Salesforce.

Attività correlate

Monitoraggio di IBM MQ Bridge to Salesforce

Riferimenti correlati

runmqsfb (eseguire IBM MQ Bridge to Salesforce)

z/OS MQ Adv. Linux V 9.1.0 Configurazione di IBM MQ per l'utilizzo con blockchain

Configura ed esegui IBM MQ Bridge to blockchain per connettere in modo sicuro un gestore code Linux IBM MQ Advanced o z/OS IBM MQ Advanced for z/OS Value Unit Edition e IBM Blockchain. Utilizza il bridge per stabilire una connessione asincrona, ricercare e aggiornare lo stato di una risorsa nella tua blockchain, utilizzando un'applicazione di messaggistica che si connette al tuo gestore code IBM MQ Advanced o IBM MQ Advanced for z/OS VUE .

Prima di iniziare

Nota: Il IBM MQ Bridge to blockchain è obsoleto in tutte le release del 22 novembre 2022 (vedi Lettera di annuncio USA 222 - 431).

Attenzione: V 9.1.4 IBM MQ Bridge to blockchain creato su Hyperledger Composer non è più supportato.

Devi eseguire IBM MQ 9.1.4 per utilizzare il IBM MQ Bridge to blockchain creato su Hyperledger Fabric.

- IBM MQ Bridge to blockchain è disponibile per la connessione a:
  - Linux IBM MQ Advancedo
  - z/OS IBM MQ Advanced for z/OS VUE

  solo gestori code.
- V 9.1.4 Il gestore code deve essere allo stesso livello di comando del bridge o superiore; ad esempio, 9.1.4.
- V 9.1.4 IBM MQ Bridge to blockchain è supportata per l'utilizzo con la tua rete blockchain basata sull'architettura Hyperledger Fabric 1.4 .

Informazioni su questa attività

Blockchain è un libro mastro condiviso, distribuito, digitale che consiste in una catena di blocchi che rappresentano le transazioni concordate tra peer in una rete. Ogni blocco nella catena è collegato al blocco precedente, e così via, di nuovo alla prima transazione.

IBM Blockchain è creato su Hyperledger Fabric e puoi sviluppare con esso localmente con Docker o in un cluster di contenitori in IBM Cloud (formerly Bluemix). È inoltre possibile attivare e utilizzare la rete IBM Blockchain in produzione, per creare e gestire una rete aziendale con livelli elevati di sicurezza, privacy e prestazioni. Per ulteriori informazioni, vedi IBM Blockchain Platform.

Hyperledger Fabric è un framework blockchain aziendale open source sviluppato in modo collaborativo dai membri di Hyperledger Project, incluso IBM come contributore del codice iniziale. Hyperledger Project, o Hyperledger, è un' Linux Foundation iniziativa collaborativa, globale e open source per promuovere le tecnologie blockchain intersettoriali. Per ulteriori informazioni, consultare IBM Blockchain, Hyperledger Projectse Hyperledger Fabric.

Se stai già utilizzando IBM MQ Advancedo IBM MQ Advanced for z/OS VUEe IBM Blockchain, puoi utilizzare IBM MQ Bridge to blockchain per inviare semplici query, aggiornamenti e ricevere risposte dalla tua rete blockchain. In questo modo, puoi integrare il software IBM in loco con un servizio blockchain cloud.

È possibile visualizzare una breve panoramica del processo operativo del bridge nella Figura 1. Un'applicazione utente inserisce un messaggio in formato JSON nella coda di input / richiesta sul gestore code IBM MQ Advancedo IBM MQ Advanced for z/OS VUE . Il bridge si connette al gestore code, riceve il messaggio dalla coda di input/richiesta, verifica che il JSON sia formattato correttamente, quindi emette la query o un aggiornamento alla blockchain. I dati restituiti dalla blockchain vengono analizzati dal bridge e inseriti nella coda di risposta, come definito nel messaggio di richiesta IBM MQ originale. L'applicazione utente può connettersi al gestore code, ricevere il messaggio di risposta dalla coda di risposte e utilizzare le informazioni.

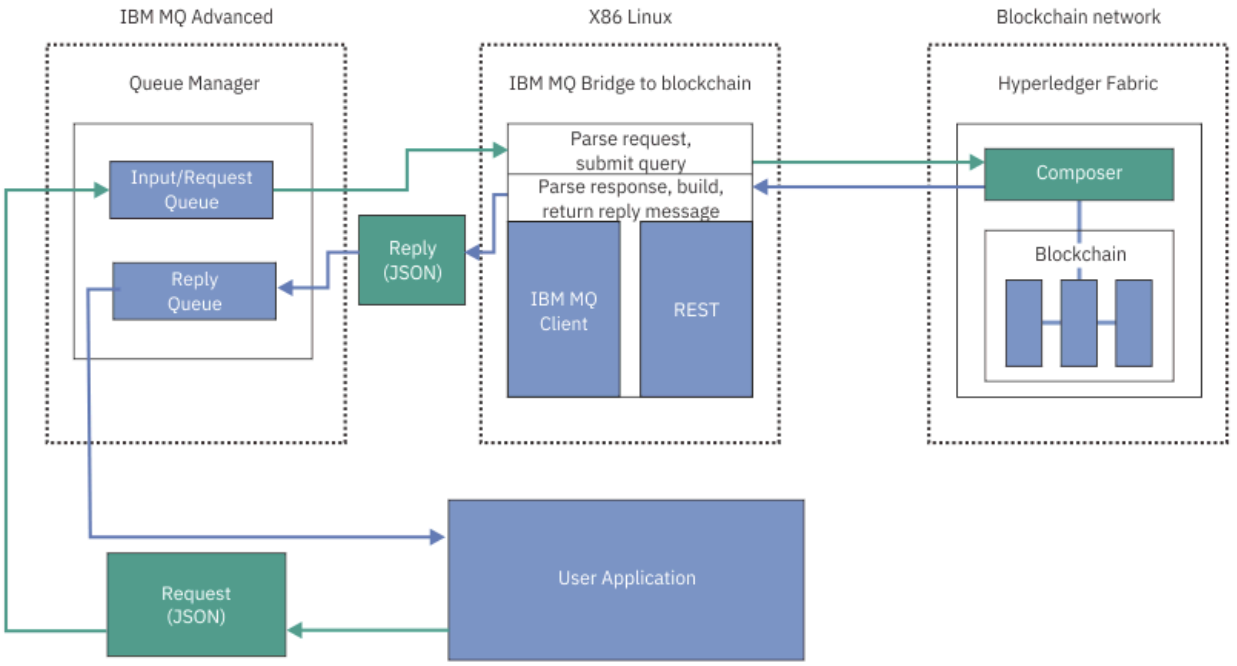


Figura 98. IBM MQ Bridge to blockchain

Puoi configurare il IBM MQ Bridge to blockchain per la connessione a una rete blockchain come partecipante o peer. Quando il bridge è in esecuzione, un'applicazione di messaggistica richiede al bridge di guidare le routine chaincode che eseguono la query o aggiornano lo stato della risorsa e restituiscono i risultati come risposta all'applicazione di messaggistica.

Procedura

1. Creare e avviare un gestore code o avviare un gestore code esistente che si desidera utilizzare con IBM MQ Bridge to blockchain.

   Crea gestore code:

   ```
   crtmqm adv_qmgr_name
   ```

   Avvia gestore code:

   ```
   strmqm adv_qmgr_name
   ```

2. Creare le code per il bridge definite nello script **DefineQ.mqsc** .

   Le definizioni di coda bridge di esempio vengono fornite per le code denominate predefinite utilizzate per:

- Credenziali utente, ad esempio SYSTEM.BLOCKCHAIN.IDENTITY.QUEUE
- Input del messaggio al bridge, ad esempio APPL1.BLOCKCHAIN.INPUT.QUEUE .
- Risposte da blockchain, ad esempio APPL1.BLOCKCHAIN.REPLY.QUEUE

Dalla directory /opt/mqm/mqbc/samp , immettere il seguente comando:

```
runmqsc adv_qmgr_name < ./DefineQ.mqsc
```

Diverse applicazioni possono utilizzare la stessa coda di input, ma è possibile specificare più code di risposta, una per ciascuna delle applicazioni. Non è necessario utilizzare code di risposta definite. Se si desidera utilizzare le code dinamiche per le risposte, è necessario considerarne la configurazione di sicurezza.

Risultati

Hai creato le code richieste dal bridge per elaborare i messaggi da IBM MQ e dalla tua rete blockchain.

Operazioni successive

Utilizza le informazioni sul tuo gestore code IBM MQ Advancedo IBM MQ Advanced for z/OS VUEe le credenziali dalla tua rete blockchain per creare un file di configurazione per IBM MQ Bridge to blockchain.

V 9.1.0 Creazione del file di configurazione per IBM MQ Bridge to blockchain

Immetti il tuo gestore code e i tuoi parametri di rete blockchain per creare il file di configurazione per IBM MQ Bridge to blockchain per la connessione alle tue reti IBM MQ e IBM Blockchain .

Prima di iniziare

- Hai creato e configurato la tua rete blockchain.
- Hai il file delle credenziali dalla tua rete blockchain.
- È stato installato IBM MQ Bridge to blockchain, nell'ambiente x86 Linux .
- È stato avviato il gestore code IBM MQ Advanced .

Informazioni su questa attività

Questa attività consente di eseguire la configurazione minima necessaria per creare il file di configurazione IBM MQ Bridge to blockchain e connettersi correttamente alle reti IBM Blockchain e IBM MQ .

Puoi utilizzare il bridge per connetterti alle reti blockchain basate su Hyperledger Fabric 1.4 architecture. Per utilizzare il bridge, hai bisogno di informazioni di configurazione dalla tua rete blockchain. In ogni passo di questa attività puoi individuare i dettagli di configurazione di esempio basati su due reti blockchain configurate in modo diverso:

- Rete Hyperledger Fabric in esecuzione in Docker. Per ulteriori informazioni, vedi Introduzione a Hyperledger Fabric, Scrittura della prima applicazionee “File delle credenziali di rete di Hyperledger Fabric di esempio” a pagina 812.
- Rete Hyperledger Fabric eseguita in un cluster Kubernetes in IBM Cloud (formerly Bluemix). Per ulteriori informazioni, vedi Develop in a cloud sandbox on IBM Blockchain Platform.

Per ulteriori informazioni sul significato e sulle opzioni per tutti i parametri IBM MQ Bridge to blockchain , consultare il comando runmqbcb . È necessario considerare i propri requisiti di sicurezza e personalizzare i parametri appropriati per la propria distribuzione.

Procedura

1. Eseguire il bridge per creare un file di configurazione.

   Hai bisogno dei parametri dal tuo file delle credenziali di rete blockchain e dal tuo gestore code IBM MQ Advanced .

   ```
   runmqbcb -o config_file_name.cfg
   ```

   Come illustrato nel seguente esempio, i valori esistenti vengono visualizzati all'interno delle parentesi. Premere `Enter` per accettare i valori esistenti, premere `Space` quindi `Enter` per cancellare i valori e digitare all'interno delle parentesi, quindi premere `Enter` per aggiungere nuovi valori. È possibile separare gli elenchi di valori (come i peer) mediante virgole o immettendo ciascun valore su una nuova riga. Una riga vuota termina l'elenco.

   Nota: Non è possibile modificare i valori esistenti. È possibile conservarli, sostituirli o cancellarli.

2. Immettere i valori per la connessione al gestore code IBM MQ Advanced .

   I valori minimi necessari per la connessione sono il nome gestore code, i nomi delle code di identità e di input del bridge definite. Per le connessioni ai gestori code remoti, sono necessari anche **MQ Channel** e **MQ Conname** (indirizzo host e porta su cui è in esecuzione il gestore code). Per utilizzare TLS per la connessione a IBM MQ nel passo “4” a pagina 811, è necessario utilizzare JNDI o CCDT e specificare **MQ CCDT URL** o **JNDI implementation class** e **JNDI provider URL** di conseguenza.

   ```
   Connection to Queue Manager
   ---------------------------
   Queue Manager                      : [adv_qmgr_name]
   Bridge Input Queue                 : [APPL1.BLOCKCHAIN.INPUT.QUEUE]
   Bridge User Identity Queue         : [SYSTEM.BLOCKCHAIN.IDENTITY.QUEUE]
   MQ Channel                         : []
   MQ Conname                         : []
   MQ CCDT URL                        : []
   JNDI implementation class          :
     [com.sun.jndi.fscontext.RefFSContextFactory]
   JNDI provider URL                  : []
   MQ Userid                          : []
   MQ Password                        : []
   ```

3. 13. Immettere le credenziali del server Hyperledger Fabric per la rete.

   Esempi di ciò che dovresti aspettarti sono mostrati nel seguente codice:

   ```
   Fabric Server
   -------------
   Network configuration file         : []connection-tls.json
   Wallet                             : []
   User Name                          : []User1
   Certificate                        : []<path_to_user_certificate>
   Private Key                        : []<path_to_private_key>/private_key.pem
   Organisation                       : []Org1MSP
   ```

4. Immettere i valori di memorizzazione certificato per connessioni TLS.

   Lasciare questa area vuota se non si dispone di alcuna area.

   ```
   Certificate stores for MQ TLS connections
   -----------------------------------------
   Personal keystore                  : []
   Keystore password                  : []
   Trusted store for signer certs     : []
   Trusted store password             : []
   ```

5. Immettere il percorso del file di log in cui devono essere scritti i log del bridge.

   ```
   Behaviour of bridge program
   ---------------------------
   Runtime logfile for copy of stdout/stderr : []bridgelog.log
   ```

```
Number of logfiles                    : [3]
Maximum size of each logfile (bytes) : [2097152]
```

Attenzione: In precedenza, i dettagli relativi ai peer, agli ordinanti e all'autorità di certificazione erano memorizzati in questa configurazione del bridge. Tuttavia, queste informazioni sono ora memorizzate nel *File configurazione di rete*, collegato nella sezione del server Hyperledger Fabric della configurazione.

Risultati

È stato creato il file di configurazione che IBM MQ Bridge to blockchain utilizza per connettersi alla rete IBM Blockchain e al gestore code IBM MQ Advanced .

Operazioni successive

Eseguire le operazioni per "Esecuzione di IBM MQ Bridge to blockchain" a pagina 814.

V 9.1.4 File delle credenziali di rete di Hyperledger Fabric di esempio

Contenuto del file `.yml` dalla tua rete blockchain Hyperledger Fabric istanziata localmente in esecuzione in Docker, che puoi utilizzare per configurare il tuo IBM MQ Bridge to blockchain.

IBM MQ Bridge to blockchain è disponibile per la connessione a:

- Linux IBM MQ Advancedo
- z/OS IBM MQ Advanced for z/OS VUE

solo gestori code.

Dopo aver utilizzato le esercitazioni Introduzione a Hyperledger Fabric , aver compreso Cosa succede dietro le quintee aver avviato la tua rete utilizzando uno degli esempi Hyperledger Fabric, dovresti avere il seguente file di configurazione nella cartella `/blockchain/fabric-samples/basic-network` .

Se vuoi connetterti alla tua rete blockchain, devi utilizzare i dettagli di configurazione da questo file quando sei "Creazione del file di configurazione per IBM MQ Bridge to blockchain" a pagina 810.

```
{
  "name": "basic-network",
  "version": "1.0.0",
  "client": {
    "organization": "Org1",
    "connection": {
      "timeout": {
        "peer": {
          "endorser": "300"
        },
        "orderer": "300"
      }
    }
  },
  "channels": {
    "mychannel": {
      "orderers": [
        "orderer.example.com"
      ],
      "peers": {
        "peer0.org1.example.com": {
          "endorsingPeer": true,
          "chaincodeQuery": true,
          "ledgerQuery": true,
          "eventSource": true
        },
        "peer0.org2.example.com": {
          "endorsingPeer": true,
          "chaincodeQuery": false,
          "ledgerQuery": true,
          "eventSource": false
        }
      }
```

```
    }
  },
  "organizations": {
    "Org1": {
      "mspid": "Org1MSP",
      "peers": [
        "peer0.org1.example.com"
      ],
      "certificateAuthorities": [
        "ca-org1"
      ],
      "adminPrivateKeyPEM": {
        "path": "$<path_to_private_key>/admin_private_key"
      },
      "signedCertPEM": {
        "path": "<path_to_org_signed_cert>/Admin@org1.example.com-cert.pem"
      }
    },
    "Org2": {
      "mspid": "Org2MSP",
      "peers": [
        "peer0.org2.example.com"
      ],
      "certificateAuthorities": [
        "ca-org2"
      ]
    }
  },
  "orderers": {
    "orderer.example.com": {
      "url": "grpcs://localhost:7050",
      "mspid": "OrdererMSP",
      "grpcOptions": {
        "ssl-target-name-override": "orderer.example.com",
        "hostnameOverride": "orderer.example.com"
      },
      "tlsCACerts": {
        "path": “<path_to_orderer_cert>/ca.crt"
      },
      "adminPrivateKeyPEM": {
        "path": <path_to_orderers_private_key>/<private_key>"
      },
      "signedCertPEM": {
        "path": "<path_to_orderer_signed_cert>/Admin@example.com-cert.pem"
      }
    }
  },
  "peers": {
    "peer0.org1.example.com": {
      "url": "grpcs://localhost:7051",
      "grpcOptions": {
        "ssl-target-name-override": "peer0.org1.example.com",
        "hostnameOverride": "peer0.org1.example.com",
        "request-timeout": 120001
      },
      "tlsCACerts": {
        "path": <path_to_peer_cert>/ca.crt"
      }
    },
    "peer0.org2.example.com": {
      "url": "grpcs://localhost:9051",
      "grpcOptions": {
        "ssl-target-name-override": "peer0.org2.example.com",
        "hostnameOverride": "peer0.org2.example.com",
        "request-timeout": 120001
      },
      "tlsCACerts": {
        "path": “<path_to_peer_cert>/ca.crt"
      }
    }
  },
  "certificateAuthorities": {
    "ca-org1": {
      "url": "https://localhost:7054",
      "grpcOptions": {
        "verify": true
      },
      "tlsCACerts": {
        "path": “<path_to_ca_cert>/ca.org1.example.com-cert.pem"
      },
      "registrar": [
        {
```

```
          "enrollId": "admin",
          "enrollSecret": "adminpw"
        }
      ]
    },
    "ca-org2": {
      "url": "https://localhost:8054",
      "grpcOptions": {
        "verify": true
      },
      "tlsCACerts": {
        "path": "<path_to_ca_cert>/ca.org2.example.com-cert.pem"
      },
      "registrar": [
        {
          "enrollId": "admin",
          "enrollSecret": "adminpw"
        }
      ]
    }
  }
}
```

V 9.1.0 Esecuzione di IBM MQ Bridge to blockchain

Eseguire IBM MQ Bridge to blockchain per connettersi a IBM Blockchain e IBM MQ. Quando è connesso, il bridge è pronto per elaborare i messaggi di richiesta, inviarli alla tua rete blockchain Hyperledger Composer e ricevere ed elaborare le risposte.

Informazioni su questa attività

Utilizzare il file di configurazione creato nell'attività precedente per eseguire IBM MQ Bridge to blockchain.

Procedura

1. Avviare il gestore code IBM MQ Advanced che si desidera utilizzare con il bridge.
2. Avviare IBM MQ Bridge to blockchain per connettersi al server REST Hyperledger Composer e al gestore code IBM MQ Advanced .

   Eseguire il comando bridge.

   ```
   runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/logFile.log
   ```

   Quando il bridge è collegato, viene restituito un output simile al seguente:

   ```
   2018-05-17 14:28:16.866 BST IBM MQ Bridge to Blockchain
   5724-H72 (C) Copyright IBM Corp. 2017, 2024.

   2018-05-17 14:28:19.331 BST Ready to process input messages.
   ```

3. Opzionale: Risolvi i problemi di connessioni al tuo gestore code IBM MQ Advanced e alla tua rete blockchain, se i messaggi restituiti dopo aver eseguito il bridge indicano che una connessione non è riuscita.

   a) Immettere il comando in modo debug con l'opzione di debug 1.

   ```
   runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/logFile.log
   -d 1
   ```

   Il bridge passa attraverso la configurazione della connessione e mostra i messaggi di elaborazione in modalità concisa.

   b) Immettere il comando in modo debug con l'opzione di debug 2.

   ```
   runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/logFile.log
   -d 2
   ```

Il bridge passa attraverso la connessione impostata e mostra i messaggi di elaborazione in modalità dettagliata. L'output completo viene scritto nel file di log.

Risultati

Hai avviato IBM MQ Bridge to blockchain e ti sei connesso al tuo gestore code e alla tua rete blockchain utilizzando il tuo server REST Hyperledger Composer .

Operazioni successive

- Segui i passi in “Esecuzione dell'esempio client IBM MQ Bridge to blockchain” a pagina 818 per formattare e inviare un messaggio di query o di aggiornamento alla tua rete blockchain.
- Utilizzare la variabile *MQBCB_EXTRA_JAVA_OPTIONS* per passare le proprietà JVM, ad esempio per abilitare la funzione di traccia IBM MQ . Per ulteriori informazioni, consultare Traccia di IBM MQ Bridge to blockchain.

z/OS V 9.1.0 Formati dei messaggi per IBM MQ Bridge to blockchain prima IBM MQ 9.1.4

Informazioni sulla formattazione dei messaggi inviati e ricevuti da IBM MQ Bridge to blockchain.

LTS

Attenzione: Il formato esistente per i formati del messaggio è obsoleto. Da IBM MQ 9.1.4, se si dispone di una rete Hyperledger Fabric , utilizzare il formato dei messaggi descritti in “Formati dei messaggi per IBM MQ Bridge to blockchain da IBM MQ 9.1.4” a pagina 817.

Un'applicazione richiede che IBM MQ Bridge to blockchain esegua l'API REST definita da Hyperledger Composer per agire sulle informazioni contenute nella blockchain. L'applicazione esegue questa operazione inserendo un messaggio di richiesta nella coda di richiesta bridge. I risultati della richiesta REST vengono formattati dal ponte in un messaggio di risposta. Il bridge utilizza le informazioni contenute nei campi **ReplyToQ** e **ReplyToQMgr** da MQMD del messaggio di richiesta come destinazione per il messaggio di risposta.

I messaggi di richiesta e risposta sono messaggi di testo (MQSTR) in formato JSON.

Formato messaggio di richiesta

I messaggi di richiesta contengono tre attributi:

metodo
Il verbo REST utilizzato per richiamare la API REST Hyperledger Composer , come POST, DELETE o GET

percorso
Il percorso dell'API REST Hyperledger Composer . Questo viene aggiunto all'URL del server di base. Il percorso deve iniziare con "`api/`".

corpo
Il contenuto specifico del metodo. Questa è spesso una struttura JSON.

Il seguente esempio utilizza il metodo POST , per il percorso `api/Trader`, per creare un nuovo oggetto Trader. Il corpo specifica la classe Traders, come definito dal modello Hyperledger Composer dell'utente, e specifica anche i valori aggiuntivi necessari per creare un nuovo oggetto Trader all'interno della rete blockchain.

```
{ "method": "POST",
  "path": "api/Trader",
  "body": {
    "$class" : "org.example.trading",
    "tradeId" : "Trader2",
```

```
    "firstName": "Jane",
    "lastName" : "Doe"
```

Formato messaggio di risposta

L'ID di correlazione dei messaggi di risposta è impostato sull'ID del messaggio in entrata. Tutte le proprietà definite dall'utente vengono copiate dal messaggio di richiesta al messaggio di risposta. L'ID utente nella risposta è impostato sull'ID utente del mittente.

statusCode è un codice di stato HTTP. Se l'errore proviene da IBM MQ o dal bridge, viene utilizzato un **statusCode** appropriato.

statusType è una stringa, *SUCCESS* o *FAILURE*.

Per le richieste con esito positivo, l'elemento "**data**" nel messaggio di risposta contiene la risposta dall'API REST Hyperledger Composer richiamata.

Un esempio di elaborazione riuscita:

```
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "data": [
      {
         "$class": "org.example.trading",
         "firstName": "John",
         "lastName": "Doe",
         "tradeId": "Trader1"
      },
      {
         "$class": "org.example.trading",
         "firstName": "Jane",
         "lastName": "Doe",
         "tradeId": "Trader2"
      }
   ]
}
```

Tutte le risposte di errore hanno gli stessi campi, indipendentemente dal fatto che siano generati dal bridge stesso, dalle chiamate al server REST Hyperledger Composer , alla blockchain o dal richiamo del chaincode. Ad esempio:

- Messaggio di input JSON errato

```
{
   "statusCode": 400,
   "statusType": "FAILURE",
   "message": "[AMQBC021E] Error: Cannot parse input message or there are
    missing fields in the message. Missing fields appear to be: "method".”
}
```

- Richiesta che non è stata elaborata dal server REST Hyperledger Composer

```
{
   "statusCode": 500,
   "statusType": "FAILURE",
   "message": "Error trying to invoke business network. Error: No valid responses
    from any peers.\nResponse from attempted peer comms was an error: Error: chaincode
    error (status: 500, message: Error: Failed to add object with ID 'Trader1'
    as the object already exists)"
}
```

Le applicazioni possono indicare se la richiesta ha avuto esito positivo o negativo esaminando la stringa **statusType** o l'esistenza del campo di dati. Quando si verifica un errore nell'elaborazione del messaggio di input e il bridge non lo invia alla blockchain, il valore restituito dal bridge è un valore MQRC, di norma **MQRC_FORMAT_ERROR**.

Linux V 9.1.4 Formati dei messaggi per IBM MQ Bridge to blockchain da IBM MQ 9.1.4

Informazioni sulla formattazione dei messaggi inviati e ricevuti da IBM MQ Bridge to blockchain.

Un'applicazione richiede che IBM MQ Bridge to blockchain porti il server Hyperledger Fabric ad agire sulle informazioni contenute nella blockchain. L'applicazione esegue questa operazione inserendo un messaggio di richiesta nella coda di richiesta bridge. I risultati della richiesta vengono formattati dal bridge in un messaggio di risposta. Il bridge utilizza le informazioni contenute nei campi **ReplyToQ** e **ReplyToQMgr** da MQMD del messaggio di richiesta come destinazione per il messaggio di risposta.

I messaggi di richiesta e risposta sono messaggi di testo (MQSTR) in formato JSON e contengono quattro elementi.

Formato messaggio di richiesta

I messaggi di richiesta contengono i seguenti attributi:

operazione
Stringa - non sensibile al maiuscolo / minuscolo

`submit` per aggiornamenti o `evaluate` per query

network
Stringa - a volte nota come `channel` in Hyperledger Fabric

contratto
Stringa - lo smart contract o il pacchetto chaincode da richiamare

args
Array - di solito di stringhe, ma alcuni elementi possono essere oggetti JSON nidificati.

Gli argomenti effettivi per **`contract`**, incluso il nome del metodo.

Ad esempio:

```
{
  "operation" : "Evaluate",
  "network"   : "mychannel",
  "contract"  : "marbles0",
  "args"      : [ "readMarble" , "marble1" ]
}
```

Nota: Oltre a garantire che questi elementi esistano e che il messaggio sia JSON valido, non viene eseguita alcuna convalida del contenuto da parte del bridge. Il bridge si affida a Hyperledger Fabric per elaborare la richiesta o restituire errori.

Formato messaggio di risposta

L'ID di correlazione dei messaggi di risposta è impostato sull'ID del messaggio in entrata. Tutte le proprietà definite dall'utente vengono copiate dal messaggio di richiesta al messaggio di risposta. L'ID utente nella risposta è impostato sull'ID utente del mittente.

`statusCode` è un codice di stato HTTP. Se l'errore proviene da IBM MQ o dal bridge, viene utilizzato un **`statusCode`** appropriato.

`statusType` è una stringa, *SUCCESS* o *FAILURE*.

Per le richieste con esito positivo, l'elemento "**data**" nel messaggio di risposta contiene la risposta dall'API REST Hyperledger Composer richiamata.

Un esempio di elaborazione riuscita:

```
{
   "statusCode": 200,
   "statusType": "SUCCESS",
```

```
   "data": [
      {
         "$class": "org.example.trading",
         "firstName": "John",
         "lastName": "Doe",
         "tradeId": "Trader1"
      },
      {
         "$class": "org.example.trading",
         "firstName": "Jane",
         "lastName": "Doe",
         "tradeId": "Trader2"
      }
   ]
}
```

Tutte le risposte di errore hanno gli stessi campi, indipendentemente dal fatto che siano generati dal bridge stesso, dalle chiamate al server REST Hyperledger Composer , alla blockchain o dal richiamo del chaincode. Ad esempio:

- Messaggio di input JSON errato

```
{
   "statusCode": 400,
   "statusType": "FAILURE",
   "message": "[AMQBC021E] Error: Cannot parse input message or there are
    missing fields in the message. Missing fields appear to be: "method".”
}
```

- Richiesta che non è stata elaborata dal server REST Hyperledger Composer

```
{
   "statusCode": 500,
   "statusType": "FAILURE",
   "message": "Error trying to invoke business network. Error: No valid responses
    from any peers.\nResponse from attempted peer comms was an error: Error: chaincode
    error (status: 500, message: Error: Failed to add object with ID 'Trader1'
    as the object already exists)"
}
```

Le applicazioni possono indicare se la richiesta ha avuto esito positivo o negativo esaminando la stringa **statusType** o l'esistenza del campo di dati. Quando si verifica un errore nell'elaborazione del messaggio di input e il bridge non lo invia alla blockchain, il valore restituito dal bridge è un valore MQRC, di norma **MQRC_FORMAT_ERROR**.

z/OS V 9.1.0 Esecuzione dell'esempio client IBM MQ Bridge to blockchain

Puoi utilizzare l'esempio del client JMS fornito con IBM MQ Bridge to blockchain, per inserire un messaggio nella coda di input che il bridge blockchain sta controllando e visualizzare la risposta ricevuta. Questo esempio si basa sull'utilizzo dell'integrazione di IBM MQ Bridge to blockchain con l'esempio di rete Hyperledger Composer Trader.

Prima di iniziare

Per ulteriori informazioni, vedi /trade_network

Il tuo IBM MQ Bridge to blockchain è in esecuzione ed è connesso al tuo gestore code IBM MQ Advancedo IBM MQ Advanced for z/OS VUEe alla tua rete blockchain.

Informazioni su questa attività

Trovare l'applicazione di esempio JMS (`ComposerBCBSamp.java`) nella directory `samp` di IBM MQ Bridge to blockchain.

Ad esempio: <MQ_INSTALL_ROOT>/mqbc/samp/ComposerBCBSamp.java, dove <MQ_INSTALL_ROOT> è:

- Linux Directory in cui è installato IBM MQ
- z/OS Directory USS in cui sono installati i componenti USS di IBM MQ

.

Procedura

1. Modificare il file di origine Java di esempio client.

   Segui le istruzioni nell'esempio per configurarlo in modo che corrisponda al tuo ambiente IBM MQ e alla tua rete blockchain.

   Il seguente codice dell'esempio definisce tre messaggi di richiesta JSON da inviare al bridge:

   a. In primo luogo, per rimuovere un 'commodity' esistente

   b. In secondo luogo, per creare un nuovo 'commodity', 'owner' e i valori associati,

   c. Infine, visualizza le nuove informazioni su 'commodity', seguendo i due messaggi di richiesta precedenti

```
private static JSONObject[] createMessageBodies() {
    JSONObject[] msgs = new JSONObject[3]; // This method creates 3 messages
    JSONObject m, m2;
    String commodityName = "BC";

    // Clean out the commodity in case it's already there. If
    // it's not there, there will be an error returned from Composer.
    m = new JSONObject();
    m.put("method", "DELETE");
    m.put("path", "api/Commodity/" + commodityName);
    msgs[0] = m;

    // To add the item to the table, the
    // operation looks like this:
    //
    // { "method": "POST",
    //   "path": "api/Commodity",
    //   "body" : {
    //     "$class": "org.example.trading.Commodity",
    //     "tradingSymbol" : "BC",
    //     "description" : "BC",
    //     "mainExchange" : "HERE",
    //     "owner" : "Me",
    //     "quantity" : 100
    //   }
    // }
    // You can see this structure in the API Explorer
    m = new JSONObject();
    m.put("method", "POST");
    m.put("path", "api/Commodity");
    m2 = new JSONObject();
    m2.put("$class", " org.example.trading.Commodity");
    m2.put("tradingSymbol", commodityName);
    m2.put("description", "Blockchain Sample Description");
    m2.put("mainExchange", "My Exchange");
    m2.put("owner", "Me");
    m2.put("quantity", 100);
    m.put("body", m2);
    msgs[1] = m;

    // And list all items that have been created
    m = new JSONObject();
    m.put("method", "GET");
    m.put("path", "api/Commodity");
    msgs[2] = m;

    return msgs;
  }
```

2. Compilare l'esempio.

   Puntare alle classi client IBM MQ e al file `JSON4J.jar` fornito nella directory bridge.

```
javac -cp <MQ_INSTALL_ROOT>/java/lib/*:<MQ_INSTALL_ROOT>/mqbc/prereqs/JSON4J.jar
ComposerBCBClient.java
```

3. Eseguire la classe compilata.

```
java -cp <MQ_INSTALL_ROOT>/java/lib/*:<MQ_INSTALL_ROOT>/mqbc/prereqs/JSON4J.jar:.
ComposerBCBClient
```

```
Starting Simple MQ Blockchain Bridge Client
Starting the connection.
Sent message:
  {"method":"DELETE"," path ":"api\/Commodity\/BC"}
Response text:
{
   "statusCode": 204,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": ""
}
SUCCESS
Sent message:
{"body":
{"$class":"org.example.trading.Commodity","owner":"Me","quantity":100,"description":"Blockcha
in Sample Description","mainExchange":"My
Exchange","tradingSymbol":"BC"},"operation":"POST","url":"Commodity"}
Response text:
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": {
      "$class": "org.example.trading.Commodity",
      "description": "Blockchain Sample Description",
      "mainExchange": "My Exchange",
      "owner": "Me",
      "quantity": 100,
      "tradingSymbol": "BC"
   }
}
SUCCESS
Sent message:
  {"method":"GET","path":"api\/Commodity"}
Response text:
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": [
      {
         "$class": "org.example.trading.Commodity",
         "description": "Blockchain Sample Description",
         "mainExchange": "My Exchange",
         "owner": "resource:org.example.trading.Trader#Me",
         "quantity": 100,
         "tradingSymbol": "BC"
      }
   ]
}
SUCCESS
```

Il campo **message** contiene "OK" per un messaggio elaborato correttamente oppure, in caso di richiesta non riuscita, informazioni relative al motivo dell'errore.

Se il client riceve un errore di timeout in attesa della risposta, verificare che il bridge sia in esecuzione.

Linux V 9.1.2 Opzioni di configurazione aggiuntive per IBM MQ Bridge to blockchain

IBM MQ 9.1.2 introduce una modifica al modo in cui la traccia e la registrazione funzionano su IBM MQ Bridge to blockchain.

Modifiche da IBM MQ 9.1.0 IBM MQ Bridge to blockchain

Per impostazione predefinita, non ci sono modifiche al comportamento dal bridge IBM MQ 9.1.0 , a parte il file di log che ora inizia a ruotare. Per ulteriori informazioni, consultare “Rotazione dei log” a pagina 821.

Interazione di traccia e debug

L'indicatore di debug continua ad agire come prima. Ovvero, *-d1* fornisce informazioni di debug del bridge e *-d2* attiva la registrazione di debug per i componenti prerequisiti. Tuttavia, se è stata abilitata la traccia IBM MQ quando si avvia il bridge, il report di livello *-d2* viene attivato automaticamente.

Rotazione dei log

Il comportamento predefinito per il file di log cambia per avere tre file di log, ciascuno di dimensione 2 MB. È possibile sovrascrivere questi valori utilizzando ulteriori proprietà di configurazione. L'attributo di configurazione esistente o il parametro della riga comandi per il file di log, viene utilizzato come nome di base per i log, con un indice aggiunto.

Se il file di log configurato ha:

- Nessun tipo di file, l'indice viene aggiunto alla fine del nome file.

  Impostando il file di log su `abc`, si ottengono log denominati `abc.0`, `abc.1`e così via.
- Un tipo di file, l'indice viene inserito prima del tipo di file.

  Impostando il file di log su `abc.log`, si ottengono log denominati `abc.0.log`, `abc.1.log`e così via.

Note:

1. Poiché i bridge possono essere in esecuzione con autorizzazioni utente arbitrarie, non è possibile forzare una particolare directory, ad esempio, `/var/mqm/qmgrs/<qm>/errors`, per i log.
2. Le stesse informazioni continuano ad essere scritte negli stream *stdout* e *stderr* .
3. Ogni volta che un singolo file di log viene riaperto, le informazioni di configurazione di base vengono ristampate. Le informazioni saranno sempre disponibili, invece di essere stampate una sola volta all'avvio del programma.

z/OS Configurazione dei gestori code su z/OS

Utilizzare queste istruzioni per configurare i gestori code su IBM MQ for z/OS.

Prima di iniziare

Prima di configurare IBM MQ, leggere le informazioni sui concetti di IBM MQ for z/OS in Concetti diIBM MQ for z/OS.

z/OS Leggi come pianificare il tuo ambiente IBM MQ for z/OS in Pianificazione del tuo ambiente IBM MQ su z/OS .

Informazioni su questa attività

Dopo aver installato IBM MQ, è necessario eseguire una serie di attività prima di renderlo disponibile agli utenti.

Procedura

- Consultare i seguenti argomenti secondari per informazioni su come configurare i gestori code su IBM MQ for z/OS.

Concetti correlati

Concetti di IBM MQ for z/OS

Attività correlate

“Creazione di gestori code su più piattaforme” a pagina 7
Prima di poter utilizzare messaggi e code, è necessario creare e avviare almeno un gestore code e i relativi oggetti associati. 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 MQ .

Protezione

“Configurazione dell'accodamento distribuito” a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

“Configurazione delle connessioni tra client e server” a pagina 15
Per configurare i link di comunicazione tra IBM MQ MQI clients e server, decidere il protocollo di comunicazione, definire le connessioni ad entrambe le estremità del link, avviare un listener e definire canali.

z/OS AmministrazioneIBM MQ for z/OS

Pianificazione

z/OS Immissione di comandi

Riferimenti correlati

z/OS I programmi di utilità IBM MQ for z/OS

z/OS Preparazione alla personalizzazione dei gestori code su z/OS

Utilizzare questo argomento quando si personalizzano i gestori code con i dettagli delle funzioni installabili, le funzioni di lingua nazionale e le informazioni sulla verifica e l'impostazione della sicurezza.

Preparazione per la personalizzazione

Program Directory elenca il contenuto del nastro di installazione IBM MQ , le informazioni sul livello di servizio e sul programma per IBM MQe descrive come installare IBM MQ for z/OS utilizzando SMP/E (System Modification Program Extended). Program Directory for IBM MQ for z/OS può essere scaricato da Centro pubblicazioni IBM (consultare File PDF diIBM MQ for z/OS Program Directory).

Una volta installato IBM MQ, è necessario eseguire una serie di attività prima di renderlo disponibile agli utenti. Per una descrizione di queste attività, consultare le seguenti sezioni:

- “Configurazione di IBM MQ for z/OS” a pagina 827
- “Test di un gestore code su z/OS” a pagina 892
- Impostazione della sicurezza su z/OS

Se si sta eseguendo la migrazione da una versione precedente di IBM MQ for z/OS, non è necessario eseguire la maggior parte delle attività di personalizzazione. Consultare Manutenzione e migrazione per ulteriori informazioni sulle attività che è necessario eseguire.

Funzioni installabili di IBM MQ for z/OS

IBM MQ for z/OS comprende le funzioni riportate di seguito:

Base
Ciò è necessario; comprende tutte le funzioni principali, tra cui

- Amministrazione e programmi di utilità
- Supporto per applicazioni di tipo CICS, IMSe batch utilizzando IBM MQ Application Programming Interface o C++

- Funzione di accodamento distribuito (che supporta le comunicazioni TCP/IP e APPC)

Caratteristiche della lingua nazionale

Questi contengono messaggi di errore e pannelli in tutte le lingue nazionali supportate. A ogni lingua è associata una lettera di lingua. Le lingue e le lettere sono:

C

Cinese semplificato

E

U.S. Inglese (maiuscolo / minuscolo)

F

Franco francese

K

Giapponese

U

U.S. Inglese (maiuscolo)

È necessario installare l'opzione Inglese (maiuscolo / minuscolo). È anche possibile installare una o più altre lingue. (Il processo di installazione per altre lingue richiede l'installazione dell'inglese americano (maiuscolo / minuscolo), anche se non si utilizza l'inglese americano (maiuscolo / minuscolo).)

Componenti di IBM MQ for z/OS Unix System Services

Questa funzione è facoltativa. Selezionare questa funzione se si desidera creare ed eseguire applicazioni Java che utilizzano Java Message Service (JMS) per connettersi a IBM MQ for z/OS o se si desidera creare ed eseguire applicazioni HTTP che utilizzano HTTP per connettersi a IBM MQ for z/OS.

V 9.1.0 **Componenti web IBM MQ for z/OS Unix System Services**

Questa funzione è facoltativa.

Selezionare questa funzione se si desidera utilizzare IBM MQ Consoleo REST API.

Per installare questa funzione, è necessario installare la funzione IBM MQ for z/OS Unix System Services Components.

Librerie esistenti dopo l'installazione

IBM MQ viene fornito con un numero di librerie di caricamento separate. Tabella 53 a pagina 823 mostra le librerie che potrebbero esistere dopo aver installato IBM MQ.

Tabella 53. Librerie IBM MQ esistenti dopo l'installazione

Nome	Descrizione
thlqual.SCSQANLC	Contiene i moduli di caricamento per la versione in cinese semplificato di IBM MQ.
thlqual.SCSQANLE	Contiene i moduli di caricamento per U.S. Versione inglese (maiuscolo / minuscolo) di IBM MQ.
thlqual.SCSQANLF	Contiene i moduli di caricamento per la versione francese di IBM MQ.
thlqual.SCSQANLK	Contiene i moduli di caricamento per la versione giapponese di IBM MQ.
thlqual.SCSQANLU	Contiene i moduli di caricamento per U.S. Versione inglese (maiuscolo) di IBM MQ.
thlqual.SCSQASMS	Contiene l'origine per i programmi di esempio assembler.

Tabella 53. Librerie IBM MQ esistenti dopo l'installazione (Continua)

Nome	Descrizione
thlqual.SCSQAUTH	Il repository principale per tutti i moduli di caricamento del prodotto IBM MQ ; contiene anche il modulo dei parametri predefinito, CSQZPARM. Questa libreria deve essere autorizzata da APF e in formato PDS - E.
thlqual.SCSQCICS	Contiene moduli di carico aggiuntivi che devono essere inclusi nella concatenazione DFHRPL CICS . Questa libreria deve essere autorizzata da APF e in formato PDS - E.
thlqual.SCSQCLST	Contiene CLIST utilizzati dai programmi di esempio.
thlqual.SCSQCOBC	Contiene i copybook COBOL, inclusi i copybook richiesti per i programmi di esempio.
thlqual.SCSQCOBS	Contiene l'origine per i programmi di esempio COBOL.
thlqual.SCSQCPPS	Contiene l'origine per i programmi di esempio C + +.
thlqual.SCSQC37S	Contiene l'origine per i programmi di esempio C.
thlqual.SCSQC370	Contiene intestazioni C, incluse le intestazioni richieste per i programmi di esempio.
thlqual.SCSQDEFS	Contiene le definizioni laterali per C++ e i DBRM Db2 per l'accodamento condiviso.
thlqual.SCSQEXEC	Contiene i file eseguibili REXX da includere nella concatenazione SYSEXEC o SYSPROC se si utilizzano le operazioni IBM MQ e i pannelli di controllo.
thlqual.SCSQHPPS	Contiene file di intestazione per C + +.
thlqual.SCSQINST	Contiene JCL per lavori di installazione.
thlqual.SCSQLINK	Libreria di codice iniziale. Contiene i moduli di caricamento caricati all'IPL (initial program load) del sistema. La libreria deve essere autorizzata da APF.
thlqual.SCSQLOAD	Caricare la libreria. Contiene moduli di caricamento per codice non APF, uscite utente, programmi di utilità, esempi, programmi di verifica dell'installazione e stub dell'adattatore. Non è necessario che la libreria disponga dell'autorizzazione APF e che non sia presente nell'elenco dei collegamenti. Questa libreria deve essere in formato PDS - E.
thlqual.SCSQMACS	Contiene macro Assembler incluse: macro di esempio, macro del prodotto e macro dei parametri di sistema.
thlqual.SCSQMAPS	Contiene le serie di mappe CICS utilizzate dai programmi di esempio.
thlqual.SCSQMSGC	Contiene i messaggi ISPF da includere nella concatenazione ISPMLIB se si utilizza la funzione di lingua cinese semplificato per le operazioni e i pannelli di controllo di IBM MQ .
thlqual.SCSQMSGE	Contiene i messaggi ISPF da includere nella concatenazione ISPMLIB se si utilizza U.S. Funzione di lingua inglese (maiuscolo / minuscolo) per le operazioni e i pannelli di controllo IBM MQ .

Tabella 53. Librerie IBM MQ esistenti dopo l'installazione (Continua)

Nome	Descrizione
thlqual.SCSQMSGF	Contiene messaggi ISPF da includere nella concatenazione ISPMLIB se si utilizza la funzione di lingua francese per le operazioni e i pannelli di controllo di IBM MQ .
thlqual.SCSQMSGK	Contiene i messaggi ISPF da includere nella concatenazione ISPMLIB se si utilizza la funzione lingua giapponese per le operazioni e i pannelli di controllo di IBM MQ .
thlqual.SCSQMSGU	Contiene i messaggi ISPF da includere nella concatenazione ISPMLIB se si utilizza U.S. Funzione lingua inglese (maiuscolo) per le operazioni e i pannelli di controllo IBM MQ .
thlqual.SCSQMVR1	Contiene i moduli di caricamento per l'accodamento distribuito. Questa libreria deve essere autorizzata da APF e in formato PDS - E.
thlqual.SCSQPLIC	Contiene i file di inclusione PL/I.
thlqual.SCSQPLIS	Contiene l'origine per i programmi di esempio PL/I.
thlqual.SCSQPNLA	Contiene i pannelli IPCS, per il programma di formattazione dump, da includere nella concatenazione ISPPLIB. Contiene anche i pannelli per programmi di esempio IBM MQ .
thlqual.SCSQPNLC	Contiene i pannelli ISPF da includere nella concatenazione ISPPLIB se si utilizza la funzione di lingua cinese semplificato per le operazioni IBM MQ e i pannelli di controllo.
thlqual.SCSQPNLE	Contiene i pannelli ISPF da includere nella concatenazione ISPPLIB se si utilizza U.S. Funzione di lingua inglese (maiuscolo / minuscolo) per le operazioni e i pannelli di controllo IBM MQ .
thlqual.SCSQPNLF	Contiene i pannelli ISPF da includere nella concatenazione ISPPLIB se si sta utilizzando la funzione di lingua francese per le operazioni IBM MQ e i pannelli di controllo.
thlqual.SCSQPNLK	Contiene i pannelli ISPF da includere nella concatenazione ISPPLIB se si utilizza la funzione di lingua giapponese per le operazioni IBM MQ e i pannelli di controllo.
thlqual.SCSQPNLU	Contiene i pannelli ISPF da includere nella concatenazione ISPPLIB se si utilizza U.S. Funzione lingua inglese (maiuscolo) per le operazioni e i pannelli di controllo IBM MQ .
thlqual.SCSQPROC	Contiene il JCL di esempio e i dataset di inizializzazione del sistema predefiniti.
thlqual.SCSQSNLC	Contiene i moduli di caricamento per le versioni in cinese semplificato dei moduli IBM MQ richiesti per la funzione di scopo speciale (ad esempio, il codice iniziale).
thlqual.SCSQSNLE	Contiene i moduli di caricamento per U.S. Versioni in inglese (maiuscole e minuscole) dei moduli IBM MQ richiesti per la funzione per scopi speciali (ad esempio il codice iniziale).
thlqual.SCSQSNLF	Contiene i moduli di caricamento per le versioni francesi dei moduli IBM MQ richiesti per funzioni speciali (ad esempio il codice iniziale).

Tabella 53. Librerie IBM MQ esistenti dopo l'installazione (Continua)	
Nome	**Descrizione**
thlqual.SCSQSNLK	Contiene i moduli di caricamento per le versioni giapponesi dei moduli IBM MQ richiesti per la funzione per scopi speciali (ad esempio, il codice iniziale).
thlqual.SCSQSNLU	Contiene i moduli di caricamento per U.S. Versioni in inglese (maiuscolo) dei moduli IBM MQ richiesti per la funzione per scopi speciali (ad esempio, il codice iniziale).
thlqual.SCSQTBLC	Contiene tabelle ISPF da includere nella concatenazione ISPTLIB se si utilizza la funzione di lingua cinese semplificato per le operazioni e i pannelli di controllo IBM MQ .
thlqual.SCSQTBLE	Contiene tabelle ISPF da includere nella concatenazione ISPTLIB se si utilizza U.S. Funzione di lingua inglese (maiuscolo / minuscolo) per le operazioni e i pannelli di controllo IBM MQ .
thlqual.SCSQTBLF	Contiene tabelle ISPF da includere nella concatenazione ISPTLIB se si utilizza la funzione di lingua francese per le operazioni IBM MQ e i pannelli di controllo.
thlqual.SCSQTBLK	Contiene le tabelle ISPF da includere nella concatenazione ISPTLIB se si utilizza la funzione di lingua giapponese per le operazioni IBM MQ e i pannelli di controllo.
thlqual.SCSQTBLU	Contiene tabelle ISPF da includere nella concatenazione ISPTLIB se si utilizza U.S. Funzione lingua inglese (maiuscolo) per le operazioni e i pannelli di controllo IBM MQ .

Nota: Non modificare o personalizzare nessuna di queste librerie. Se si desidera apportare modifiche, copiare le librerie e apportare le modifiche alle copie.

Concetti correlati

Concetti di IBM MQ for z/OS

"Utilizzo di IBM MQ con IMS" a pagina 932
L'adattatore IBM MQ -IMS e il bridge IBM MQ - IMS sono i due componenti che consentono a IBM MQ di interagire con IMS.

"Utilizzo di IBM MQ con CICS" a pagina 941
Per utilizzare IBM MQ con CICS, è necessario configurare l'adattatore IBM MQ CICS e, facoltativamente, i componenti IBM MQ CICS bridge .

"Utilizzo delle uscite OTMA in IMS" a pagina 943
Utilizzare questo argomento se si desidera utilizzare le uscite IMS Open Transaction Manager Access con IBM MQ for z/OS.

Attività correlate

"Impostazione delle comunicazioni con altri gestori code su z/OS" a pagina 901
Questa sezione descrive le preparazioni IBM MQ for z/OS che è necessario effettuare prima di poter iniziare a utilizzare l'accodamento distribuito.

AmministrazioneIBM MQ for z/OS

Riferimenti correlati

"Aggiornamento e applicazione del servizio a Language Environment o z/OS Callable Services" a pagina 941
Le azioni che è necessario eseguire variano a seconda che si utilizzi CALLLIBS o LINK e la versione di SMP/E.

z/OS Configurazione di IBM MQ for z/OS

Utilizzare questo argomento come guida dettagliata per personalizzare il sistema IBM MQ for z/OS .

Il modo migliore per configurare un gestore code consiste nell'effettuare le seguenti operazioni nell'ordine mostrato:

1. Configurare il gestore code di base.
2. Configurare l'iniziatore del canale, che esegue le comunicazioni da gestore code a gestore code e le comunicazioni dell'applicazione client remota.
3. Se si desidera crittografare o proteggere i messaggi, configurare Advanced Message Security for z/OS.
4. Se si desidera utilizzare IBM MQ per trasferire i file, configurare Managed File Transfer for z/OS.
5. Se si desidera utilizzare il REST APIdi gestione o di messaggistica o il MQ Console per gestire IBM MQ da un browser Web, configurare il server mqweb.

Questo argomento illustra le diverse fasi di configurazione di IBM MQ dopo averlo installato correttamente. Il processo di installazione è descritto in Program Directory. Program Directory for IBM MQ for z/OS può essere scaricato da Centro pubblicazioni IBM (consultare File PDF diIBM MQ for z/OS Program Directory).

Gli esempi vengono forniti con IBM MQ per facilitare la personalizzazione. I membri del dataset di esempio hanno nomi che iniziano con quattro caratteri CSQ4 e si trovano nella libreria thlqual.SCSQPROC.

Prima di eseguire le attività di personalizzazione descritte in questo argomento, è necessario considerare una serie di opzioni di configurazione perché influenzano le prestazioni e i requisiti di risorsa di IBM MQ for z/OS. Ad esempio, è necessario decidere quali librerie di globalizzazione si desidera utilizzare.

Se si desidera automatizzare alcuni dei passi di personalizzazione, consultare “Utilizzo di IBM z/OSMF per automatizzare IBM MQ” a pagina 948.

Opzioni di configurazione

Per ulteriori informazioni su tali opzioni, consultare Pianificazione su z/OS.

La descrizione di ciascuna attività in questa sezione indica se:

- L'attività fa parte del processo di configurazione di IBM MQ. Ciò significa che si esegue l'attività una sola volta quando si personalizza IBM MQ nel sistema z/OS . (In un sysplex parallelo, è necessario eseguire l'attività per ogni z/OS sistema nel sysplex e verificare che ogni sistema z/OS sia impostato in maniera identica.)
- L'attività fa parte dell'aggiunta di un gestore code. In altre parole, l'attività viene eseguita una sola volta per ogni gestore code quando si aggiunge tale gestore code.

Nessuna delle attività richiede l'esecuzione di un IPL del sistema z/OS , se si utilizzano i comandi per modificare i diversi parametri di sistema z/OS ed eseguire “Aggiornare SYS1.PARMLIB” a pagina 842 come suggerito.

Per semplificare le operazioni e facilitare la determinazione dei problemi, accertarsi che tutti i sistemi z/OS in un sysplex siano configurati in modo identico, in modo che i gestori code possano essere creati rapidamente su qualsiasi sistema in caso di emergenza.

Per semplificare la manutenzione, considerare la definizione degli alias per fare riferimento alle librerie IBM MQ ; per ulteriori informazioni, consultare Utilizzo di un alias per fare riferimento a una libreria IBM MQ.

Concetti correlati

Concetti di IBM MQ for z/OS

“Utilizzo di IBM MQ con IMS” a pagina 932
L'adattatore IBM MQ -IMS e il bridge IBM MQ - IMS sono i due componenti che consentono a IBM MQ di interagire con IMS.

“Utilizzo di IBM MQ con CICS” a pagina 941

Per utilizzare IBM MQ con CICS, è necessario configurare l'adattatore IBM MQ CICS e, facoltativamente, i componenti IBM MQ CICS bridge .

“Utilizzo delle uscite OTMA in IMS” a pagina 943
Utilizzare questo argomento se si desidera utilizzare le uscite IMS Open Transaction Manager Access con IBM MQ for z/OS.

Attività correlate

“Impostazione delle comunicazioni con altri gestori code su z/OS” a pagina 901
Questa sezione descrive le preparazioni IBM MQ for z/OS che è necessario effettuare prima di poter iniziare a utilizzare l'accodamento distribuito.

AmministrazioneIBM MQ for z/OS

Riferimenti correlati

“Aggiornamento e applicazione del servizio a Language Environment o z/OS Callable Services” a pagina 941
Le azioni che è necessario eseguire variano a seconda che si utilizzi CALLLIBS o LINK e la versione di SMP/E.

Informazioni correlate

Program Directory per IBM MQ for z/OS

z/OS Configurazione del sistema z/OS per IBM MQ

Utilizzare questi argomenti come guida dettagliata per la personalizzazione del sistema IBM MQ for z/OS .

z/OS *Identificare i parametri di sistema z/OS*

Alcune delle attività implicano l'aggiornamento dei parametri di sistema z/OS . È necessario conoscere quali sono stati specificati quando è stato eseguito l'IPL del sistema.

- *È necessario eseguire questa attività una volta per ogni sistema z/OS in cui si desidera eseguire IBM MQ.*
- *Potrebbe essere necessario eseguire questa attività durante la migrazione da una versione precedente.*

SYS1.PARMLIB(IEASYSpp) contiene un elenco di parametri che puntano ad altri membri di SYS1.PARMLIB (dove pp rappresenta l'elenco di parametri di sistema z/OS utilizzato per eseguire un IPL del sistema).

Le voci che è necessario trovare sono:

Per “L'APF autorizza le librerie di caricamento IBM MQ” a pagina 828:
PROG=xx o APF=aa puntano all'elenco di librerie autorizzate APF (Authorized Program Facility) (membro PROGxx o IEFAPFaa)

Per “Aggiornare l'elenco di link z/OS e LPA” a pagina 830:
LNK=kk punta alla lista dei collegamenti (membro LNKLSTkk) LPA=mm punta alla lista LPA (membro LPALSTmm)

Per “Aggiornare la tabella delle proprietà del programma z/OS” a pagina 833:
SCH=xx punta alla tabella delle proprietà del programma (PPT) (membro SCHEDxx)

Per “Definire il sistema secondario IBM MQ in z/OS” a pagina 834:
SSN=ss punta all'elenco dei sottosistemi definiti (membro IEFSSNss)

z/OS *L'APF autorizza le librerie di caricamento IBM MQ*

Autorizzazione APF per varie librerie. Alcuni moduli di caricamento potrebbero già essere autorizzati.

- *È necessario eseguire questa attività una volta per ogni sistema z/OS in cui si desidera eseguire IBM MQ.*
- *Se si utilizzano gruppi di condivisione code, è necessario assicurarsi che le impostazioni per IBM MQ siano identiche su ogni z/OS sistema nel sysplex.*
- *Potrebbe essere necessario eseguire questa attività durante la migrazione da una versione precedente.*
- *Utilizzo di LLA (Library Look aside):*

– *Alcuni IBM MQ utilizzi possono causare un elevato I/O (Input / Output) per caricare i moduli dalle librerie. Questo IO può essere ridotto utilizzando la funzionalità LLA del sistema operativo.*
– *Questo IO elevato può verificarsi durante:*
  - *Applicazioni con una frequenza MQCONN/MQDISC elevata, ad esempio in una procedura memorizzata WLM*
  - *Caricamento delle uscite del canale. Se si dispone di canali che si avviano e si arrestano frequentemente e si utilizzano uscite canale.*

– *Il membro CSVLLAxx in SYS1.PARMLIB specifica l'impostazione LLA. L'inclusione di un nome di libreria nell'istruzione LIBRARIES significa che una copia di programma verrà sempre presa da VLF (Virtual Lookaside Facility) e quindi di solito non richiederà I/O quando viene utilizzata in modo massiccio.*

  L'inclusione nell'istruzione FREEZE significa che non c'è alcun I/O per ottenere le directory di concatenazione delle istruzioni DD rilevanti (spesso può essere più I/O del caricamento del programma stesso).

  Utilizzare il comando del sistema operativo " F LLA, REFRESH " dopo eventuali modifiche a una di queste librerie.

Le IBM MQ librerie di caricamento thlqual.SCSQAUTH e thlqual.SCSQLINK devono essere autorizzate da APF. È inoltre necessario autorizzare APF le librerie per la funzione lingua nazionale (thlqual.SCSQANLx e thlqual.SCSQSNLx) e per la funzione di accodamento distribuito (thlqual.SCSQMVR1). Se si utilizza Advanced Message Security , è necessario autorizzare anche APF la libreria thlqual.SDRQAUTH.

Tuttavia, tutti i moduli di caricamento in LPA sono automaticamente autorizzati APF. Così sono tutti i membri dell'elenco di link se SYS1.PARMLIB membro IEASYSpp contiene l'istruzione:

```
LNKAUTH=LNKLST
```

LNKAUTH=LNKLST è il valore predefinito se LNKAUTH non è specificato.

A seconda di ciò che si sceglie di inserire nell'LPA o nell'elenco di collegamenti (consultare “Aggiornare l'elenco di link z/OS e LPA” a pagina 830), potrebbe non essere necessario inserire le librerie nell'elenco di collegamenti APF

Nota: È necessario autorizzare con APF tutte le librerie incluse in IBM MQ STEPLIB. Se si inserisce una libreria non autorizzata ad APF in STEPLIB, l'intera concatenazione di librerie perde la relativa autorizzazione APF.

Gli elenchi APF si trovano in SYS1.PARMLIB membro PROGxx o IEAAPFaa. Gli elenchi contengono i nomi delle librerie z/OS autorizzate APF. L'ordine delle voci negli elenchi non è significativo. Per informazioni sugli elenchi APF, consultare il manuale *z/OS MVS Initialization and Tuning Reference* .

Per ulteriori informazioni sull'ottimizzazione del sistema, consultare SupportPac MP16

Se si utilizzano membri PROGxx con formato dinamico, è necessario immettere solo il comando z/OS `SETPROG APF,ADD,DSNAME=hlq.SCSQ XXXX,VOLUME= YYYYYY` per rendere effettive le modifiche: dove *XXXX* varia in base al nome della libreria e dove *YYYYY* è il volume. Altrimenti, se si utilizza il formato statico o i membri IEAAPFaa, è necessario eseguire un IPL sul sistema.

Tenere presente che è necessario utilizzare il nome effettivo della libreria nell'elenco APF. Se si tenta di utilizzare l'alias del dataset della libreria, l'autorizzazione ha esito negativo.

Concetti correlati

“Aggiornare l'elenco di link z/OS e LPA” a pagina 830
Aggiornare le librerie LPA con la nuova versione delle prime librerie di codice. L'altro codice può essere inserito nell'elenco dei link o nell'area LPA.

“Preparazione alla personalizzazione dei gestori code su z/OS” a pagina 822

Utilizzare questo argomento quando si personalizzano i gestori code con i dettagli delle funzioni installabili, le funzioni di lingua nazionale e le informazioni sulla verifica e l'impostazione della sicurezza.

z/OS *Aggiornare l'elenco di link z/OS e LPA*

Aggiornare le librerie LPA con la nuova versione delle prime librerie di codice. L'altro codice può essere inserito nell'elenco dei link o nell'area LPA.

- È necessario eseguire questa attività una volta per ogni sistema z/OS in cui si desidera eseguire IBM MQ.
- Se si utilizzano gruppi di condivisione code, è necessario aggiornare il codice iniziale in ciascun gestore code in QSG al livello IBM MQ 9.1.0 prima di migrare uno qualsiasi dei gestori code a IBM MQ 9.1.0.

  Installare l'ultimo codice iniziale su ogni LPAR, quindi aggiornare i gestori code uno alla volta prima della migrazione. Non è necessario migrare tutti i gestori code contemporaneamente.
- Potrebbe essere necessario eseguire questa attività quando si esegue la migrazione da una versione precedente. Per ulteriori dettagli, consultare Program Directory. Program Directory for IBM MQ for z/OS può essere scaricato da Centro pubblicazioni IBM (consultare File PDF diIBM MQ for z/OS Program Directory).

Nota: Il dataset per LPA è specifico della versione. Se si sta utilizzando un LPA esistente nel sistema, contattare l'amministratore di sistema per decidere quale LPA utilizzare.

Codice iniziale

Alcuni moduli di caricamento IBM MQ devono essere aggiunti a MVS perché IBM MQ agisca come un sottosistema. Questi moduli sono noti come codice Early e possono essere eseguiti anche se un gestore code non è attivo. Ad esempio, quando un comando operatore viene emesso sulla console con un prefisso di comando IBM MQ , questo codice Early acquisirà il controllo e controllerà se è necessario avviare un gestore code o passare la richiesta a un gestore code in esecuzione. Questo codice viene caricato in LPA (Link Pack Area). Esiste una serie di moduli Early, utilizzati per tutti i gestori code, che devono essere al livello più alto di IBM MQ. Il codice iniziale proveniente da una versione superiore di IBM MQ funzionerà con un gestore code con una versione inferiore di IBM MQ, ma non il contrario.

Il codice iniziale comprende i seguenti moduli di caricamento:

- CSQ3INI e CSQ3EPX nella libreria thqual.SCSQLINK
- CSQ3ECMX nella libreria thqual.SCSQSNL *x*, dove *x* è la lettera della lingua:
  - thlqual.SCSQSNLE, per l'inglese americano con lettere maiuscole e minuscole
  - thlqual.SCSQSNLU, per l'inglese americano maiuscolo
  - thlqual.SCSQSNLK, per il giapponese
  - thlqual.SCSQSNLF, per il francese
  - thlqual.SCSQSNLC, per il cinese

IBM MQ include una modifica utente che sposta il contenuto della libreria thqual.SCSQSNL *i* nella libreria thqual.SCSQLINK e informa SMP/E. Questa modifica utente è denominata CSQ8UERL ed è descritta in *Program Directory for IBM MQ for z/OS* , per Long Term Support o Continuous Delivery. Program Directory for IBM MQ for z/OS può essere scaricato da Centro pubblicazioni IBM (consultare File PDF diIBM MQ for z/OS Program Directory).

Una volta aggiornato il codice iniziale nelle librerie LPA, sarà disponibile dal successivo IPL z/OS (con l'opzione CLPA) a tutti i sottosistemi del gestore code aggiunti durante l'IPL dalle definizioni nei membri IEFSSNss in SYS1.PARMLIB.

È possibile renderla immediatamente disponibile senza un IPL per qualsiasi nuovo sottosistema del gestore code aggiunto successivamente (come descritto in “Definire il sistema secondario IBM MQ in z/OS” a pagina 834) aggiungendolo all'LPA come segue:

- Se non è stato utilizzato CSQ8UERL, immettere i seguenti comandi z/OS :

```
SETPROG LPA,ADD,MODNAME=(CSQ3INI,CSQ3EPX),DSNAME=thqual.SCSQLINK
SETPROG LPA,ADD,MODNAME=(CSQ3ECMX),DSNAME=thqual.SCSQSNL x
```

- Se si utilizza CSQ8UERL, è possibile caricare il codice iniziale nell'area LPA utilizzando il comando z/OS riportato di seguito:

```
SETPROG LPA,ADD,MASK=*,DSNAME=thqual.SCSQLINK
```

- Se si utilizza Advanced Message Security , è necessario immettere anche il seguente comando z/OS per includere un modulo aggiuntivo nell'area LPA:

```
SETPROG LPA,ADD,MODNAME=(CSQ0DRTM),DSNAME=thqual.SCSQLINK
```

Se è stata applicata la manutenzione o se si intende riavviare un gestore code con una versione o una release successive di IBM MQ, il codice precedente può essere reso disponibile per i gestori code esistenti utilizzando la seguente procedura. I gestori code per i quali non si eseguono queste operazioni continuano a utilizzare la versione del codice iniziale già utilizzata. Non è necessario eseguire questa procedura per tutti i gestori code su una LPAR, a meno che non si stia specificamente tentando di applicare la manutenzione a tutti i gestori code o di aggiornarli tutti a una versione o release più recenti di IBM MQ.

1. Aggiungerlo all'LPA utilizzando i comandi z/OS SETPROG come descritto in precedenza in questo argomento.
2. Arrestare il gestore code utilizzando il comando IBM MQ STOP QMGR.
3. Accertarsi che qmgr.REFRESH.QMGR è impostato. Consultare Comandi MQSC, profili e relativi livelli di accesso.
4. Aggiornare il codice iniziale per il gestore code utilizzando il comando IBM MQ REFRESH QMGR TYPE (EARLY).
5. Riavviare il gestore code utilizzando il comando IBM MQ START QMGR.

I comandi IBM MQ STOP QMGR, REFRESH QMGR e START QMGR sono descritti in Comandi MQSC.

Altro codice

Tutti i moduli di caricamento forniti da IBM MQ nelle seguenti librerie sono rientranti e possono essere inseriti nell'area LPA:

- SCSQAUTH
- SCSQANL *x*, dove *x* è la tua lettera della lingua
- SCSQMVR1

Importante: Tuttavia, se si posizionano le librerie nell'area LPA, ogni volta che si applica la manutenzione, è necessario copiare manualmente i moduli modificati nell'area LPA. Pertanto, è preferibile inserire le librerie di caricamento IBM MQ nell'elenco dei collegamenti, che possono essere aggiornati dopo la manutenzione immettendo il comando z/OS REFRESH LLA.

Questo è particolarmente consigliato per SCSQAUTH in modo che non sia necessario includerlo in diversi STEPLIBs. Solo una libreria di lingua, SCSQANL *x* , deve essere inserita nell'elenco LPA o link. Le librerie dell'elenco dei collegamenti sono specificate in un membro LNKLSTkk di SYS1.PARMLIB.

La funzione di accodamento distribuito e CICS bridge (ma non il gestore code stesso) richiedono l'accesso alla libreria di runtime LE (Language Environment) SCEERUN. Se si utilizza una di queste funzioni, è necessario includere SCEERUN nell'elenco dei collegamenti.

Alcuni moduli vengono caricati all'avvio del gestore code in ECSA. Negli ambienti vincolati ECSA, è possibile inserire questi moduli nell'area LPA. Per ulteriori informazioni, consultare “Inserimento di moduli globali IBM MQ nell'area LPA” a pagina 832.

Importante: Per utilizzare questa funzione in IBM MQ 9.1 è necessario applicare l'APAR PH52358.

Concetti correlati

“Aggiornare la tabella delle proprietà del programma z/OS” a pagina 833
Alcune voci PPT aggiuntive sono necessarie per il gestore code IBM MQ .

z/OS *Inserimento di moduli globali IBM MQ nell'area LPA*

Quando un gestore code IBM MQ for z/OS viene avviato, carica alcuni dei moduli di caricamento (moduli globali) nell'ECSA (extended common service area). All'arresto del gestore code, ECSA viene liberato.

Importante: Per utilizzare questa funzione in IBM MQ 9.1 è necessario applicare l'APAR PH52358.

Esistono 19 moduli globali, che in IBM MQ 9.1, consumano circa 1.2 MB di ECSA per gestore code in esecuzione. In ambienti che eseguono più gestori code per LPAR e che richiedono una riduzione dell'utilizzo di ECSA a causa di ECSA o di vincoli privati elevati, è possibile posizionare i moduli globali nell'area LPA.

Nota: Sebbene CSQ7GPLM sia un modulo globale, non deve essere aggiunto all'area LPA.

Se il gestore code non è in grado di trovare un modulo globale nella STEPLIB e rileva che il modulo si trova nell'area LPA, utilizza direttamente la copia LPA invece di caricare una copia del modulo in ECSA. In alternativa, se il codice dei gestori code viene normalmente caricato dall'elenco di link, tutti i moduli globali nell'area LPA vengono caricati di preferenza rispetto a qualsiasi modulo globale nell'elenco di link.

La funzione di traccia della memoria comune z/OS (consultare Utilizzo della funzione di traccia della memoria comune) traccia la memoria sotto lo spazio di indirizzo MSTR di ciascun gestore code per ogni gestore code e può essere utilizzata per rilevare la quantità di spazio utilizzato dai moduli globali.

Per impostazione predefinita, i moduli globali sono nella libreria di caricamento SCSQAUTH. Se lo spazio di indirizzo MSTR di un gestore code individua SCSQAUTH tramite la concatenazione STEPLIB, i moduli globali da lì vengono utilizzati di preferenza rispetto a quelli nell'LPA e vengono caricati in ECSA.

I moduli globali sono:

CSQ0GPLM, CSQ3AMGP, CSQ3SSGP, CSQ9PREP,
CSQ9SCNB, CSQGGPLM, CSQMCGLM, CSQMGPLM, CSQRGLM1,
CSQSLD1, CSQVGEPL, CSQVSRX, CSQWDLD2, CSQWDLD3,
CSQWVZSA, CSQWZDG0, CSQWVZPS, CSQWVGTM, CSQZTDDM

Note:

- Il nome dei moduli globali per IBM MQ rimane costante tra le diverse versioni IBM MQ . Pertanto, se si caricano i moduli globali nell'area LPA, essi devono provenire da una singola versione di IBM MQ e devono essere utilizzati solo dai gestori code in esecuzione alla stessa versione di IBM MQ .
- Se più versioni di IBM MQ vengono eseguite sulla stessa LPAR, solo uno di essi può avere i propri moduli globali nell'area LPA in qualsiasi momento.

Se la manutenzione viene applicata a un'installazione di IBM MQ che ha moduli globali caricati nell'area LPA e tale manutenzione aggiorna uno qualsiasi dei moduli globali, è necessario eseguire nuovamente la procedura descritta nel seguente testo.

Procedura

Per inserire i moduli globali da una versione di IBM MQ in LPA, effettuare le seguenti operazioni:

1. Creare una copia della libreria di caricamento `thlqual.SCSQAUTH` e il relativo contenuto, ad esempio: `thlqual.LOCAL.SCSQAUTH`. Verificare che questa libreria di caricamento sia protetta dall'accesso non autorizzato mediante ESM (External Security Manager).
2. APF autorizza la libreria di caricamento `thlqual.LOCAL.SCSQAUTH` ; consultare “L'APF autorizza le librerie di caricamento IBM MQ” a pagina 828.
3. Creare una nuova libreria di caricamento `thlqual.GLOBAL.SCSQAUTH` con gli stessi attributi di `thlqual.LOCAL.SCSQAUTH`.

Nota: Non è necessario che questa libreria di caricamento sia autorizzata APF. Assicurarsi che questa libreria di caricamento sia protetta dall'accesso non autorizzato utilizzando l'ESM.

4. Copiare i 19 moduli globali da `thlqual.LOCAL.SCSQAUTH` in `thlqual.GLOBAL.SCSQAUTH`.
5. Eliminare i 19 moduli globali da `thlqual.LOCAL.SCSQAUTH`.
6. Inserire i 19 moduli globali da `thlqual.GLOBAL.SCSQAUTH` nell'area LPA, mediante:
   a. a. Aggiunta di `thlqual.GLOBAL.SCSQAUTH` in un membro LPALSTxx di SYS1.PARMLIB. È necessario quindi eseguire l'IPL del sistema con l'opzione CLPA per assicurarsi che il contenuto della libreria sia caricato in PLPA.
   b. b. Aggiunta dinamica dei moduli all'area LPA utilizzando il seguente comando:

```
SETPROG
LPA,ADD,MODNAME=(CSQ0GPLM,CSQ3AMGP,CSQ3SSGP,CSQ9PREP,CSQ9SCNB,CSQGGPLM,
CSQMCGLM,CSQMGPLM,CSQRGLM1,CSQSLD1,CSQVGEPL,CSQVSRX,CSQWDLD2,CSQWDLD3,
CSQWVZSA,CSQWZDG0,CSQWVZPS,CSQWVGTM,CSQZTDDM),DSNAME= thlqual.GLOBAL.SCSQAUTH
```

Nota: LPALSTxx è il mezzo a lungo termine preferito per inserire i moduli in LPA.

7. Convalidare che i moduli si trovino nell'area LPA immettendo il seguente comando:

```
D PROG,LPA,MODNAME=CSQMCGLM
```

L'output del comando deve indicare i punti di ingresso e di caricamento del modulo se è stato caricato correttamente nell'area LPA.

Per ogni gestore code che deve utilizzare i moduli globali dall'area LPA, se si posiziona normalmente:

1. `thlqual.SCSQAUTH` nell'elenco dei collegamenti, è sufficiente arrestare e avviare il proprio gestore code. I moduli globali vengono caricati dall'area LPA e i moduli locali dall'elenco di collegamenti.
2. `thlqual.SCSQAUTH` in MSTR JCL STEPLIB, modificare il JCL in modo che STEPLIB utilizzi `thlqual.LOCAL.SCSQAUTH` invece che `thlqual.SCSQAUTH`. Arrestare e avviare il gestore code; i moduli globali vengono caricati da LPA e i moduli locali da STEPLIB.

Il CHIN e il JCL AMSM possono continuare ad utilizzare `thlqual.SCSQAUTH` come qualsiasi applicazione IBM MQ .

Per ripristinare il gestore code al caricamento dei moduli globali in ECSA, effettuare le seguenti operazioni:

1. Arresta i gestori code
2. Rimuovere i moduli globali dall'LPA, al successivo IPL rimuovendo le definizioni LPALSTxx o utilizzando il seguente comando:

```
SETPROG LPA,DELETE,MODNAME=(xxx) FORCE=YES
```

3. Se `thlqual.LOCAL.SCSQAUTH` si trova in STEPLIB del gestore code, sostituirlo con `thlqual.SCSQAUTH`.
4. Riavviare i gestori code.

Concetti correlati

“Aggiornare l'elenco di link z/OS e LPA” a pagina 830
Aggiornare le librerie LPA con la nuova versione delle prime librerie di codice. L'altro codice può essere inserito nell'elenco dei link o nell'area LPA.

z/OS *Aggiornare la tabella delle proprietà del programma z/OS*

Alcune voci PPT aggiuntive sono necessarie per il gestore code IBM MQ .

- *È necessario eseguire questa attività una volta per ciascun sistema z/OS in cui si desidera eseguire IBM MQ.*
- *Se si utilizzano gruppi di condivisione code, è necessario assicurarsi che le impostazioni per IBM MQ siano identiche su ogni z/OS sistema nel sysplex.*

- *Non è necessario eseguire questa attività quando si esegue la migrazione da una versione precedente.*
- *È necessario eseguire la parte CSQ0DSRV di questa attività quando si richiede Advanced Message Security.*

Un esempio contenente tutte le voci PPT richieste viene fornito in thlqual.SCSQPROC(CSQ4SCHD). Assicurarsi che le voci richieste siano aggiunte al PPT, che è possibile trovare in SYS1.PARMLIB(SCHEDxx).

In z/OS 1.12 e versioni successive, CSQYASCP è già definito per il sistema operativo con gli attributi dettagliati e non deve più essere incluso in un membro SCHEDxx di PARMLIB.

Il gestore code IBM MQ controlla lo scambio. Tuttavia, se si dispone di una rete IBM MQ con un carico elevato e il tempo di risposta è critico, potrebbe essere utile rendere non sostituibile l'iniziatore del canale IBM MQ , aggiungendo la voce PPT CSQXJST, a rischio di influire sulle prestazioni del resto del sistema z/OS .

Se si richiede Advanced Message Security, aggiungere la voce PPT CSQ0DSRV .

Immettere il comando z/OS **SET SCH=xx**, dove *xx* è il suffisso del membro SCHEDxx di PARMLIB, per rendere effettive queste modifiche.

Concetti correlati

"Definire il sistema secondario IBM MQ in z/OS" a pagina 834
Aggiornare la tabella dei nomi del sottosistema e decidere una convenzione per le stringhe del prefisso del comando.

z/OS Configurazione del gestore code e dell'iniziatore di canali

Utilizzare questi argomenti come guida dettagliata per configurare il gestore code e l'iniziatore di canali.

z/OS *Definire il sistema secondario IBM MQ in z/OS*

Aggiornare la tabella dei nomi del sottosistema e decidere una convenzione per le stringhe del prefisso del comando.

Ripetere questa attività per ogni gestore code IBM MQ . Non è necessario eseguire questa attività durante la migrazione da una versione precedente.

Concetti correlati

"Creare le procedure per il gestore code IBM MQ" a pagina 838
Ogni sottosistema IBM MQ necessita di una procedura catalogata per avviare il gestore code. È possibile creare la propria libreria o utilizzare la libreria di procedure fornita da IBM.

z/OS *Aggiornamento della tabella dei nomi dei sottosistemi*

Quando si definisce il sottosistema IBM MQ , è necessario aggiungere una voce alla tabella dei nomi dei sottosistemi.

La tabella dei nomi dei sottosistemi di z/OS, ricavata inizialmente da SYS1.PARMLIB membro IEFSSNss, contiene le definizioni dei sottosistemi z/OS definiti formalmente. Per definire ogni sottosistema IBM MQ , è necessario aggiungere una voce a questa tabella, modificando il membro IEFSSNss di SYS1.PARMLIBo, preferibilmente, utilizzando il comando z/OS SETSSI.

L'inizializzazione del sottosistema IBM MQ supporta l'elaborazione parallela, quindi le istruzioni di definizione del sottosistema IBM MQ possono essere aggiunte sopra e sotto la parola chiave BEGINPARALLEL nella tabella IEFSSNss disponibile in z/OS V1.12 e versioni successive.

Se si utilizza il comando SETSSI, la modifica diventa immediatamente effettiva e non è necessario eseguire un IPL del proprio sistema. Assicurarsi di aggiornare SYS1.PARMLIB , come descritto in "Aggiornare SYS1.PARMLIB" a pagina 842 in modo che le modifiche rimangano effettive dopo gli IPL successivi.

Il comando SETSSI per definire dinamicamente un sottosistema IBM MQ è:

```
SETSSI ADD,S=ssid,I=CSQ3INI,P='CSQ3EPX,cpf,scope'
```

Le informazioni corrispondenti in IEFSSNss possono essere specificate in due modi:

- Il formato del parametro della parola chiave della definizione di sottosistema IBM MQ in IEFSSNss. Questo rappresenta il metodo di migrazione consigliato.

```
SUBSYS SUBNAME(ssid) INITRTN(CSQ3INI) INITPARM('CSQ3EPX,cpf,scope')
```

- Il formato del parametro posizionale della definizione del sottosistema IBM MQ .

```
ssid,CSQ3INI,'CSQ3EPX,cpf,scope'
```

Non combinare le due forme in un membro IEFSSNss. Se sono richiesti moduli differenti, utilizzare un membro IEFSSNss separato per ogni tipo, aggiungendo l'operando SSN del nuovo membro a IEASYSpp SYS1.PARMLIB . Per specificare più di un SSN, utilizzare SSN = (aa, bb, ...) in IEASYSpp.

Negli esempi,

ssid
L'identificativo del sottosistema. Può avere una lunghezza massima di quattro caratteri. Tutti i caratteri devono essere alfanumerici (da A a Z in maiuscolo, da 0 a 9) e devono iniziare con un carattere alfabetico. Il gestore code avrà lo stesso nome del sottosistema, quindi è possibile utilizzare solo i caratteri consentiti sia per i nomi dei sottosistemi z/OS che per quelli degli oggetti IBM MQ .

cpf
La stringa del prefisso del comando (consultare “Definizione delle stringhe di prefisso del comando (CPFs)” a pagina 836 per informazioni sui CPF).

scope
L'ambito del sistema, utilizzato se si è in esecuzione in un sysplex z/OS (consultare “CPF in un ambiente sysplex” a pagina 837 per informazioni sull'ambito del sistema).

Figura 99 a pagina 835 mostra diversi esempi di istruzioni IEFSSNss.

```
CSQ1,CSQ3INI,'CSQ3EPX,+mqs1cpf,S'
CSQ2,CSQ3INI,'CSQ3EPX,+mqs2cpf,S'
CSQ3,CSQ3INI,'CSQ3EPX,++,S'
```

Figura 99. Istruzioni IEFSSNss di esempio per la definizione di sottosistemi

Nota: Una volta creati gli oggetti in un sottosistema, non è possibile modificare il nome del sottosistema o utilizzare le serie di pagine da un sottosistema in un altro sottosistema. Per eseguire una di queste operazioni, è necessario scaricare tutti gli oggetti e i messaggi da un sottosistema e ricaricarli in un altro.

Tabella 54 a pagina 835 fornisce un certo numero di esempi che mostrano le associazioni di nomi di sottosistemi e di stringhe di prefisso di comando (CPF), come definito dalle istruzioni in Figura 99 a pagina 835.

Tabella 54. Associazioni nome sottosistema a CPF

IBM MQ Nome sottosistema	**CPF**
CSQ1	+mqs1cpf

Tabella 54. Associazioni nome sottosistema a CPF (Continua)	
IBM MQ Nome sottosistema	**CPF**
CSQ2	+mqs2cpf
CSQ3	++

Nota: Le funzioni ACTIVATE e DEACTIVATE del comando z/OS SETSSI non sono supportate da IBM MQ.

Per controllare lo stato delle modifiche, immettere il seguente comando in SDSF: `/D SSI,L`. Verranno visualizzati i nuovi sottosistemi creati con stato ATTIVO.

z/OS *Definizione delle stringhe di prefisso del comando (CPFs)*

Ogni istanza di sottosistema di IBM MQ può avere una stringa di prefisso di comando per identificare tale sottosistema.

Adottare una convenzione a livello di sistema per i CPF per tutti i sottosistemi per evitare conflitti. Attenersi alle seguenti linee guida:

- Definire un CPF come stringa con un massimo di otto caratteri.
- Non utilizzare un CPF già utilizzato da altri sottosistemi ed evitare di utilizzare il carattere di backspace JES definito sul sistema come primo carattere della stringa.
- Definire il CPF utilizzando i caratteri della serie di caratteri validi elencati in Tabella 56 a pagina 837.
- Non utilizzare un CPF che è un'abbreviazione per un processo già definito o che potrebbe essere confuso con la sintassi del comando. Ad esempio, un CPF come 'D' è in conflitto con i comandi z/OS come DISPLAY. Per evitare che ciò accada, utilizzare uno dei caratteri speciali (mostrati in Tabella 56 a pagina 837) come primo o unico carattere nella stringa CPF.
- Non definire un CPF che sia un sottoinsieme o un superinsieme di un CPF esistente. Per un esempio, consultare Tabella 55 a pagina 836.

Tabella 55. Esempio di sottoinsieme CPF e regole superset		
Nome sottosistema	**CPF definito**	**Comandi instradati a**
MQA	!A	MQA
MQB	!B	MQB
MQC1	!C1	MQC1
MQC2	!C2	MQC2
MQB1	!B1	MQB

Comandi previsti per il sottosistema MQB1 (utilizzando CPF!B1) vengono instradati al sottosistema MQB perché il CPF per questo sottosistema è!B, un sottoinsieme di!B1. Ad esempio, se è stato immesso il comando:

```
!B1  START  QMGR
```

MQB del sottosistema riceve il comando:

```
1 START QMGR
```

(che, in questo caso, non può trattare).

È possibile vedere quali prefissi esistono immettendo il comando z/OS DISPLAY OPDATA.

Se si è in esecuzione in un sysplex, z/OS esegue la diagnosi di eventuali conflitti di questo tipo al momento della registrazione CPF (consultare “CPF in un ambiente sysplex” a pagina 837 per informazioni sulla registrazione CPF).

Tabella 56 a pagina 837 mostra i caratteri che è possibile utilizzare quando si definiscono le stringhe CPF:

Tabella 56. Serie di caratteri valida per stringhe CPF

Serie di caratteri	**Contenuto**
Alfabetico	Maiuscolo da A a Z, minuscolo da a a z
Numerico	Da 0 a 9
Nazionale (vedi nota)	@ $# (Caratteri che possono essere rappresentati come valori esadecimali)
Speciale	. □ ( ) * & + - = ¢ < | ! ; % _ ? : >

Nota:

Il sistema riconosce le seguenti rappresentazioni esadecimali dei caratteri nazionali: @ come X'7C', $come X'5B' e # come X'7B'. In paesi diversi da U.S., i caratteri nazionali U.S. rappresentati sulle tastiere del terminale potrebbero generare una rappresentazione esadecimale differente e causare un errore. Ad esempio, in alcuni paesi il carattere $potrebbe generare una X'4A'.

Il punto e virgola (;) è valido come CPF ma sulla maggior parte dei sistemi, questo carattere è il delimitatore del comando.

z/OS *CPF in un ambiente sysplex*

Utilizzare questo argomento per comprendere come utilizzare i CPF nell'ambito di un sysplex.

Se utilizzato in un ambiente sysplex, IBM MQ registra i CPF per consentire l'immissione di un comando da qualsiasi console nel sysplex e l'instradamento di tale comando al sistema appropriato per l'esecuzione. Le risposte del comando vengono restituite alla console di origine.

Definizione dell'ambito per l'operazione sysplex

L'ambito viene utilizzato per stabilire il tipo di registrazione CPF eseguita dal sottosistema IBM MQ quando si esegue IBM MQ in un ambiente sysplex.

I valori possibili per l'ambito sono i seguenti:

M

Ambito del sistema.

Il CPF viene registrato con z/OS al momento dell'IPL del sistema da IBM MQ e rimane registrato per tutto il tempo in cui il sistema z/OS è attivo.

I comandi IBM MQ devono essere immessi in una console collegata all'immagine z/OS che esegue il sottosistema di destinazione oppure è necessario utilizzare i comandi ROUTE per indirizzare il comando a tale immagine.

Utilizzare questa opzione se non si è in esecuzione in un sysplex.

S

Sysplex ha avviato l'ambito.

Il CPF viene registrato con z/OS quando il sottosistema IBM MQ viene avviato e rimane attivo finché il sottosistema IBM MQ non termina.

È necessario utilizzare i comandi ROUTE per indirizzare il comando START QMGR originale al sistema di destinazione, ma tutti gli altri comandi IBM MQ possono essere immessi su qualsiasi console connessa al sysplex e vengono instradati automaticamente al sistema di destinazione.

Dopo la terminazione di IBM MQ , è necessario utilizzare i comandi ROUTE per indirizzare i comandi START successivi al sottosistema IBM MQ di destinazione.

X

Ambito IPL sysplex.

Il CPF viene registrato con z/OS al momento dell'IPL del sistema da IBM MQ e rimane registrato per tutto il tempo in cui il sistema z/OS è attivo.

I comandi IBM MQ possono essere immessi da qualsiasi console connessa al sysplex e vengono instradati all'immagine che esegue automaticamente il sistema di destinazione.

Un sottosistema IBM MQ con un CPF con ambito S può essere definito su una o più immagini z/OS all'interno di un sysplex, in modo che queste immagini possano condividere una singola tabella di nomi del sottosistema. Tuttavia, è necessario assicurarsi che il comando START iniziale venga immesso (o instradato) sull'immagine z/OS su cui si desidera eseguire il sottosistema IBM MQ . Se si utilizza questa opzione, è possibile arrestare il sottosistema IBM MQ e riavviarlo su un'immagine z/OS differente all'interno del sysplex senza dover modificare la tabella dei nomi dei sottosistemi o eseguire un IPL di un sistema z/OS .

Un sottosistema IBM MQ con CPF con ambito X può essere definito solo su un'immagine z/OS all'interno di un sysplex. Se si utilizza questa opzione, è necessario definire una tabella di nomi di sottosistema univoca per ogni z/OS immagine che richiede IBM MQ sottosistemi con CPF di ambito X.

Se si desidera utilizzare z/OS ARM (automatic restart manager) per riavviare automaticamente i gestori code in immagini z/OS differenti, ogni gestore code deve essere definito in ciascuna immagine z/OS su cui tale gestore code potrebbe essere riavviato. Ogni gestore code deve essere definito con un nome di sottosistema univoco a 4 caratteri a livello di sistema con un ambito CPF di S.

z/OS *Creare le procedure per il gestore code IBM MQ*

Ogni sottosistema IBM MQ necessita di una procedura catalogata per avviare il gestore code. È possibile creare la propria libreria o utilizzare la libreria di procedure fornita da IBM.

- Ripetere questa attività per ogni gestore code IBM MQ .
- Potrebbe essere necessario modificare la procedura catalogata durante la migrazione da una versione precedente.

Per ogni sottosistema IBM MQ definito nella tabella dei nome sottosistema, creare una procedura catalogata in una libreria di procedura per l'avvio del gestore code. La libreria della procedura fornita da IBMè denominata SYS1.PROCLIB, ma l'installazione potrebbe utilizzare la propria convenzione di denominazione.

Il nome della procedura dell'attività avviata del gestore code è formato concatenando il nome del sottosistema con i caratteri MSTR. Ad esempio, il sottosistema CSQ1 ha il nome procedura CSQ1MSTR. È necessaria una procedura per ogni sottosistema definito.

È necessario includere la libreria contenente i messaggi nella lingua selezionata:

- thlqual.SCSQSNLE, per l'inglese americano con lettere maiuscole e minuscole
- thlqual.SCSQSNLU, per l'inglese americano maiuscolo
- thlqual.SCSQSNLK, per il giapponese
- thlqual.SCSQSNLF, per il francese
- thlqual.SCSQSNLC, per il cinese

Molti esempi e istruzioni in questa documentazione del prodotto presuppongono che si disponga di un sottosistema denominato CSQ1. Questi esempi potrebbero essere più semplici da utilizzare se un sottosistema denominato CSQ1 viene creato inizialmente per scopi di test e verifica dell'installazione.

Due procedure di attività avviate di esempio sono fornite in thlqual.SCSQPROC. Il membro CSQ4MSTR utilizza una serie di pagine per ciascuna classe di messaggi, il membro CSQ4MSRR utilizza più serie di pagine per le principali classi di messaggi. Copiare una di queste procedure nel membro xxxxMSTR (dove xxxx è il nome del sottosistema IBM MQ) del SYS1.PROCLIB o, se non si utilizza SYS1.PROCLIB, la libreria delle procedure. Copiare la procedura di esempio in un membro nella libreria delle procedure per ogni sottosistema IBM MQ definito.

Una volta copiati i membri, è possibile adattarli ai requisiti di ciascun sottosistema, utilizzando le istruzioni nel membro. Per informazioni su come specificare i limiti di memoria utilizzati dal gestore code, consultare Dimensioni regione consigliate. È anche possibile utilizzare parametri simbolici in JCL per consentire la modifica della procedura quando viene avviata. Se si dispone di diversi sottosistemi IBM MQ , potrebbe risultare vantaggioso utilizzare i gruppi di inclusione JCL per le parti comuni della procedura, per semplificare la manutenzione futura.

Se si utilizzano gruppi di condivisione code, la concatenazione STEPLIB deve includere la libreria di destinazione di runtime Db2 SDSNLOAD e deve essere autorizzata da APF. Questa libreria è richiesta solo nella concatenazione STEPLIB se non è accessibile tramite l'elenco di collegamenti o LPA.

Se si utilizza Advanced Message Security , la concatenazione STEPLIB deve includere *thlqual*.SDRQAUTH e deve essere autorizzata da APF.

Nota: È possibile prendere nota dei nomi del dataset bootstrap (BSDS), dei log e delle serie di pagine da utilizzare in JCL e quindi definire tali serie in una fase successiva del processo.

Concetti correlati

“Crea procedure per l'iniziatore di canali” a pagina 839
Per ogni sottosistema IBM MQ , personalizzare una copia di CSQ4CHIN. A seconda degli altri prodotti che si stanno utilizzando, potrebbe essere necessario consentire l'accesso ad altri dataset.

z/OS *Crea procedure per l'iniziatore di canali*

Per ogni sottosistema IBM MQ , personalizzare una copia di CSQ4CHIN. A seconda degli altri prodotti che si stanno utilizzando, potrebbe essere necessario consentire l'accesso ad altri dataset.

- Ripetere questa attività per ogni gestore code IBM MQ .
- Potrebbe essere necessario modificare la procedura catalogata durante la migrazione da una versione precedente.

È necessario creare una procedura di attività avviata dall'iniziatore di canale per ogni sottosistema IBM MQ che utilizzerà l'accodamento distribuito.

Per far ciò:

1. Copiare la procedura dell'attività avviata di esempio thlqual.SCSQPROC(CSQ4CHIN) nella libreria delle procedure. Denominare la procedura *xxxx* CHIN, dove *xxxx* è il nome del sottosistema IBM MQ (ad esempio, CSQ1CHIN è la procedura dell'attività avviata dall'iniziatore del canale per il gestore code CSQ1).
2. Creare una copia per ogni sottosistema IBM MQ che si sta per utilizzare.
3. Adattare le procedure ai propri requisiti utilizzando le istruzioni contenute nella procedura di esempio CSQ4CHIN. È anche possibile utilizzare parametri simbolici in JCL per consentire la modifica della procedura quando viene avviata. Questa operazione è descritta con le opzioni di avvio in Amministrazione IBM MQ for z/OS.

   Concatenare la libreria di accodamento distribuita thlqual.SCSQMVR1.

   È richiesto l'accesso alla libreria di runtime LE SCEERUN; se non è presente nell'elenco dei collegamenti (SYS1.PARMLIB(LNKLSTkk), concatenarlo nell'istruzione STEPLIB DD.
4. Autorizzare le procedure da eseguire con il gestore della sicurezza esterno.

5. È necessario includere la libreria contenente i messaggi nella lingua selezionata:
   - thlqual.SCSQSNLE, per l'inglese americano con lettere maiuscole e minuscole
   - thlqual.SCSQSNLU, per l'inglese americano maiuscolo
   - thlqual.SCSQSNLK, per il giapponese
   - thlqual.SCSQSNLF, per il francese
   - thlqual.SCSQSNLC, per il cinese

L'iniziatore del canale è uno spazio di indirizzo di lunga durata. Per impedirne la terminazione dopo che è stata consumata una quantità limitata di CPU, confermare che:

- Il valore predefinito per le attività avviate nel sistema z/OS è CPU illimitata; un'istruzione di configurazione JES2 per JOBCLASS (STC) con TIME = (1440,00) ottiene questo risultato oppure
- Aggiungere esplicitamente un parametro TIME=1440, o TIME=NOLIMIT, all'istruzione EXEC per CSQXJST.

È possibile aggiungere la libreria di uscita (CSQXLIB) a questa procedura in un secondo momento se si desidera utilizzare le uscite del canale. È necessario arrestare e riavviare l'iniziatore di canali per eseguire questa operazione.

Se si utilizza TLS, è richiesto l'accesso alla libreria di runtime TLS del sistema. Questa libreria è denominata SIEALNKE. La libreria deve essere autorizzata APF.

Se si utilizza TCP/IP, lo spazio di indirizzo dell'iniziatore di canali deve essere in grado di accedere a TCPIP.DATA che contiene i parametri di sistema TCP/IP. I modi in cui deve essere impostato il data set dipendono dal prodotto TCP/IP e dall'interfaccia utilizzati. Includono:

- Variabile di ambiente, RESOLVER_CONFIG
- /etc/resolv.conf sul file system
- // istruzione SYSTCPD DD
- // istruzione SYSTCPDD DD
- *jobname/userid*.TCPIP.DATA
- SYS1.TCPPARMS(TCPDATA)
- *zapname*.TCPIP.DATA

Alcune di queste influiscono sul JCL della procedura dell'attività avviata. Per ulteriori informazioni, consultare z/OS Communications Server: IP Configuration Guide.

Concetti correlati

“Definire il sottosistema IBM MQ in una classe di servizi z/OS WLM” a pagina 840
Per dare a IBM MQ la priorità delle prestazioni appropriata nel sistema z/OS , è necessario assegnare gli spazi di indirizzo del gestore code e dell'iniziatore di canali a una classe di servizio WLM (workload management) z/OS appropriata. Se non si esegue questa operazione in modo esplicito, potrebbero essere applicati valori predefiniti inappropriati.

z/OS *Definire il sottosistema IBM MQ in una classe di servizi z/OS WLM*

Per dare a IBM MQ la priorità delle prestazioni appropriata nel sistema z/OS , è necessario assegnare gli spazi di indirizzo del gestore code e dell'iniziatore di canali a una classe di servizio WLM (workload management) z/OS appropriata. Se non si esegue questa operazione in modo esplicito, potrebbero essere applicati valori predefiniti inappropriati.

- *Ripetere questa attività per ogni gestore code IBM MQ*
- *Non è necessario eseguire questa attività quando si esegue la migrazione da una versione precedente.*

Utilizzare la finestra di dialogo ISPF fornita con WLM per eseguire le attività riportate di seguito:

- Estrarre la definizione della politica z/OS WLM dal dataset di coppia WLM.

- Aggiornare questa definizione della politica aggiungendo i nomi di procedura dell'attività avviata del gestore code e dell'iniziatore di canale alla classe di servizio scelta
- Installa la politica modificata sul dataset di coppia WLM

Quindi attivare questa politica utilizzando il comando z/OS

```
V WLM,POLICY=policyname,REFRESH
```

Consultare Pianificazione dell'ambiente IBM MQ su z/OS per ulteriori informazioni sull'impostazione delle opzioni delle prestazioni.

Concetti correlati

“Impostazione dell'ambiente Db2” a pagina 877
Se si utilizzano gruppi di condivisione code, è necessario creare gli oggetti Db2 richiesti personalizzando ed eseguendo un numero di lavori di esempio.

z/OS *Implementare i controlli di sicurezza ESM*

Implementare i controlli di sicurezza per gestori code e iniziatore di canali.

- *Ripetere questa attività per ogni gestore code IBM MQ*
- *Potrebbe essere necessario eseguire questa attività durante la migrazione da una versione precedente.*

Se si utilizza RACF come gestore della sicurezza esterno, consultare Impostazione della sicurezza su z/OS , che descrive come implementare questi controlli di sicurezza.

Se si utilizza l'iniziatore di canali, è necessario effettuare le seguenti operazioni:

- Se il sottosistema ha la sicurezza di connessione attiva, definire un profilo di sicurezza di connessione ssid.CHIN per il gestore di sicurezza esterno (consultare Profili di sicurezza di connessione per l'iniziatore di canali per informazioni su questo).
- Se si utilizza TLS (Transport Layer Security) o un'interfaccia socket, verificare che l'ID utente con cui è in esecuzione l'iniziatore di canali sia configurato per utilizzare UNIX System Services, come descritto nella documentazione di *OS/390 UNIX System Services Planning* .
- Se si sta utilizzando TLS, assicurarsi che l'ID utente sotto la cui autorizzazione è in esecuzione l'iniziatore del canale sia configurato per accedere al keyring specificato nel parametro SSLKEYR del comando ALTER QMGR.

Prima di avviare il gestore code, impostare la sicurezza del sistema e del dataset IBM MQ mediante:

- Autorizzazione della procedura dell'attività avviata del gestore code da eseguire nel gestore di sicurezza esterno.
- Autorizzazione dell'accesso ai dataset del gestore code.
- V 9.1.4 Configurazione della codifica del dataset z/OS , se richiesto.

  Consultare la sezione, Riservatezza per i dati inattivi su IBM MQ for z/OS con la crittografia del dataset. per ulteriori informazioni.

Per dettagli su come eseguire questa operazione, consultare Attività di installazione della sicurezza per z/OS.

Se si utilizza RACF, se si utilizza la classe RACF STARTED, non è necessario eseguire un IPL del sistema (consultare RACF autorizzazione delle procedure delle attività avviate).

Concetti correlati

“Aggiornare SYS1.PARMLIB” a pagina 842
Per assicurarsi che le proprie modifiche rimangano attive dopo un IPL, è necessario aggiornare alcuni membri di SYS1.PARMLIB

“Implementare i controlli di sicurezza ESM per il gruppo di condivisione code” a pagina 881
Implementare i controlli di sicurezza per tutti i gestori code in un gruppo di condivisione code, per accedere a Db2 e alle strutture dell'elenco CF (Coupling Facility).

z/OS *Aggiornare SYS1.PARMLIB*

Per assicurarsi che le proprie modifiche rimangano attive dopo un IPL, è necessario aggiornare alcuni membri di SYS1.PARMLIB

- *È necessario eseguire questa attività una volta per ogni sistema z/OS in cui si desidera eseguire IBM MQ.*
- *Se si utilizzano gruppi di condivisione code, è necessario assicurarsi che le impostazioni per IBM MQ siano identiche su ogni z/OS sistema nel sysplex.*
- *Potrebbe essere necessario eseguire questa attività durante la migrazione da una versione precedente.*

Aggiornare SYS1.PARMLIB come segue:

1. Aggiornare il membro IEFSSNss come descritto in "Definire il sistema secondario IBM MQ in z/OS" a pagina 834.
2. Modificare IEASYSpp in modo che i seguenti membri vengano utilizzati quando si esegue un IPL:
   - i membri PROGxx o IEAAPFaa utilizzati in "L'APF autorizza le librerie di caricamento IBM MQ" a pagina 828
   - i membri LNKLSTkk e LPALSTmm utilizzati in "Aggiornare l'elenco di link z/OS e LPA" a pagina 830
   - il membro SCHEDxx utilizzato in "Aggiornare la tabella delle proprietà del programma z/OS" a pagina 833
   - il membro IEFSSNss utilizzato in "Definire il sistema secondario IBM MQ in z/OS" a pagina 834

Concetti correlati

"Personalizzazione dei dataset di input di inizializzazione" a pagina 842
Creare copie di lavoro dei dataset di input di inizializzazione di esempio e personalizzarle in base ai requisiti di sistema.

z/OS *Personalizzazione dei dataset di input di inizializzazione*

Creare copie di lavoro dei dataset di input di inizializzazione di esempio e personalizzarle in base ai requisiti di sistema.

- *Ripetere questa attività per ogni gestore code IBM MQ*
- *È necessario eseguire questa attività quando si esegue la migrazione da una versione precedente.*

Ogni gestore code IBM MQ ottiene la definizione iniziale da una serie di comandi contenuti nei IBM MQ *dataset di input di inizializzazione*. A questi dataset fanno riferimento i nomi DD CSQINP1, CSQINP2 e CSQINPT definiti nella procedura dell'attività avviata del gestore code.

Le risposte a questi comandi vengono scritte nei dataset di output di inizializzazione a cui fanno riferimento i nomi DD CSQOUT1, CSQOUT2 e CSQOUTT.

Per preservare gli originali, creare copie di lavoro di ciascun campione. Quindi, è possibile personalizzare i comandi in queste copie di lavoro per soddisfare i requisiti di sistema.

Se si utilizza più di un sottosistema IBM MQ , se si include il nome del sottosistema nel qualificatore di alto livello del nome del dataset di input di inizializzazione, è possibile identificare più facilmente il sottosistema IBM MQ associato a ciascun dataset.

Fare riferimento ai seguenti argomenti per ulteriori informazioni sugli esempi:

- Formati dataset di inizializzazione
- Utilizzo dell'esempio CSQINP1
- Utilizzo degli esempi CSQINP2
- Utilizzo dell'esempio CSQINPX
- Utilizzo dell'esempio CSQINPT

Formati dataset di inizializzazione

I dataset di input di inizializzazione possono essere membri PDS (partitioned data set) o dataset sequenziali. Possono essere una serie concatenata di dataset. Definirli con una lunghezza record di 80 byte, dove:

- Solo le colonne da 1 a 72 sono significative. Le colonne da 73 a 80 vengono ignorate.
- I record con un asterisco (*) nella colonna 1 vengono interpretati come commenti e ignorati.
- I record vuoti vengono ignorati.
- Ogni comando deve iniziare su un nuovo record.
- Un termine finale significa continuare dalla colonna 1 del record successivo.
- Un + finale significa continuare dalla prima colonna non vuota del record successivo.
- Il numero massimo di caratteri consentiti in un comando è 32 762.

I dataset di output di inizializzazione sono dataset sequenziali, con una lunghezza record di 125, un formato record VBA e una dimensione blocco di 629.

Utilizzo dell'esempio CSQINP1

Il data set thlqual.SCSQPROC contiene due membri che contengono le definizioni dei pool di buffer, la serie di pagine per le associazioni del pool di buffer e un comando ALTER SECURITY.

Il membro CSQ4INP1 utilizza una serie di pagine per ogni classe di messaggio. Il membro CSQ4INPR utilizza più serie di pagine per le classi principali di messaggi.

Includere l'esempio appropriato nella concatenazione CSQINP1 della procedura dell'attività avviata del gestore code.

Note:

1. IBM MQ supporta fino a 100 pool di buffer nell'intervallo compreso tra zero e 99. Il comando DEFINE BUFFPOOL può essere immesso solo da un dataset di inizializzazione CSQINP1 . Le definizioni nell'esempio specificano quattro pool di buffer.
2. Ogni serie di pagine utilizzata dal gestore code deve essere definita nel dataset di inizializzazione CSQINP1 utilizzando il comando DEFINE PSID. La definizione della serie di pagine associa un ID pool di buffer ad una serie di pagine. Se non viene specificato alcun pool di buffer, per impostazione predefinita viene utilizzato il pool di buffer zero.

   È necessario definire la serie di pagine zero (00). Contiene tutte le definizioni di oggetto. È possibile definire fino a 100 serie di pagine per ciascun gestore code.
3. Il comando ALTER SECURITY può essere utilizzato per modificare gli attributi di sicurezza TIMEOUT e INTERVAL. In CSQ4INP1, i valori predefiniti sono definiti come 54 per TIMEOUT e 12 per INTERVAL.

Consultare Pianificazione su z/OS per informazioni sull'organizzazione dei pool di buffer e delle serie di pagine.

Se si modificano dinamicamente le definizioni di pool di buffer e serie di pagine mentre il gestore code è in esecuzione, è necessario aggiornare anche le definizioni CSQINP1 . Le modifiche vengono conservate solo per un avvio a freddo di IBM MQ, a meno che la definizione del pool di buffer non includa l'attributo REPLACE.

Utilizzo degli esempi CSQINP2

Questa tabella elenca i membri di thlqual.SCSQPROC che è possibile includere nella concatenazione CSQINP2 della procedura dell'attività avviata del gestore code, con una descrizione della relativa funzione. La convenzione di denominazione è CSQ4INS*. CSQ4INY* dovrà essere modificato per la tua configurazione. Si consiglia di evitare di modificare i membri CSQINS* poiché sarà necessario riapplicare le modifiche quando si migra alla release successiva. Invece, è possibile inserire comandi DEFINE o ALTER nei membri CSQ4INY* .

Tabella 57. Membri di thlqual.SCSQPROC	
Nome membro	**Descrizione**
CSQ4INSG	Definizioni oggetto di sistema.
CSQ4INSA	Oggetto di sistema e regole predefinite per l'autenticazione di canale.
CSQ4INSX	Definizioni oggetto di sistema.
CSQ4INSS	Personalizzare e includere questo membro se si utilizzano gruppi di condivisione code.
CSQ4INSJ	Personalizzare e includere questo membro se si utilizza la pubblicazione / sottoscrizione utilizzando JMS.
CSQ4INSM	Definizioni di oggetti di sistema per Advanced Message Security.
CSQ4INSR	Personalizzare e includere questo membro se si utilizza WebSphere Application Servero l'interfaccia di pubblicazione / sottoscrizione in coda supportata dal daemon di pubblicazione / sottoscrizione in coda in IBM MQ V7 o versioni successive.
CSQ4DISP	Esempio CSQINP2 per visualizzare le definizioni di oggetto.
CSQ4INYC	Definizioni di cluster.
CSQ4INYD	Definizioni di accodamento distribuito.
CSQ4INYG	Definizioni generali.
CSQ4INYR	Definizioni di classi di memoria, utilizzando più serie di pagine per le classi principali di messaggi.
CSQ4INYS	Definizioni della classe di archiviazione, utilizzando una serie di pagine per ciascuna classe di messaggi.

È necessario definire gli oggetti una sola volta, non ogni volta che si avvia un gestore code, quindi non è necessario includere queste definizioni in CSQINP2 ogni volta. Se li si include ogni volta, si sta tentando di definire oggetti già esistenti e si riceveranno messaggi simili ai seguenti:

```
CSQM095I +CSQ1 CSQMAQLC QLOCAL(SYSTEM.DEFAULT.LOCAL.QUEUE) ALREADY EXISTS
CSQM090E +CSQ1 CSQMAQLC FAILURE REASON CODE X'00D44003'
CSQ9023E +CSQ1 CSQMAQLC ' DEFINE QLOCAL' ABNORMAL COMPLETION
```

Gli oggetti non sono danneggiati da questo errore. Se si desidera lasciare il dataset delle definizioni di SISTEMA nella concatenazione CSQINP2 , è possibile evitare i messaggi di errore specificando l'attributo REPLACE per ciascun oggetto.

Utilizzo dell'esempio CSQINPX

L'esempio thlqual.SCSQPROC(CSQ4INPX) contiene una serie di comandi che è possibile eseguire ogni volta che viene avviato l'iniziatore di canali. Si tratta generalmente di comandi correlati al canale, come START LISTENER, che sono richiesti ogni volta che viene avviato l'iniziatore del canale, piuttosto che ogni volta che viene avviato il gestore code, e che non sono consentiti nei dataset di input CSQINP1 o CSQINP2. È necessario personalizzare questo esempio prima dell'utilizzo; è quindi possibile includerlo nel dataset CSQINPX per l'iniziatore di canali.

I comandi IBM MQ contenuti nel dataset vengono eseguiti alla fine dell'inizializzazione dell'iniziatore di canali e l'output viene scritto nel dataset specificato dall'istruzione CSQOUTX DD. L'output è simile a quello prodotto dalla funzione COMMAND del programma di utilità IBM MQ (CSQUTIUTIL). Consultare Il programma di utilità CSQUTIL per ulteriori dettagli.

È possibile specificare qualsiasi comando IBM MQ che può essere immesso da CSQUTIL, non solo i comandi del canale. È possibile immettere comandi da altre origini durante l'elaborazione di CSQINPX. Tutti i comandi vengono emessi in sequenza, indipendentemente dalla riuscita del precedente comando.

Per specificare un tempo di risposta del comando, è possibile utilizzare lo pseudo comando COMANDO come primo comando nel dataset. Questa operazione richiede una singola parola chiave facoltativa RESPTIME (*nnn*), dove *nnn* è il tempo di attesa, in secondi, per una risposta a ciascun comando. È compreso tra 5 e 999; il valore predefinito è 30.

Se IBM MQ rileva che le risposte a quattro comandi hanno impiegato troppo tempo, l'elaborazione di CSQINPX viene arrestata e non vengono emessi ulteriori comandi. L'iniziatore del canale non viene arrestato, ma il messaggio CSQU052E viene scritto nel dataset CSQOUTX e il messaggio CSQU013E viene inviato alla console.

Quando IBM MQ ha completato correttamente l'elaborazione di CSQINPX, il messaggio CSQU012I viene inviato alla console.

Utilizzo dell'esempio CSQINPT

Questa tabella elenca i membri di thlqual.SCSQPROC che è possibile includere nella concatenazione CSQINPT della procedura di attività avviata del gestore code, con una descrizione della relativa funzione.

Tabella 58. Membri di thlqual.SCSQPROC

Nome membro	Descrizione
CSQ4INST	Definizione sottoscrizione predefinita del sistema.
CSQ4INYT	Definizioni di pubblicazione / sottoscrizione.

I comandi IBM MQ contenuti nel data set vengono eseguiti al termine dell'inizializzazione della pubblicazione / sottoscrizione e l'output viene scritto nel data set specificato dall'istruzione CSQOUTT DD. L'output è simile a quello prodotto dalla funzione COMMAND del programma di utilità IBM MQ (CSQUTIUTIL). Consultare Il programma di utilità CSQUTIL per ulteriori dettagli.

Concetti correlati

“Creare i dataset bootstrap e log” a pagina 845
Utilizzare il programma fornito CSQJU003 per preparare i dataset bootstrap (BSDS) e i dataset di log.

z/OS *Creare i dataset bootstrap e log*

Utilizzare il programma fornito CSQJU003 per preparare i dataset bootstrap (BSDS) e i dataset di log.

- *Ripetere questa attività per ogni gestore code IBM MQ*
- V 9.1.4 *Se si utilizza la codifica del dataset z/OS per proteggere il BSDS o i dataset del log attivo, è necessario configurare questa opzione prima che i dataset vengano assegnati in questo passo.*
- *Non è necessario eseguire questa attività quando si esegue la migrazione da una versione precedente.*

  V 9.1.4 *Se si sta migrando un gestore code e si sta aggiungendo la codifica del dataset z/OS per i dataset di log attivi o BSDS, è necessario convertire i dataset.*

  V 9.1.4 *Consultare la sezione,* Riservatezza per i dati inattivi su IBM MQ for z/OS con la crittografia del dataset. *Per ulteriori informazioni sulla configurazione della codifica del dataset z/OS e sulla conversione dei dataset IBM MQ esistenti da codificare.*

Le istruzioni di controllo JCL e AMS (Access Method Services) di esempio per eseguire CSQJU003 per creare un ambiente di registrazione singolo o doppio si trovano in thlqual.SCSQPROC(CSQ4BSDS). Personalizza ed esegue questo lavoro per creare BSDS e log e per preformattare i log.

Importante: Si consiglia di utilizzare la versione più recente di CSQ4BSDSo aggiornare manualmente il JCL per utilizzare RECORDS (850 60).

La procedura dell'attività avviata, CSQ4MSTR, descritta in “Creare le procedure per il gestore code IBM MQ” a pagina 838, fa riferimento a BSDS in istruzioni del formato:

```
//BSDS1   DD DSN=++HLQ++.BSDS01,DISP=SHR
//BSDS2   DD DSN=++HLQ++.BSDS02,DISP=SHR
```

I BSDS fanno riferimento ai dataset di log.

Nota:

1. BLKSIZE deve essere specificato nell'istruzione SYSPRINT DD nel passo LOGDEF. BLKSIZE deve essere 629.
2. Per facilitare l'identificazione dei dataset bootstrap e dei dataset di log da gestori code differenti, includere il nome del sottosistema nel qualificatore di alto livello di tali dataset.
3. Se si utilizzano gruppi di condivisione code, è necessario definire i dataset bootstrap e log con SHAREOPTIONS (2 3).

Consultare Pianificazione su z/OS per informazioni sulla pianificazione dei dataset di log e di bootstrap e sulle relative dimensioni.

Da IBM MQ 8.0, il miglioramento RBA di log a 8 byte migliora la disponibilità di un gestore code, come descritto in Indirizzo byte relativo di log più grande. Per abilitare RBA di log a 8 byte su un gestore code prima che il gestore code venga avviato per la prima volta, effettuare le seguenti operazioni dopo aver creato l'ambiente di registrazione.

1. Utilizzando **IDCAMS ALTER**, ridenominare il formato BSDS della versione 1 (creato utilizzando il programma CSQJU003) con un valore simile a `++HLQ++.V1.BSDS01`.

   Nota: Assicurarsi di ridenominare i componenti dati e indice e il cluster VSAM.
2. Assegnare nuovi BSDS con gli stessi attributi già definiti. Questi diventeranno BSDS in formato versione 2 che verranno utilizzati dal gestore code quando viene avviato.
3. Eseguire il programma di utilità di conversione BSDS (CSQJUCNV) per convertire i BSDS in formato versione 1 nel nuovo formato BSDS versione 2.
4. Una volta completata correttamente la conversione, eliminare i BSDS in formato versione 1.

Nota: V 9.1.0 Se il gestore code si trova in un gruppo di condivisione code, tutti i gestori code nel gruppo di condivisione code devono essere stati avviati come segue prima di poter abilitare l'RBA di log di 8 byte:

- Se il gestore code è IBM MQ 8.0.0 deve essere stato avviato con **OPMODE**(*NEWFUNC,800*)
- Se il gestore code si trova in IBM MQ 9.0.0 LTS deve essere stato avviato con **OPMODE**(NEWFUNC,900) o **OPMODE**(*NEWFUNC,800*)
- Se il gestore code si trova su IBM MQ 9.0.n CD, IBM MQ 9.1.0 LTSo versione successiva, è necessario che sia stato avviato a tale livello

Concetti correlati

“Definisci le serie di pagine” a pagina 846
Definire le serie di pagine per ogni gestore code utilizzando uno dei campioni forniti.

z/OS *Definisci le serie di pagine*

Definire le serie di pagine per ogni gestore code utilizzando uno dei campioni forniti.

- *Ripetere questa attività per ogni gestore code IBM MQ*

  V 9.1.4 *Se si utilizza la codifica del dataset z/OS per proteggere le serie di pagine, è necessario configurare questa opzione prima che i dataset vengano assegnati in questo passo.*
- *Non è necessario eseguire questa attività quando si esegue la migrazione da una versione precedente.*

V 9.1.4 *Se si sta migrando un gestore code e si sta aggiungendo la codifica del dataset z/OS per i set di pagine, è necessario convertire i set di pagine.*

V 9.1.4 *Consultare la sezione,* Riservatezza per i dati inattivi su IBM MQ for z/OS con la crittografia del dataset. *Per ulteriori informazioni sulla configurazione della codifica del dataset z/OS e sulla conversione dei dataset IBM MQ esistenti da codificare.*

Definire serie di pagine separate per ciascun gestore code IBM MQ . thlqual.SCSQPROC(CSQ4PAGE) e thlqual.SCSQPROC(CSQ4PAGR) contengono istruzioni di controllo AMS (access method services) JCL e z/OS per definire e formattare le serie di pagine. Il membro CSQ4PAGE utilizza una serie di pagine per ciascuna classe di messaggi, il membro CSQ4PAGR utilizza più serie di pagine per le principali classi di messaggi. Il JCL esegue il programma di utilità fornito CSQUTIL. Rivedere gli esempi e personalizzarli per il numero di serie di pagine che si desidera e le dimensioni da utilizzare. Consultare Pianificazione su z/OS per informazioni sulle serie di pagine e su come calcolare le dimensioni appropriate.

La procedura dell'attività avviata CSQ4MSTR descritta in "Creare le procedure per il gestore code IBM MQ" a pagina 838 fa riferimento alle serie di pagine, in un'istruzione del formato:

```
//CSQP00nn DD DISP=OLD,DSN=xxxxxxxxxx
```

dove *nn* è il numero della serie di pagine compreso tra 00 e 99 e *xxxxxxxxxx* è il dataset definito.

Nota:

1. Se si intende utilizzare la funzione di espansione della serie di pagine dinamica, accertarsi che le estensioni secondarie siano definite per ciascuna serie di pagine. thlqual.SCSQPROC(CSQ4PAGE) mostra come effettuare questa operazione.
2. Per facilitare l'identificazione delle serie di pagine da gestori code differenti, includere il nome del sottosistema nel qualificatore di alto livello del dataset associato a ciascuna serie di pagine.
3. Se si desidera consentire l'utilizzo dell'opzione FORCE con la funzione FORMAT del programma di utilità CSQUTIL, è necessario aggiungere l'attributo REUSE all'istruzione AMS DEFINE CLUSTER. Ciò è descritto in Amministrazione di IBM MQ for z/OS.
4. Se le serie di pagine devono essere più grandi di 4 GB, è necessario utilizzare la funzione SMS (Storage Management System) EXTENDED ADDRESSABILITY.

Concetti correlati

"Aggiungere le voci IBM MQ alle tabelle Db2" a pagina 880
Se si utilizzano i gruppi di condivisione code, eseguire il programma di utilità CSQ5PQSG per aggiungere le voci del gruppo di condivisione code e del gestore code alle tabelle IBM MQ nel gruppo di condivisione dati Db2 .

z/OS *Personalizzare il modulo dei parametri di sistema*

Il modulo di parametri di sistema IBM MQ controlla gli ambienti di registrazione, archiviazione, traccia e connessione che IBM MQ utilizza nella sua operazione. Viene fornito un modulo predefinito. È necessario creare il proprio modulo dei parametri di sistema poiché alcuni parametri, ad esempio i nomi dei dataset, sono di solito specifici del sito.

- *Ripetere questa attività per ogni gestore code IBM MQ , come richiesto.*
- *Potrebbe essere necessario eseguire questa attività durante la migrazione da una versione precedente. Per i dettagli, consultare* Migrazione di IBM MQ su z/OS*.*
- *Per abilitare Advanced Message Security for z/OS su un gestore code esistente, è necessario impostare SPLCAP su YES come descritto in* "Utilizzo di CSQ6SYSP" a pagina 849*. Se si sta configurando questo gestore code per la prima volta, completare l'intera attività.*

Il modulo dei parametri di sistema dispone di V 9.1.0 quattro macro come segue:

Nome Macro	Finalità
CSQ6SYSP	Specifica i parametri di connessione e traccia, consultare “Utilizzo di CSQ6SYSP” a pagina 849
CSQ6LOGP	Controlla l'inizializzazione del log, consultare “Utilizzo di CSQ6LOGP” a pagina 858
CSQ6ARVP	Controlla l'inizializzazione dell'archivio, consultare “Utilizzo di CSQ6ARVP” a pagina 863
V 9.1.0 V 9.1.0 CSQ6USGP	Controlla la registrazione dell'utilizzo, consultare “Utilizzo di CSQ6USGP” a pagina 870

IBM MQ fornisce un modulo del parametro di sistema predefinito, CSQZPARM, che viene richiamato automaticamente se si immette il comando START QMGR (senza un parametro PARM) per avviare un'istanza di IBM MQ. CSQZPARM si trova nella libreria autorizzata APF thlqual.SCSQAUTH fornita anche con IBM MQ. I valori di questi parametri vengono visualizzati come una serie di messaggi quando si avvia IBM MQ.

Consultare START QMGR per ulteriori informazioni su come viene utilizzato questo comando.

Creazione del proprio modulo parametri di sistema

Se CSQZPARM non contiene i parametri di sistema desiderati, è possibile creare il proprio modulo di parametri di sistema utilizzando il JCL di esempio fornito in thlqual.SCSQPROC(CSQ4ZPRM).

Per creare il proprio modulo di parametri di sistema:

1. Creare una copia di lavoro dell'esempio JCL.
2. Modificare i parametri per ciascuna macro nella copia come richiesto. Se si rimuovono i parametri dalle chiamate macro, i valori predefiniti vengono automaticamente selezionati al runtime.
3. Sostituire il segnaposto ++NAME++ con il nome che il modulo di caricamento deve assumere (può essere CSQZPARM).
4. Se l'assembler non è un assembler di alto livello, modificare il JCL come richiesto dall'assembler.
5. Eseguire il JCL per assemblare e collegare le versioni personalizzate delle macro dei parametri di sistema per produrre un modulo di caricamento. Questo è il modulo del nuovo parametro di sistema con il nome specificato.
6. Inserire il modulo di caricamento prodotto in una libreria utente autorizzata APF.
7. Aggiungere l'accesso READ utente alla libreria utente autorizzato APF.
8. Includere questa libreria nella procedura STEPLIB dell'attività avviata del gestore code IBM MQ . Questo nome di libreria deve precedere la libreria thlqual.SCSQAUTH in STEPLIB.
9. Richiamare il modulo del nuovo parametro di sistema quando si avvia il gestore code. Ad esempio, se il nuovo modulo è denominato NEWMODS, immettere il comando:

   ```
   START QMGR PARM(NEWMODS)
   ```

10. Verificare il corretto completamento del comando controllando la registrazione del lavoro. Nel log dovrebbe essere presente una voce simile alla seguente:

    ```
    CSQ9022I CDL1 CSQYASCP 'START QMGR' NORMAL COMPLETION
    ```

È possibile anche specificare il nome del modulo del parametro nel JCL di avvio del gestore code. Per ulteriori informazioni, consultare Avvio e arresto di un gestore code.

Nota: Se si sceglie di denominare il modulo CSQZPARM, non è necessario specificare il parametro PARM nel comando START QMGR.

Ottimizzazione di un modulo di parametri di sistema

IBM MQ fornisce anche una serie di tre moduli di origine assembler, che possono essere utilizzati per ottimizzare un modulo di parametri di sistema esistente. Questi moduli si trovano nella libreria thlqual.SCSQASMS. In genere, questi moduli vengono utilizzati in un ambiente di test per modificare i parametri predefiniti nelle macro dei parametri di sistema. Ogni modulo di origine richiama una diversa macro di parametri di sistema:

Questo modulo di origine assembler ...	**Richiama questa macro ...**
CSQFSYSP	CSQ6SYSP (parametri di connessione e traccia)
CSQJLOGP	CSQ6LOGP (inizializzazione log)
VARVMQ	CSQ6ARVP (inizializzazione archivio)

Questo è il modo in cui si utilizzano questi moduli:

1. Creare copie di lavoro di ciascun modulo di origine assembler in una libreria assembler utente.
2. Modificare le copie aggiungendo o modificando i valori di qualsiasi parametro come richiesto.
3. Assemblare le copie di qualsiasi modulo modificato per creare moduli oggetto in una libreria oggetti utente.
4. Modificare questi moduli di codice oggetto con un modulo di parametro di sistema esistente per produrre un modulo di caricamento che sia il nuovo modulo di parametro di sistema.
5. Assicurarsi che il modulo del nuovo parametro di sistema sia un membro di una libreria utente autorizzata.
6. Includere questa libreria nella procedura STEPLIB dell'attività avviata del gestore code. Questa libreria deve precedere la libreria thlqual.SCSQAUTH in STEPLIB.
7. Richiamare il nuovo modulo del parametro di sistema emettendo un comando START QMGR, specificando il nuovo nome modulo nel parametro PARM, come prima.

Un usermod di esempio viene fornito nel membro CSQ4UZPR di SCSQPROC che dimostra come gestire i parametri di sistema personalizzati sotto il controllo SMP/E.

Modifica dei parametri di sistema

È possibile modificare alcuni parametri di sistema mentre un gestore code è in esecuzione; consultare i comandi SET SYSTEM, SET LOGe SET ARCHIVE .

Inserire i comandi SET nei dataset di input di inizializzazione in modo che diventino effettivi ogni volta che si avvia il gestore code.

Concetti correlati

“Adattare i parametri dell'iniziatore di canali” a pagina 871
Utilizzare ALTER QMGR per personalizzare l'iniziatore di canali in base ai propri requisiti.

z/OS *Utilizzo di CSQ6SYSP*

Utilizzare questo argomento come riferimento per l'impostazione dei parametri di sistema utilizzando CSQ6SYSP.

I parametri predefiniti per CSQ6SYSP, e se è possibile modificare ciascun parametro utilizzando il comando SET SYSTEM, sono riportati in Tabella 59 a pagina 850. Se si desidera modificare uno di questi valori, consultare le descrizioni dettagliate dei parametri.

Tabella 59. Valori predefiniti dei parametri CSQ6SYSP			
Parametro	**Descrizione**	**Valore predefinito**	**comando set**
ACELIM	Dimensione del pool di archiviazione ACE in blocchi da 1 KB.	0 (nessun limite)	✓
CLCACHE	Specifica il tipo di cache del cluster da utilizzare.	STATICO	-
CMDUSER	L'ID utente predefinito per i controlli di sicurezza dei comandi.	CSQOPR	-
EXCLMSG	Specifica un elenco di messaggi da escludere da qualsiasi registrazione. I messaggi in questo elenco non vengono inviati alla console z/OS e al log della copia cartacea. Di conseguenza, l'utilizzo del parametro EXCLMSG per escludere i messaggi è più efficiente da una prospettiva CPU rispetto all'utilizzo dei metodi descritti in “Elimina messaggi informativi” a pagina 876	( )	✓
EXITLIM	Tempo (in secondi) per cui le uscite del gestore code possono essere eseguite durante ogni chiamata.	30	-
EXITTCB	Il numero di attività del server avviate da utilizzare per eseguire le uscite del gestore code.	8	-
LOGLOAD	Numero di record di log scritti da IBM MQ tra l'avvio di un punto di controllo e il successivo.	500 000	✓
MULCCAPT	Determina la proprietà Determinazione del prezzo dell'utilizzo misurato che controlla l'algoritmo per raccogliere i dati utilizzati da MULC (Measured Usage License Charging).	Vedere descrizione parametro	-
OTMACON	Parametri di connessione OTMA.	Vedere descrizione parametro	-
QINDXBLD	Determina se il riavvio del gestore code attende la ricreazione di tutti gli indici o viene completato prima della ricreazione di tutti gli indici.	ATTESA	-
QMCCSID	CCSID (Coded character set identifier) per il gestore code.	Zero	-
DATAQG	Parametri del gruppo di condivisione code.	Vedere descrizione parametro	-
RESAUDIT	Parametro di controllo RESLEVEL.	SÌ	-
ROUTCDE	Il codice di instradamento del messaggio assegnato ai messaggi non sollecitati da una console specifica.	1	-
SERVICE	Riservato per l'utilizzo da parte di IBM.	0	✓

Tabella 59. Valori predefiniti dei parametri CSQ6SYSP (Continua)			
Parametro	**Descrizione**	**Valore predefinito**	**comando set**
SMFACCT	Specifica se i dati di account SMF devono essere raccolti all'avvio del gestore code. Tenere presente che i dati di account di canale di classe 4 vengono raccolti solo quando viene avviato l'iniziatore di canali.	No	-
SMFSTAT	Specifica se le statistiche SMF devono essere raccolte all'avvio del gestore code. Tenere presente che i dati statistici dell'iniziatore di canali di classe 4 vengono raccolti solo quando viene avviato l'iniziatore di canali.	No	-
SPLCAP	Specifica se la funzionalità della politica di sicurezza della coda è abilitata su questo gestore code. Per Advanced Message Security for z/OS, impostare questo parametro su YES.	No	-
STATIME	Tempo predefinito, in minuti, tra ogni raccolta di statistiche.	30	✓
TRACSTR	Specifica se la traccia deve essere avviata automaticamente.	No	-
TRACTBL	Dimensione della tabella di traccia, in blocchi da 4 KB, che deve essere utilizzata dalla funzione di traccia globale.	99 (396 KB)	✓
WLMTIME	Intervallo di tempo tra la scansione dell'indice della coda per le code gestite da WLM.	30	-
WLMTIMU	Unità (minuti o secondi) per WLMTIME.	minuti	-

ACELIM

Specifica la dimensione massima del pool di memoria ACE in blocchi da 1 KB. Il numero deve essere compreso tra 0 e 999999. Il valore predefinito zero indica nessun vincolo imposto, oltre a quanto è disponibile nel sistema.

È necessario impostare un valore solo per ACELIM sui gestori code che sono stati identificati come quelli che utilizzano quantità esorbitanti di memoria ECSA. Il limite del pool di memoria ACE ha l'effetto di limitare il numero di connessioni nel sistema, e quindi, la quantità di memoria ECSA utilizzata da un gestore code.

Una volta che il gestore code raggiunge il limite, non è possibile che le applicazioni ottengano nuove connessioni. La mancanza di nuove connessioni causa del malfunzionamenti nell'elaborazione MQCONN e le applicazioni coordinate tramite RRS riscontreranno probabilmente dei malfunzionamenti in qualsiasi API IBM MQ.

Un ACE rappresenta circa il 12,5% dell'ECSA totale richiesta per i blocchi di controllo correlati ai thread per una connessione. Quindi, ad esempio, specificando ACELIM=5120 si prevede di limitare la quantità totale di ECSA assegnata dal gestore code (per i blocchi di controllo relativi ai thread) a circa 40960K; , ossia 5120 moltiplicata per 8.

Per limitare la quantità totale di ECSA assegnata dal gestore code, per i blocchi di controllo correlati al thread a 5120K, è richiesto un valore ACELIM di 640.

È possibile utilizzare i record SMF 115 di sottotipo 5, prodotti dalla traccia CLASS(3) delle statistiche, per monitorare la dimensione del pool di memoria 'ACE/PEB' e impostare, quindi, un valore appropriato per ACELIM.

È possibile ottenere la quantità totale di memoria ECSA utilizzata dal gestore code, per i blocchi di controllo, dai record SMF 115 di sottotipo 7, scritti dalla traccia CLASS(2) delle statistiche; ossia i primi due elementi QSRSPHBT aggiunti insieme.

Tenere presente che si dovrebbe considerare l'impostazione di ACELIM come meccanismo per proteggere un'immagine z/OS da un comportamento errato del gestore code, anziché come mezzo per controllare le connessioni dell'applicazione a un gestore code.

CACHE
Specifica il tipo di cache del cluster da utilizzare.

La cache del cluster è un'area di memoria utilizzata per memorizzare le informazioni relative al cluster.

Se la cache del cluster è statica, ha una dimensione fissa, allocata all'avvio del gestore code. Se la cache si riempie, viene emesso il messaggio CSQM060E e la richiesta dell'applicazione che richiede più spazio riceve un MQRC_CLUSTER_RESOURCE_ERROR.

Se si imposta CLCACHE su dinamico, la cache del cluster può espandersi come richiesto. Tuttavia, è necessario prima assicurarsi che le uscite del carico di lavoro del cluster installate possano funzionare con una cache dinamica.

Se un'uscita del carico di lavoro del cluster installato non può funzionare con un messaggio della cache dinamica, viene emesso CSQM061E .

MQXCLWLNviene fornito per le uscite del carico di lavoro del cluster per navigare nella cache del cluster in modo che funzioni indipendentemente dal fatto che vengano utilizzate cache dinamiche o statiche.

Per i nuovi gestori code, impostare CLCACHE=DYNAMIC, a meno che non si stia utilizzando un'uscita del carico di lavoro del cluster che non supporta la cache dinamica.

Per i gestori code esistenti che utilizzano già una cache statica e che si trovano in un cluster a cui non sono state aggiunte molte nuove code e gestori code, è ragionevole continuare a utilizzare CLCACHE=STATIC.

Per i gestori code esistenti che già utilizzano una cache statica e che si trovano in un cluster a cui verranno aggiunte molte nuove code o gestori code, iniziare a utilizzare CLCACHE=DYNAMIC.

STATICO
Quando la cache del cluster è statica, la sua dimensione è fissa all'avvio del gestore code, sufficiente per la quantità corrente di informazioni sul cluster più spazio per l'espansione. La dimensione non può aumentare mentre il gestore code è attivo. Questa è l'opzione predefinita.

DINAMICO
Quando la cache del cluster è dinamica, la dimensione iniziale assegnata all'avvio del gestore code può essere aumentata automaticamente se richiesto mentre il gestore code è attivo.

CMDUSER
Specifica l'ID utente predefinito utilizzato per i controlli di sicurezza dei comandi. Questo ID utente deve essere definito in ESM (ad esempio, RACF). Specificare un nome composto da 1 a 8 caratteri alfanumerici. Il primo carattere deve essere un carattere alfabetico.

Il valore predefinito è CSQOPR.

EXCLMSG
Specifica un elenco di messaggi di errore da escludere.

Questo elenco è dinamico e viene aggiornato utilizzando il comando SET SYSTEM.

Il valore predefinito è un elenco vuoto ().

I messaggi vengono forniti senza il prefisso CSQ e senza il suffisso del codice azione (I - D - E - A). Ad esempio, per escludere il messaggio CSQX500I, aggiungere X500 a questo elenco. Questo elenco può contenere un massimo di 16 identificativi di messaggio.

Per essere idoneo ad essere incluso nell'elenco, il messaggio deve essere emesso dopo il normale avvio degli spazi di indirizzo MSTR o CHIN e deve iniziare con uno dei seguenti caratteri E, H, I, J, L, M, N, P, R, T, V, W, X, Y, 2, 3, 5, 9.

Gli ID messaggio emessi come risultato dei comandi di elaborazione possono essere aggiunti all'elenco, tuttavia non verranno esclusi. Ad esempio, un identificativo di messaggio viene emesso come risultato del comando DISPLAY USAGE PSID (*), tuttavia, questo messaggio non può essere eliminato.

EXITLIM
Specifica il tempo, in secondi, consentito per ogni richiamo delle uscite del gestore code. (Questo parametro non ha alcun effetto sulle uscite del canale.)

Specificare un valore compreso tra 5 e 9999.

Il valore predefinito è 30. Il gestore code esegue il polling delle uscite in esecuzione ogni 30 secondi. Su ogni polling, tutti quelli che sono stati in esecuzione per un periodo di tempo superiore a quello specificato da EXITLIM vengono forzatamente terminati.

EXITTCB
Specifica il numero di attività del server avviate da utilizzare per eseguire le uscite nel gestore code. (Questo parametro non ha alcun effetto sulle uscite del canale.) È necessario specificare un numero almeno pari al numero massimo di uscite (diverse dalle uscite del canale) che il gestore code potrebbe dover eseguire, altrimenti avrà esito negativo con una fine anomala 6c6 .

Specificare un valore compreso tra zero e 99. Un valore zero indica che non è possibile eseguire alcuna uscita.

Il valore predefinito è 8.

LOGLOAD
Specifica il numero di record di log che IBM MQ scrive tra l'avvio di un checkpoint e il successivo. IBM MQ avvia un nuovo checkpoint dopo aver scritto il numero di record specificato.

Specificare un valore compreso tra 200 e 16 000 000.

Il valore predefinito è 500 000.

Maggiore è il valore, migliori sono le prestazioni di IBM MQ ; tuttavia, il riavvio richiede più tempo se il parametro è impostato su un valore elevato.

Impostazioni suggerite:

Sistema di test	10 000
Sistema di produzione	500 000 In un sistema di produzione, il valore predefinito fornito potrebbe risultare in una frequenza di checkpoint troppo elevata.

Il valore di LOGLOAD determina la frequenza dei checkpoint del gestore code. Un valore troppo grande significa che una grande quantità di dati viene scritta nel log tra i punti di controllo, determinando un aumento del tempo di riavvio del ripristino di inoltro del gestore code in seguito a un errore. Un valore troppo piccolo fa sì che i checkpoint si verifichino troppo frequentemente durante il carico di picco, influenzando negativamente i tempi di risposta e l'utilizzo del processore.

Per LOGLOAD si suggerisce un valore iniziale di 500 000. Per una frequenza di messaggi persistenti da 1 KB di 100 messaggi al secondo (ossia, 100 MQPUT con commit e 100 MQGET con commit) l'intervallo tra i punti di controllo è di circa 5 minuti.

Nota: Ciò è inteso solo come una linea guida e il valore ottimale per questo parametro dipende dalle caratteristiche del singolo sistema.

MULCCAPT
Specifica l'algoritmo da utilizzare per la raccolta dei dati utilizzati da MULC (Measured Usage License Charging).

STANDARD
MULC è basato sull'ora dalla chiamata MQCONN API IBM MQ all'ora della chiamata MQDISC API IBM MQ .

Dettagliato
MULC si basa sul tempo che va dall'inizio di una chiamata API IBM MQ alla fine della chiamata API IBM MQ .

Il valore predefinito è STANDARD

OTMACON
Parametri OTMA. Questa parola chiave accetta cinque parametri posizionali:

OTMACON = (`Group,Member,Druexit,Age,Tpipepfx`)

Gruppo
Questo è il nome del gruppo XCF a cui appartiene questa particolare istanza di IBM MQ .

Può essere lungo da 1 a 8 caratteri e deve essere immesso in caratteri maiuscoli.

Il valore predefinito è vuoto, che indica che IBM MQ non deve tentare di unirsi a un gruppo XCF.

Membro
Questo è il nome del membro di questa istanza particolare di IBM MQ all'interno del gruppo XCF.

Può contenere da 1 a 16 caratteri e deve essere immesso in caratteri maiuscoli.

Il valore predefinito è il nome del gestore code di 4 caratteri.

Druexit
Specifica il nome dell'uscita utente di risoluzione della destinazione OTMA che deve essere eseguito da IMS.

Può contenere da 1 a 8 caratteri.

Il valore predefinito è DFSYDRU0.

Questo parametro è facoltativo; è obbligatorio se IBM MQ deve ricevere i messaggi da un'applicazione IMS che non è stata avviata da IBM MQ. Il nome deve corrispondere all'uscita utente di risoluzione di destinazione codificata nel sistema IMS . Per ulteriori informazioni, fare riferimento a “Utilizzo delle uscite OTMA in IMS” a pagina 943.

Età
Rappresenta il periodo di tempo, in secondi, in cui un ID utente da IBM MQ viene considerato precedentemente verificato da IMS.

Può essere compreso tra zero e 2 147 483 647.

Il valore predefinito è 2 147 483 647.

Si consiglia di impostare questo parametro insieme al parametro `interval` del comando ALTER SECURITY per mantenere la coerenza delle impostazioni della cache di sicurezza nel mainframe.

Tpipepfx
Rappresenta il prefisso da utilizzare per i nomi Tpipe.

Comprende tre caratteri; il primo carattere è compreso nell'intervallo da A a Z, i caratteri successivi sono da A a Z o da 0 a 9. Il valore predefinito è CSQ.

Viene utilizzato ogni volta che IBM MQ crea un Tpipe; il resto del nome viene assegnato da IBM MQ. Non è possibile impostare il nome Tpipe completo per qualsiasi Tpipe creato da IBM MQ.

QINDXBLD
Determina se il riavvio del gestore code attende la ricreazione di tutti gli indici della coda o viene completato prima della ricreazione di tutti gli indici.

ATTESA
Il riavvio del gestore code attende il completamento di tutte le build dell'indice della coda. Ciò significa che non viene ritardata alcuna applicazione durante la normale elaborazione dell'API IBM MQ durante la creazione dell'indice, poiché tutti gli indici vengono creati prima che le applicazioni possano connettersi al gestore code.

Questa è l'opzione predefinita.

Nessuna attesa
Il gestore code può essere riavviato prima che venga completata la creazione dell'indice della coda.

QMCCSID
Specifica il CCSID (coded character set identifier) predefinito che il gestore code (e quindi l'accodamento distribuito) deve utilizzare.

Specificare un valore compreso tra zero e 65535. Il valore deve rappresentare una codepage EBCDIC elencata come codepage z/OS nativa per la lingua scelta in Lingue nazionali.

Zero, che è il valore predefinito, significa utilizzare il CCSID correntemente impostato oppure, se non è impostato, utilizzare il CCSID 500. Ciò significa che se il CCSID è stato esplicitamente impostato su un valore diverso da zero, non è possibile reimpostarlo impostando QMCCSID su zero; è ora necessario utilizzare il CCSID diverso da zero corretto. Se QMCCSID è zero, è possibile controllare quale CCSID è attualmente in uso immettendo il comando DISPLAY QMGR CCSID.

DATASGQ
Dati del gruppo di condivisione code. Questa parola chiave accetta cinque parametri posizionali:

QSGDATA = (Qsgname,Dsgname,Db2name,Db2serv ,Db2blob)

QSGNAME
Questo è il nome del gruppo di condivisione code a cui appartiene il gestore code.

Consultare Regole per la denominazione degli oggetti IBM MQ per i caratteri validi. Il nome:

- Può contenere da 1 a 4 caratteri
- Non deve iniziare con un valore numerico
- Non deve terminare con @.

  Questo perché, per motivi di implementazione, i nomi con meno di quattro caratteri vengono riempiti internamente con simboli @,

Il valore predefinito è vuoto, che indica che il gestore code non è un membro di alcun gruppo di condivisione code.

Nomegg
Questo è il nome del gruppo di condivisione dati Db2 a cui deve connettersi il gestore code.

Può essere lungo da 1 a 8 caratteri e deve essere immesso in caratteri maiuscoli.

Il valore predefinito è vuoto, che indica che non si stanno utilizzando gruppi di condivisione code.

Db2name
Questo è il nome del sottosistema o del gruppo Db2 a cui deve connettersi il gestore code.

Può contenere da 1 a 4 caratteri e deve essere immesso in caratteri maiuscoli.

Il valore predefinito è vuoto, che indica che non si stanno utilizzando gruppi di condivisione code.

Nota: Il sottosistema Db2 (o l'allegato del gruppo) deve far parte del gruppo di condivisione dati Db2 specificato in Dsgnamee tutti i gestori code devono specificare lo stesso gruppo di condivisione dati Db2 .

Db2serv
Questo è il numero di attività del server utilizzate per accedere a Db2.

Può essere compreso tra 4 e 10.

Il valore predefinito è 4.

Db2blob
Questo è il numero di attività Db2 utilizzate per accedere ai BLOB (Binary Large Object).

Può essere compreso tra 4 e 10.

Il valore predefinito è 4.

Se si specifica uno dei parametri del nome (ovvero, **Qsgname**, **Dsgname**o **Db2name**), è necessario immettere i valori per gli altri nomi, altrimenti IBM MQ non riesce.

RESAUDIT
Specifica se i record di controllo RACF vengono scritti per i controlli di sicurezza RESLEVEL eseguiti durante l'elaborazione della connessione.

Specificare uno tra:

No
Il controllo RESLEVEL non viene eseguito.

SÌ
Viene eseguito il controllo RESLEVEL.

Il valore predefinito è YES.

ROUTCDE
Specifica il codice di instradamento del messaggio z/OS predefinito assegnato ai messaggi che non vengono inviati in risposta diretta a un comando MQSC.

Specificare uno tra:

1. Un valore compreso nell'intervallo tra 1 e 16, inclusi.
2. Un elenco di valori, separati da una virgola e racchiusi tra parentesi. Ciascun valore deve essere compreso tra 1 e 16, inclusi.

Il valore predefinito è 1.

Per ulteriori informazioni sui codici di instradamento z/OS , consultare *Descrizione del messaggio* in uno dei volumi del manuale *z/OS MVS Routing and Descriptor Codes* .

SERVICE
Questo campo è riservato per l'utilizzo da parte di IBM.

SMFACCT
Specifica se IBM MQ invia i dati di account a SMF automaticamente quando viene avviato il gestore code.

Specificare uno tra:

No
Non avviare automaticamente la raccolta dei dati di account.

SÌ
Avviare la raccolta automatica dei dati di account per la classe predefinita 1.

numeri interi
Un elenco di classi per cui la contabilità viene raccolta automaticamente nell'intervallo compreso tra 1 e 4.

Il valore predefinito è NO.

SMFSTAT
Specifica se raccogliere le statistiche SMF automaticamente all'avvio del gestore code.

Specificare uno tra:

No
Non avviare automaticamente la raccolta delle statistiche.

SÌ
Avviare la raccolta automatica delle statistiche per la classe predefinita 1.

numeri interi
Un elenco di classi per cui le statistiche vengono raccolte automaticamente nell'intervallo compreso tra 1 e 4. Per raccogliere le statistiche di classe 2 o 3, è necessario specificare anche la classe 1.

Il valore predefinito è NO.

SPLCAP
La funzione della politica di sicurezza abilita un livello più elevato di sicurezza dei messaggi tramite politiche che controllano se i messaggi sono firmati o codificati, quando vengono scritti e letti dalle code.

L'elaborazione della politica di sicurezza è abilitata per questo gestore code, configurando SPLCAP con uno dei seguenti valori:

No
La funzione di implementazione delle politiche di sicurezza dei messaggi per le code non viene abilitata durante l'inizializzazione del gestore code.

SÌ
LTS Le funzioni di sicurezza dei messaggi sono abilitate durante l'inizializzazione del gestore code.

Se questo controllo è impostato, il gestore code tenta di caricare il modulo di abilitazione licenza da SDRQAUTH durante l'inizializzazione e di avviare un ulteriore spazio di indirizzo (AMSM).

Il gestore code non viene avviato a meno che AMS non disponga della licenza e che non sia attiva la configurazione necessaria per la sicurezza dei messaggi.

V 9.1.3 Se il gestore code è in esecuzione su IBM MQ 9.1.2 o versioni precedenti, controlla che la libreria SDRQAUTH faccia parte di STEPLIB del gestore code e contenga il modulo di abilitazione AMS .

Se in esecuzione su IBM MQ 9.1.3 o versioni successive, il gestore code controlla che l'attributo AMSPROD sia impostato su AMS, ADVANCED o ADVANCEDVUE.

Se questi controlli hanno esito positivo, le funzioni di sicurezza dei messaggi vengono abilitate durante l'inizializzazione del gestore code e lo spazio di indirizzo AMSM viene avviato.

Se questi controlli non riescono o se è attiva la configurazione necessaria per la sicurezza dei messaggi, l'avvio del gestore code non riesce.

Il valore predefinito è NO.

STATIME
Specifica il tempo predefinito, in minuti, tra le raccolte consecutive di statistiche.

Specificare un numero compreso nell'intervallo tra zero e 1440.

Se si specifica il valore zero, vengono raccolti sia i dati statistici che i dati sugli account alla trasmissione della raccolta dati di SMF. Consultare Utilizzo di System Management Facility per informazioni sull'impostazione.

Il valore predefinito è 30.

TRACSTR
Specifica se la traccia globale deve essere avviata automaticamente.

Specificare uno tra:

No
Non avviare automaticamente la traccia globale.

SÌ
Avviare automaticamente la traccia globale per la classe predefinita, classe 1.

numeri interi
Un elenco di classi per cui la traccia globale deve essere avviata automaticamente nell'intervallo compreso tra 1 e 4.

*****
Avviare automaticamente la traccia globale per tutte le classi.

Il valore predefinito è NO se non si specifica la parola chiave nella macro.

Nota: Il modulo di caricamento del parametro di sistema predefinito fornito (CSQZPARM) ha TRACSTR=YES (impostato nel modulo assembler CSQFSYSP). Se non si desidera avviare la traccia automaticamente, creare il proprio modulo dei parametri di sistema o immettere il comando STOP TRACE dopo l'avvio del gestore code.

Per i dettagli sul comando STOP TRACE, consultare STOP TRACE.

TRACTBL
Specifica la dimensione predefinita, in blocchi da 4 KB, della tabella di traccia in cui la funzione di traccia globale memorizza i record di traccia IBM MQ .

Specificare un valore compreso tra 1 e 999.

Il valore predefinito è 99. Ciò equivale a 396 KB.

Nota: La memoria per la tabella di traccia è assegnata in ECSA. Pertanto, è necessario selezionare questo valore con attenzione.

WLMTIME
Specifica il tempo (in minuti o secondi a seconda del valore di WLMTIMU) tra ogni scansione degli indici per le code gestite da WLM.

Specificare un valore compreso tra 1 e 9999.

Il valore predefinito è 30.

WLMTIMU
Unità di tempo utilizzate con il parametro WLMTIME.

Specificare uno tra:

minuti
WLMTIME rappresenta un numero di minuti.

sec.
WLMTIME rappresenta un numero di secondi.

Il valore predefinito è MINS.

Riferimenti correlati

“Utilizzo di CSQ6LOGP” a pagina 858
Utilizzare questo argomento come riferimento per la specifica delle opzioni di registrazione utilizzando CSQ6LOGP.

“Utilizzo di CSQ6ARVP” a pagina 863
Utilizzare questo argomento come riferimento per specificare l'ambiente di archiviazione utilizzando CSQ6ARVP .

z/OS *Utilizzo di CSQ6LOGP*

Utilizzare questo argomento come riferimento per la specifica delle opzioni di registrazione utilizzando CSQ6LOGP.

Utilizzare CSQ6LOGP per stabilire le opzioni di registrazione.

I parametri predefiniti per CSQ6LOGPe se è possibile modificare ciascun parametro utilizzando il comando SET LOG , vengono visualizzati in Valori predefiniti dei parametri CSQ6LOGP. Se è necessario modificare uno qualsiasi di questi valori, fare riferimento alle descrizioni dettagliate dei parametri.

Tabella 60. Valori predefiniti dei parametri CSQ6LOGP

Parametro	Descrizione	Valore predefinito	comando set
COMPLOG	Controlla se la compressione del log è abilitata.	NESSUNO	X
DEALLCT	L'intervallo di tempo durante il quale un'unità nastro di archiviazione rimane inutilizzata prima che venga annullata l'assegnazione.	zero	X
INBUFF	Dimensione della memoria buffer di input per i dataset di log di archivio e attivi.	60 KB	-
MAXARCH	Numero massimo di volumi di log di archivio che è possibile registrare.	500	X
MAXCNOFF	Numero massimo di attività offload CSQJOFF7 che possono essere eseguite in parallelo.	31	-
MAXRTU	Numero massimo di unità nastro dedicate assegnate per leggere simultaneamente i volumi nastro del log di archivio.	2	X
OFFLOAD	Archiviazione attiva o disattiva.	SÌ (ON)	-
OUTBUFF	Dimensione della memoria buffer di output per i dataset di log di archivio e attivi.	4.000 KB	-
TWOACTV	Registrazione attiva singola o doppia.	YES (duale)	-
TWOARCH	Registrazione di archivio singola o doppia.	YES (duale)	-
TWOBSDS	BSDS singolo o doppio.	YES (doppio BSDS)	-
WRTHRSH	Numero di buffer di output da riempire prima che vengano scritti nei dataset di log attivi.	20	X
V 9.1.2 V 9.1.2 ZHYWRITE	Specifica se la funzione di scrittura zHyperè abilitata.	NO	X

COMPLOG

Specifica se la compressione log è abilitata.

Specificare:

NESSUNO

La compressione log non è abilitata.

RLE

La compressione log è abilitata utilizzando la codifica di lunghezza di esecuzione.

ANY

Il gestore code seleziona l'algoritmo di compressione che fornisce il maggior grado di compressione dei record di log. Questa opzione risulta nella compressione RLE.

Il valore predefinito è Nessuno.

Per ulteriori dettagli sulla compressione log, consultare Compressione log.

DEALLCT
Specifica l'intervallo di tempo, in minuti, durante il quale un'unità nastro di lettura di archivio può rimanere inutilizzata prima che ne venga annullata l'assegnazione.

Specificare una delle seguenti opzioni:

- Tempo, in minuti, compreso tra zero e 1440
- Nessun limite

Specificare 1440 o NOLIMIT significa che l'unità nastro non viene mai deallocata.

Il valore predefinito è zero.

Quando i dati del log di archivio vengono letti dal nastro, si consiglia di impostare questo valore su un valore sufficientemente elevato da consentire a IBM MQ di ottimizzare la gestione del nastro per più applicazioni di lettura.

INBUFF
Specifica la dimensione, in kilobyte, del buffer di input per la lettura dei log attivi e di archiviazione durante il ripristino. Utilizzare un numero decimale compreso tra 28 e 60. Il valore specificato viene arrotondato a un multiplo di 4.

Il valore predefinito è 60 KB.

Impostazioni suggerite:

Sistema di test	28 KB
Sistema di produzione	60 KB Impostare questo valore sul valore massimo per le migliori prestazioni di lettura del log.

MAXARCH
Specifica il numero massimo di volumi di log di archivio che possono essere registrati in BSDS. Quando questo numero viene superato, la registrazione inizia di nuovo all'avvio del BSDS.

Utilizzare un numero decimale compreso tra 10 e 1000.

Il valore predefinito è 500.

Impostazioni suggerite:

Sistema di test	500 (valore predefinito)
Sistema di produzione	1 000 Impostare questo valore su un valore massimo, in modo che BSDS possa registrare il maggior numero di log possibile.

Per informazioni sui log e su BSDS, vedi Gestione delle risorse IBM MQ.

MAXCNOFF
Specifica il numero di attività offload CSQJOFF7 che possono essere eseguite in parallelo.

Ciò consente a un gestore code, o gestori code, di essere ottimizzati in modo che non utilizzino tutte le unità nastro disponibili.

Il gestore code, invece, attende il completamento di un'attività di offload CSQJOFF7 prima di tentare di allocare nuovi dataset di archivio.

Se il gestore code è in fase di archiviazione su nastro, impostare questo parametro in modo che il numero di richieste nastro simultanee non sia uguale o superiore al numero di unità nastro disponibili, altrimenti il sistema potrebbe bloccarsi.

Tenere presente che se è in uso l'archiviazione doppia, ogni attività di offload esegue entrambi gli archivi, quindi il parametro deve essere impostato di conseguenza. Ad esempio, se il gestore code è una doppia archiviazione su nastro, un valore di MAXCNOFF=2 consente di archiviare contemporaneamente fino a due log attivi su quattro nastri.

Se diversi gestori code condividono le unità nastro, è necessario impostare MAXCNOFF per ciascun gestore code di conseguenza.

Il valore predefinito è 31.

Specificare un valore compreso tra 1 e 31.

MAXRTU
Specifica il numero massimo di unità nastro dedicate che possono essere assegnate per leggere simultaneamente i volumi nastro di registrazione archivio.

Questo parametro e il parametro DEALLCT consentono a IBM MQ di ottimizzare la lettura del log di archiviazione dalle periferiche nastro.

Specificare un valore compreso tra 1 e 99.

Il valore predefinito è 2.

Si consiglia di impostare il valore in modo che sia almeno uno in meno del numero di unità nastro disponibili per IBM MQ. In caso contrario, il processo di offload potrebbe essere ritardato, il che potrebbe influire sulle prestazioni del proprio sistema. Per la massima velocità di trasmissione durante l'elaborazione del log di archivio, specificare il valore massimo possibile per questa opzione, ricordando che è necessaria almeno un'unità nastro per l'elaborazione dell'offload.

OFFLOAD
Specifica se l'archiviazione è attiva o disattivata.

Specificare:

Sì
L'archiviazione è attiva

NO
L'archiviazione è disattivata

Il valore predefinito è YES.

Attenzione: Non disattivare l'archiviazione a meno che non si stia lavorando in un ambiente di test. Se lo si disattiva, non è possibile garantire che i dati vengano recuperati in caso di errore di sistema o di transazione.

OUTBUFF
Specifica la dimensione totale, in kilobyte, della memoria che deve essere utilizzata da IBM MQ per i buffer di output per la scrittura dei dataset di log di archiviazione e attivi. Ogni buffer di output è di 4 KB.

Il valore del parametro deve essere compreso tra 128 e 4000. Il valore specificato viene arrotondato a un multiplo di 4. I valori compresi tra 40 e 128 verranno accettati per motivi di compatibilità e vengono considerati come un valore di 128.

Il valore predefinito è 4000 KB.

Impostazioni suggerite:

Sistema di test	400 KB
Sistema di produzione	4.000 KB Impostare questo valore sul valore massimo per evitare di esaurire i buffer di output del log.

TWOACTV
Specifica la registrazione attiva singola o doppia.

Specificare:

NO
Singoli log attivi

Sì
Log attivi doppi

Il valore predefinito è YES.

Per ulteriori informazioni sull'utilizzo della registrazione singola e doppia, vedi Gestione delle risorse IBM MQ.

TWOARCH
Specifica il numero di log di archivio che IBM MQ produce quando il log attivo viene scaricato.

Specificare:

NO
Log di archivio singoli

Sì
Log di archivio doppi

Il valore predefinito è YES.

Impostazioni suggerite:

Sistema di test	NO
Sistema di produzione	Sì (impostazione predefinita)

Per ulteriori informazioni sull'utilizzo della registrazione singola e doppia, vedi Gestione delle risorse IBM MQ.

TWOBSDS
Specifica il numero di dataset bootstrap.

Specificare:

NO
BSDS singolo

Sì
BSDS doppio

Il valore predefinito è YES.

Per ulteriori informazioni sull'utilizzo della registrazione singola e doppia, vedi Gestione delle risorse IBM MQ.

WRTHRSH
Specifica il numero di buffer di output da 4 KB da riempire prima che vengano scritti nei dataset di log attivi.

Maggiore è il numero di buffer, minore è la frequenza di scrittura e ciò migliora le prestazioni di IBM MQ. I buffer potrebbero essere scritti prima che questo numero venga raggiunto se si verificano eventi significativi, come un punto di commit.

Specificare il numero di buffer compreso tra 1 e 256.

Il valore predefinito è 20.

V 9.1.2 **ZHYWRITE**
Specifica se le scritture sui log attivi vengono effettuate con zHyperWrite abilitato. I dataset di log attivi devono trovarsi su volumi con supporto zHyperWrite affinché zHyperWrite sia abilitato.

Per ulteriori informazioni sull'abilitazione dei log attivi con zHyperWrite, consultare Utilizzo di zHyperWrite con i log attivi IBM MQ.

Il valore può essere:

No
zHyperWrite non è abilitato.

SÌ
zHyperWrite è abilitato.

Riferimenti correlati

“Utilizzo di CSQ6SYSP” a pagina 849
Utilizzare questo argomento come riferimento per l'impostazione dei parametri di sistema utilizzando CSQ6SYSP.

“Utilizzo di CSQ6ARVP” a pagina 863
Utilizzare questo argomento come riferimento per specificare l'ambiente di archiviazione utilizzando CSQ6ARVP .

z/OS *Utilizzo di CSQ6ARVP*

Utilizzare questo argomento come riferimento per specificare l'ambiente di archiviazione utilizzando CSQ6ARVP .

Utilizzare CSQ6ARVP per definire l'ambiente di archiviazione.

I parametri predefiniti per CSQ6ARVPe se è possibile modificare ciascun parametro utilizzando il comando SET ARCHIVE, sono riportati in Tabella 61 a pagina 863. Se è necessario modificare uno qualsiasi di questi valori, fare riferimento alle descrizioni dettagliate dei parametri. Per ulteriori informazioni sulla pianificazione della tua archiviazione, vedi Pianificazione dei requisiti di archiviazione e prestazioni su z/OS .

Tabella 61. Valori predefiniti dei parametri di CSQ6ARVP

Parametro	Descrizione	Valore predefinito	comando set
ALCUNIT	Unità in cui vengono effettuate le assegnazioni di spazio primario e secondario.	BLK (blocchi)	X
ARCPFX1	Prefisso per il nome del primo dataset di log di archivio.	CSQARC1	X
ARCPFX2	Prefisso per il secondo nome dataset di log di archiviazione.	CSQARC2	X
ARCRETN	Il periodo di conservazione del dataset del log di archivio in giorni.	9999	X
ARCWRTC	Elenco di codici di instradamento per i messaggi all'operatore sui dataset di log di archivio.	1,3,4	X
ARCWTOR	Indica se inviare il messaggio all'operatore e attendere la risposta prima di provare a montare un dataset del log di archivio.	SÌ	X
BLKSIZE	Dimensione blocco del dataset del log di archiviazione.	28 672	X
Catalogo	Indica se i dataset di log di archiviazione sono catalogati in ICF.	No	X
COMPACT	Se i dataset di log di archivio devono essere compattati.	No	X
PRIQTY	Assegnazione spazio principale per i dataset DASD.	25 715	X

Tabella 61. Valori predefiniti dei parametri di CSQ6ARVP (Continua)			
Parametro	**Descrizione**	**Valore predefinito**	**comando set**
PROTECT	Indica se i dataset di log di archiviazione sono protetti dai profili ESM quando vengono creati i dataset.	No	X
QUIESCE	Tempo massimo, in secondi, consentito per la sospensione quando viene specificato ARCHIVE LOG con MODE (QUIESCE).	5	X
SECQTY	Allocazione spazio secondario per i dataset DASD. Consultare il parametro ALCUNIT per le unità da utilizzare.	540	X
TSTAMP	Se il nome del dataset di archivio deve includere una data / ora.	No	X
Unità	Il tipo di dispositivo o il nome dell'unità su cui è memorizzata la prima copia dei dataset del log di archivio.	Nastro	X
UNIT2	Tipo di dispositivo o nome unità su cui è memorizzata la seconda copia dei dataset del log di archivio.	Spazio	X

ALCUNIT
Specifica l'unità in cui vengono create le allocazioni di spazio primarie e secondarie.

Specificare uno tra:

CYL
Cilindri

TRK
Tracce

BLK
Blocchi

Si consiglia di utilizzare BLK perché è indipendente dal tipo di unità.

Il valore predefinito è BLK.

Se è probabile che lo spazio libero sui volumi DASD di archivio sia frammentato, si consiglia di specificare un'estensione primaria più piccola e consentire l'espansione in estensioni secondarie. Per ulteriori informazioni sull'allocazione dello spazio per i log attivi, fare riferimento a Pianificazione dell'archivio di log.

ARCPFX1
Specifica il prefisso per il nome del primo dataset del log di archiviazione.

Consultare il parametro TSTAMP per una descrizione del modo in cui sono denominati i dataset e per le restrizioni sulla lunghezza di ARCPFX1.

Questo parametro non può essere lasciato vuoto.

Il valore predefinito è CSQARC1.

Potrebbe essere necessario autorizzare l'ID utente associato allo spazio di indirizzo del gestore code IBM MQ per creare i log di archivio con questo prefisso.

ARCPFX2
Specifica il prefisso per il secondo nome dataset di log di archiviazione.

Consultare il parametro TSTAMP per una descrizione di come vengono denominati i dataset e per le restrizioni sulla lunghezza di ARCPFX2.

Questo parametro non può essere vuoto anche se il parametro TWOARCH è specificato come NO.

Il predefinito è CSQARC2.

Potrebbe essere necessario autorizzare l'ID utente associato allo spazio di indirizzo del gestore code IBM MQ per creare i log di archivio con questo prefisso.

ARCRETN
Specifica il periodo di conservazione, in giorni, da utilizzare quando viene creato il dataset del log di archiviazione.

Il valore del parametro deve essere compreso tra zero e 9999.

Il valore predefinito è 9999.

Impostazioni suggerite:

Sistema di test	3 In un sistema di test, i log di archivio probabilmente non sono richiesti per lunghi periodi.
Sistema di produzione	9 999 (valore predefinito) Impostare questo valore su un valore elevato per disattivare in modo efficace l'eliminazione automatica del log di archiviazione.

Per ulteriori informazioni sull'eliminazione dei dataset di log di archiviazione, consultare Eliminazione dei dataset di log di archiviazione.

ARCWRTC
Specifica l'elenco di codici di instradamento z/OS per i messaggi relativi ai dataset di log di archivio all'operatore. Questo campo viene ignorato se ARCWTOR è impostato su NO.

Specificare un massimo di 14 codici di instradamento, ciascuno con un valore compreso tra 1 e 16. È necessario specificare almeno un codice. Separare i codici nell'elenco con virgole e non con spazi.

Il valore predefinito è l'elenco dei valori: 1,3,4.

Per ulteriori informazioni sui codici di instradamento z/OS , consultare *Routing codes* in *Descrizione del messaggio* in uno dei volumi dei manuali *z/OS MVS System Messages* .

ARCWTOR
Specifica se deve essere inviato un messaggio all'operatore e si deve ricevere una risposta prima di tentare il montaggio di un dataset di log di archivio.

Altri utenti di IBM MQ potrebbero essere forzati ad attendere che venga montato il dataset ma non ne risentono mentre IBM MQ attende la risposta al messaggio.

Specificare:

SÌ
Il dispositivo richiede molto tempo per montare i dataset di log di archivio. Ad esempio, un'unità nastro.

No
Il dispositivo non ha lunghi ritardi. Ad esempio, DASD.

Il valore predefinito è YES.

Impostazioni suggerite:

Sistema di test	No

Sistema di produzione	Sì (impostazione predefinita) Ciò dipende dalle procedure operative. Se vengono utilizzati i robot nastro, NO potrebbe essere più appropriato.

BLKSIZE
Specifica la dimensione blocco del dataset del log di archiviazione. La dimensione del blocco specificata deve essere compatibile con il tipo di unità specificato nel parametro UNIT.

Il parametro deve essere compreso tra 4 097 e 28 672. Il valore specificato viene arrotondato per eccesso a un multiplo di 4 096.

Il valore predefinito è 28 672.

Questo parametro viene sovrascritto dalla dimensione di blocco della classe di dati SMS (storage management subsystem), se fornita.

Se il dataset del log di archiviazione viene scritto in DASD, si consiglia di scegliere la dimensione massima del blocco che consente due blocchi per ogni traccia. Ad esempio, per un dispositivo 3390, è necessario utilizzare una dimensione blocco di 24 576.

Se il dataset del log di archivio viene scritto su nastro, la specifica della dimensione di blocco più grande possibile migliora la velocità di lettura del log di archivio. È necessario utilizzare una dimensione blocco di 28 672.

Impostazioni suggerite:

Sistema di test	Utilizzare il suggerimento per la dimensione del blocco in base al supporto utilizzato per i log di archiviazione. Vale a dire, per il disco 24 576 e il nastro 28 672.
Sistema di produzione	Utilizzare il suggerimento per la dimensione del blocco in base al supporto utilizzato per i log di archiviazione. Vale a dire, per il disco 24 576 e il nastro 28 672.

CATALOG
Specifica se i dataset di log di archivio vengono catalogati nel catalogo ICF (Integrated Catalog Facility) primario.

Specificare:

No
I dataset di log di archiviazione non vengono catalogati

SÌ
I dataset di log di archivio sono catalogati

Il valore predefinito è NO.

Tutti i dataset del log di archivio assegnati su DASD devono essere catalogati. Se si archivia su DASD con il parametro CATALOG impostato su NO, viene visualizzato il messaggio CSQJ072E ogni volta che viene assegnato un dataset di log di archivio e IBM MQ cataloga il dataset.

Impostazioni suggerite:

Sistema di test	SÌ
Sistema di produzione	SI, quando gli archivi sono assegnati su DASD

COMPACT
Specifica se i dati scritti nei log di archivio devono essere compattati. Questa opzione si applica solo a un dispositivo 3480 o 3490 che ha la funzione IDRC (improved data recording capability). Quando questa funzione è attivata, l'hardware dell'unità di controllo nastro scrive i dati con una densità maggiore di quella normale, consentendo una quantità maggiori di dati su ogni volume. Specificare NO

se non si utilizza una periferica 3480 con la funzione IDRC o un modello di base 3490, ad eccezione di 3490E. Specificare YES se si desidera che i dati vengano compressi.

Specificare:

No
Non comprimere i dataset

SÌ
Comprimere i dataset

Il valore predefinito è NO.

La specifica di YES influisce negativamente sulle prestazioni. Inoltre, tenere presente che i dati compressi su nastro possono essere letti solo utilizzando un'unità che supporta la funzione IDRC. Questo può essere un problema se è necessario inviare nastri di archivio a un altro sito per il ripristino remoto.

Impostazioni suggerite:

Sistema di test	Non applicabile
Sistema di produzione	No (predefinito) Si applica solo alla compressione 3480 e 3490 IDR. L'impostazione su YES potrebbe compromettere le prestazioni di lettura del log di archiviazione durante il recupero e il riavvio; tuttavia, non influisce sulla scrittura su nastro.

PRIQTY
Specifica l'allocazione dello spazio primario per i dataset DASD in ALCUNITs.

Il valore deve essere maggiore di zero.

Il valore predefinito è 25 715.

Questo valore deve essere sufficiente per una copia del dataset di log o del BSDS corrispondente, a seconda di quale sia il più grande. Per determinare il valore necessario, attenersi alla seguente procedura:

1. Determinare il numero di record di log attivi assegnati (c) come descritto in “Creare i dataset bootstrap e log” a pagina 845.
2. Determinare il numero di blocchi di 4096 byte in ciascun blocco di log archivio:

```
d = BLKSIZE / 4096
```

   dove BLKSIZE è il valore arrotondato.
3. Se ALCUNIT = BLK:

```
PRIQTY = INT(c / d) + 1
```

   dove INT indica l'arrotondamento a un numero intero.

   Se ALCUNIT = TRK:

```
PRIQTY = INT(c / (d * INT(e/BLKSIZE))) + 1
```

dove e è il numero di byte per ciascuna traccia (56664 per una periferica 3390) e INT indica l'arrotondamento a un numero intero.

Se ALCUNIT = CYL:

```
PRIQTY = INT(c / (d * INT(e/BLKSIZE) * f)) + 1
```

dove f è il numero di tracce per ogni cilindro (15 per un dispositivo 3390) e INT significa arrotondato a un numero intero.

Per informazioni sulla dimensione dei dataset di log e archivio, consultare "Creare i dataset bootstrap e log" a pagina 845 e "Definisci le serie di pagine" a pagina 846.

Impostazioni suggerite:

Sistema di test 1 680

Sufficiente per conservare l'intero log attivo, ovvero:

```
10  080 / 6 = 1  680 blocks
```

Sistema di produzione Non applicabile durante l'archiviazione su nastro.

Se è probabile che lo spazio libero sui volumi DASD di archivio sia frammentato, si consiglia di specificare un'estensione primaria più piccola e consentire l'espansione in estensioni secondarie. Per ulteriori informazioni sull'allocazione dello spazio per i log attivi, fare riferimento a Pianificazione su z/OS.

PROTECT
Specifica se i dataset di log di archivio devono essere protetti da profili ESM (External Security Manager) discreti al momento della creazione dei dataset.

Specificare:

No
I profili non vengono creati.

SÌ
I profili di dataset discreti vengono creati quando i log vengono scaricati. Se si specifica YES:

- La protezione ESM deve essere attiva per IBM MQ.
- L'ID utente associato allo spazio di indirizzo del gestore code IBM MQ deve avere l'autorità per creare questi profili.
- La classe TAPEVOL deve essere attiva se si sta archiviando su nastro.

Altrimenti, lo scaricamento non riesce.

Il valore predefinito è NO.

QUIESCE
Specifica il tempo massimo in secondi consentito per la sospensione quando viene emesso un comando ARCHIVE LOG con MODE (QUIESCE) specificato.

Il parametro deve essere compreso tra 1 e 999.

Il valore predefinito è 5.

SECQTY
Specifica l'allocazione dello spazio secondario per i dataset DASD in ALCUNITs. L'estensione secondaria può essere assegnata fino a 15 volte; consultare *z/OS MVS JCL Reference* e *z/OS MVS JCL User's Guide* per i dettagli.

Il parametro deve essere maggiore di zero.

Il valore predefinito è 540.

TSTAMP
Specifica se il nome del dataset di log di archivio contiene una data/ora.

Specificare:

No
I nomi non includono una data / ora. I dataset di log di archiviazione sono denominati:

```
arcpfxi.A nnnnnnn
```

Dove *arcpfxi* è il prefisso del nome del dataset specificato da ARCPFX1 o ARCPFX2. *arcpfxi* può contenere un massimo di 35 caratteri.

SÌ
I nomi includono una data/ora. I dataset di log di archiviazione sono denominati:

```
arcpfxi.cyyddd.T hhmmsst.A nnnnnnn
```

dove *c* è 'D' per gli anni fino al 1999 incluso o ' E'per l'anno 2000 e successivo e *arcpfxi* è il prefisso del nome del data set specificato da ARCPFX1 o ARCPFX2. *arcpfxi* può contenere fino a 19 caratteri.

EST
I nomi includono una data/ora. I dataset di log di archiviazione sono denominati:

```
arcpfxi.D yyyyddd.T hhmmsst.A nnnnnnn
```

Dove *arcpfxi* è il prefisso del nome del dataset specificato da ARCPFX1 o ARCPFX2. *arcpfxi* può avere un massimo di 17 caratteri.

Il valore predefinito è NO.

UNIT
Specifica il tipo di periferica o il nome unità della periferica utilizzata per memorizzare la prima copia del dataset del log di archivio.

Specificare un tipo di unità o un nome unità da 1 a 8 caratteri alfanumerici. Il primo carattere deve essere un carattere alfabetico.

Questo parametro non può essere vuoto.

Il valore predefinito è TAPE.

Se si archivia in DASD, è possibile specificare un tipo di unità generico con un intervallo di volumi limitato, ad esempio UNIT=3390.

Se si archivia su DASD, assicurarsi che:

- L'allocazione dello spazio primario è abbastanza grande da contenere tutti i dati dai dataset del log attivo.
- L'opzione del catalogo del dataset di log di archivio (CATALOG) è impostata su YES.
- È stato utilizzato un valore appropriato per BLKSIZE.

Se si archivia su TAPE, IBM MQ può estendersi fino a un massimo di 20 volumi.

Impostazioni suggerite:

Sistema di test	DASD
Sistema di produzione	Nastro

Per ulteriori informazioni sulla scelta di un'ubicazione per i log di archiviazione, fare riferimento a Pianificazione su z/OS.

UNIT2
Specifica il tipo di periferica o il nome unità dell'unità utilizzata per memorizzare la seconda copia dei dataset del log di archivio.

Specificare un tipo di unità o un nome unità da 1 a 8 caratteri alfanumerici. Il primo carattere deve essere un carattere alfabetico. Se questo parametro è vuoto, viene utilizzato il valore impostato per il parametro UNIT.

Il valore predefinito è vuoto.

Riferimenti correlati

"Utilizzo di CSQ6SYSP" a pagina 849
Utilizzare questo argomento come riferimento per l'impostazione dei parametri di sistema utilizzando CSQ6SYSP.

"Utilizzo di CSQ6LOGP" a pagina 858
Utilizzare questo argomento come riferimento per la specifica delle opzioni di registrazione utilizzando CSQ6LOGP.

z/OS V 9.1.0 *Utilizzo di CSQ6USGP*
Utilizzare questo argomento come riferimento per impostare i propri parametri di sistema utilizzando CSQ6USGP

Utilizzare CSQ6USGP per controllare la registrazione dell'utilizzo del prodotto.

I parametri predefiniti per CSQ6USGP sono riportati in Tabella 62 a pagina 870. Se è necessario modificare uno qualsiasi di questi valori, fare riferimento alle descrizioni dettagliate dei parametri.

Attenzione: Non è possibile modificare nessuno di questi parametri utilizzando il comando SET SYSTEM.

Tabella 62. Valori predefiniti dei parametri CSQ6USGP

Parametro	Descrizione	Valore predefinito
QMGRPROD	Prodotto rispetto al quale deve essere registrato l'utilizzo del gestore code	Spazio
AMSPROD	Prodotto rispetto al quale deve essere registrato l'utilizzo di Advanced Message Security (AMS)	Spazio

PROD QMGR
Specifica il prodotto rispetto al quale deve essere registrato l'utilizzo del gestore code.

Specificare uno tra:

MQ
L'utilizzo del gestore code viene registrato come prodotto IBM MQ for z/OS autonomo, con ID prodotto 5655-MQ9.

VUE
L'utilizzo del gestore code viene registrato come prodotto IBM MQ for z/OS Value Unit Edition (VUE) autonomo, con ID prodotto 5655-VU9.

AVANZATOVUE
L'utilizzo del gestore code viene registrato come parte di un prodotto IBM MQ Advanced for z/OS Value Unit Edition con ID prodotto 5655-AV1.

PROD SMS
V 9.1.3 Se questo parametro non è impostato, lo spazio di indirizzo AMS non verrà avviato e verrà emesso il messaggio CSQY024I .

Specifica il prodotto rispetto al quale deve essere registrato l'utilizzo di Advanced Message Security , se utilizzato.

Specificare uno tra:

AMS
L'utilizzo di AMS viene registrato come un prodotto Advanced Message Security for z/OS autonomo, con ID prodotto 5655-AM9.

AVANZATE
L'utilizzo AMS viene registrato come parte di un prodotto IBM MQ Advanced for z/OS , con ID prodotto 5655-AV9.

AVANZATOVUE
L'utilizzo AMS viene registrato come parte di un prodotto IBM MQ Advanced for z/OS Value Unit Edition , con ID prodotto 5655-AV1.

Consultare Informazioni sul prodotto di report per ulteriori informazioni sulla registrazione dell'utilizzo del prodotto.

Riferimenti correlati

"Utilizzo di CSQ6SYSP" a pagina 849
Utilizzare questo argomento come riferimento per l'impostazione dei parametri di sistema utilizzando CSQ6SYSP.

"Utilizzo di CSQ6LOGP" a pagina 858
Utilizzare questo argomento come riferimento per la specifica delle opzioni di registrazione utilizzando CSQ6LOGP.

z/OS *Adattare i parametri dell'iniziatore di canali*

Utilizzare ALTER QMGR per personalizzare l'iniziatore di canali in base ai propri requisiti.

- *Ripetere questa attività per ogni gestore code IBM MQ , come richiesto.*
- *È necessario eseguire questa attività durante la migrazione da una versione precedente.*

Diversi attributi del gestore code controllano il funzionamento dell'accodamento distribuito. Impostare questi attributi utilizzando il comando MQSC ALTER QMGR. L'esempio dataset di inizializzazione thlqual.SCSQPROC(CSQ4INYG) contiene alcune impostazioni che è possibile personalizzare. Per ulteriori informazioni, consultare ALTER QMGR.

I valori di questi parametri vengono visualizzati come una serie di messaggi ogni volta che si avvia l'iniziatore di canali.

La relazione tra adattatori, dispatcher e numero massimo di canali

I parametri ALTER QMGR CHIADAPS e CHIDISPS definiscono il numero di TCB (task control block) utilizzati dall'iniziatore del canale. I TCB CHIADAPS (adattatore) vengono utilizzati per effettuare chiamate API IBM MQ sul gestore code. I TCB CHIDISPS (dispatcher) vengono utilizzati per effettuare chiamate alla rete di comunicazione.

Il parametro ALTER QMGR MAXCHL influenza la distribuzione dei canali sui TCB del dispatcher.

CHIDISPS

Se si dispone di un numero ridotto di canali, utilizzare il valore predefinito.

Un'attività per ogni processore ottimizza le prestazioni del sistema. Poiché le attività del dispatcher richiedono molta CPU, il principio è quello di mantenere il minor numero possibile di attività, in modo che il tempo impiegato per trovare e avviare i thread sia ridotto al minimo.

CHIDISPS (20) è adatto per sistemi con più di 100 canali. È improbabile che vi sia uno svantaggio significativo nell'avere CHIDISPS (20) quando si tratta di un numero di TCB del dispatcher superiore al necessario.

Come linea guida, se si dispone di più di 1000 canali, consentire un dispatcher per ogni 50 canali correnti. Ad esempio, specificare CHIDISPS (40) per gestire fino a 2000 canali attivi.

Se si sta utilizzando TCP/IP, il numero massimo di dispatcher utilizzati per i canali TCP/IP è 100, anche se si specifica un valore maggiore in CHIDISPS.

CHIADAPS

Ogni chiamata API IBM MQ al gestore code è indipendente da qualsiasi altra chiamata e può essere effettuata su qualsiasi TCB dell'adattatore. Le chiamate che utilizzano messaggi persistenti possono impiegare molto più tempo di quelle per i messaggi non persistenti a causa dell'I/O del log. Pertanto, un iniziatore di canali che elabora un numero elevato di messaggi persistenti su molti canali potrebbe richiedere più dei TCB dell'adattatore predefinito 8 per prestazioni ottimali. Ciò è particolarmente vero quando la dimensione batch raggiunta è piccola, poiché la fine dell'elaborazione batch richiede anche I/O di log e dove vengono utilizzati i canali thin client.

Il valore consigliato per un ambiente di produzione è CHIADAPS (30). È improbabile che l'utilizzo di più di questo possa fornire un vantaggio supplementare significativo e non è probabile che vi sia uno svantaggio significativo nell'avere CHIADAPS (30) se si tratta di più TCB dell'adattatore del necessario.

MAXCHL

Ogni canale è associato a un particolare TCB del dispatcher all'avvio del canale e rimane associato a tale TCB fino a quando il canale non viene arrestato. Molti canali possono condividere ogni TCB. MAXCHL viene utilizzato per diffondere i canali tra i TCB dispatcher disponibili. Il primo (MIN ((MAXCHL / CHIDISPS)) , 10)) i canali da avviare sono associati al primo TCB del dispatcher e così via, fino a quando tutti i TCB del dispatcher sono in uso.

L'effetto di questo per un numero ridotto di canali e un MAXCHL di grandi dimensioni è che i canali NON sono distribuiti in modo uniforme tra i dispatcher. Ad esempio, se si imposta CHIDISPS (10) e si lascia MAXCHL al valore predefinito di 200 ma si hanno solo 50 canali, cinque dispatcher saranno associati a 10 canali ciascuno e cinque non saranno utilizzati. Si consiglia di impostare MAXCHL sul numero di canali effettivamente da utilizzare quando si tratta di un piccolo numero fisso.

Se si modifica questa proprietà del gestore code, è necessario rivedere anche le proprietà del gestore code ACTCHL, LU62CHLe TCPCHL per assicurarsi che i valori siano compatibili. Per una descrizione completa di queste proprietà e della loro relazione, consultare Parametri del gestore code .

Impostazione dell'ambiente dei servizi di sistema z/OS UNIX per gli iniziatori di canali

L'iniziatore di canali (CHINIT) utilizza thread OMVS. Esaminare i parametri di configurazione OMVS prima di creare un nuovo CHINIT o modificare il numero di dispatcher o SSLTASKS.

Ogni CHINIT utilizza 3 thread + CHIDISP + SSLTASKS OMVS. Contribuiscono al numero totale di thread OMVS utilizzati nella LPAR e al numero di thread utilizzati dall'ID utente dell'attività avviata CHINIT.

È possibile utilizzare il **D OMVS,L** ed esaminare l'utilizzo corrente, l'utilizzo delle risorse idriche e il limite di sistema di MAXPROCSYS (il numero massimo di processi consentito dal sistema).

Se si sta aggiungendo un nuovo CHINIT o si stanno aumentando i valori di CHIDISPS o SSLTASKS, è necessario calcolare l'aumento dei thread ed esaminare l'impatto sui valori MAXPROCSYS. È possibile utilizzare il comando **SETOMVS** per modificare in modo dinamico MAXPROCSYS o aggiornare il valore parmlib BPXPRCxx o entrambi.

Il parametro OMVS MAXPROCUSER è il numero di thread OMVS che un singolo utente OMVS, con lo stesso UID, può avere. I thread vengono conteggiati per questo valore. Quindi, se si dispone di 2 CHINITS con lo stesso ID utente dell'attività avviata, con 10 dispatcher e 3 SSLTASKS ciascuno, ci sono 2 * (3 +10 + 3) = 32 thread per l'uid OMVS.

È possibile visualizzare il valore predefinito MAXPROCUSER emettendo il comando **D OMVS,O** ed è possibile utilizzare il comando **SETOMVS** per modificare dinamicamente MAXPROCUSER o aggiornare il valore parmlib BPXPRCxx o entrambi.

È possibile sovrascrivere questo valore in base all'utente con il comando RACF **ALTUSER userid OMVS(PROCUSERMAX(nnnn))** o equivalente.

Per avviare l'iniziatore di canali, immettere il seguente comando:

```
START CHINIT
```

Per assicurarsi che l'iniziatore del canale sia stato avviato correttamente, verificare che non vi sia alcun errore ICH408I nel log del lavoro xxxxCHIN(ssidCHIN).

Concetti correlati

"Impostazione di adattatori Batch, TSO e RRS" a pagina 873
Rendere gli adattatori disponibili per le applicazioni aggiungendo le librerie alle concatenazioni STEPLIB appropriate. Per soddisfare i dump SNAP emessi da un adattatore, assegnare un DDname CSQSNAP. Considerare l'utilizzo di CSQBDEFV per migliorare la portabilità dei programmi applicativi

Record di dati delle statistiche dell'iniziatore di canale

z/OS *Impostazione di adattatori Batch, TSO e RRS*

Rendere gli adattatori disponibili per le applicazioni aggiungendo le librerie alle concatenazioni STEPLIB appropriate. Per soddisfare i dump SNAP emessi da un adattatore, assegnare un DDname CSQSNAP. Considerare l'utilizzo di CSQBDEFV per migliorare la portabilità dei programmi applicativi

- *Ripetere questa attività per ogni gestore code IBM MQ come richiesto.*
- *Potrebbe essere necessario eseguire questa attività durante la migrazione da una versione precedente.*

Per rendere gli adattatori disponibili per batch e altre applicazioni utilizzando connessioni batch, aggiungere le seguenti librerie IBM MQ alla concatenazione STEPLIB per l'applicazione batch:

- thlqual.SCSQANL *x*
- thlqual.SCSQAUTH

dove *x* è la lettera della lingua per la propria lingua nazionale. (Non è necessario eseguire questa operazione se le librerie si trovano nell'area LPA o nell'elenco dei collegamenti.)

Per le applicazioni TSO, aggiungere le librerie alla concatenazione STEPLIB nella procedura di collegamento TSO oppure attivarle utilizzando il comando TSO TSOLIB.

Se l'adattatore rileva un errore IBM MQ imprevisto, emette un z/OS dump SNAP per DDname CSQSNAP ed emette il codice di errore MQRC_UNEXPECTED_ERROR per l'applicazione.Se l'istruzione CSQSNAP DD non si trova nel JCL dell'applicazione o CSQSNAP non è assegnata a un dataset in TSO, non viene eseguito alcun dump. Se ciò si verifica, è possibile includere l'istruzione CSQSNAP DD nel JCL dell'applicazione o assegnare CSQSNAP a un dataset in TSO ed eseguire nuovamente l'applicazione. Tuttavia, poiché alcuni problemi sono intermittenti, si consiglia di includere un'istruzione CSQSNAP nel JCL dell'applicazione o di assegnare CSQSNAP a un dataset nella procedura di accesso TSO per catturare il motivo dell'errore nel momento in cui si verifica.

Il programma fornito CSQBDEFV migliora la portabilità dei programmi applicativi. In CSQBDEFV, è possibile specificare il nome di un gestore code o di un gruppo di condivisione code a cui connettersi invece di specificarlo nella chiamata MQCONN o MQCONNX in un programma applicativo. È possibile creare una nuova versione di CSQBDEFV per ciascun gestore code o gruppo di condivisione code. Per effettuare questa operazione, attenersi a quanto segue:

1. Copiare il programma assembler IBM MQ CSQBDEFV da thlqual.SCSQASMS in una libreria utente.
2. Il programma fornito contiene il nome del sottosistema predefinito CSQ1. È possibile conservare questo nome per il test e la verifica dell'installazione. Per i sottosistemi di produzione, è possibile modificare NAME=CSQ1 con il nome del sottosistema da uno a quattro caratteri oppure utilizzare CSQ1.

   Se si utilizzano i gruppi di condivisione code, è possibile specificare un nome gruppo di condivisione code invece di CSQ1. In questo caso, il programma invia una richiesta di connessione a un gestore code attivo all'interno di tale gruppo.

3. Assemblare e modificare il programma per produrre il modulo di caricamento CSQBDEFV. Per l'assemblaggio, inserire la libreria thlqual.SCSQMACS nella concatenazione SYSLIB; utilizzare i parametri di modifica del link `RENT,AMODE=31,RMODE=ANY`. Ciò viene mostrato nel JCL di esempio in thlqual.SCSQPROC(CSQ4DEFV). Quindi includere la libreria di caricamento in z/OS Batch o TSO STEPLIB, prima di thlqual.SCSQAUTH.

Concetti correlati

"Impostare le operazioni e i pannelli di controllo" a pagina 874
Per impostare le operazioni e i pannelli di controllo, è necessario prima impostare le librerie che contengono i pannelli, gli EXEC, i messaggi e le tabelle richiesti. Per fare ciò, è necessario considerare quale caratteristica della lingua nazionale deve essere utilizzata per i pannelli. Una volta eseguita questa operazione, è possibile aggiornare il menu ISPF principale per le IBM MQ operazioni e i pannelli di controllo e modificare le impostazioni dei tasti funzionali.

z/OS *Impostare le operazioni e i pannelli di controllo*

Per impostare le operazioni e i pannelli di controllo, è necessario prima impostare le librerie che contengono i pannelli, gli EXEC, i messaggi e le tabelle richiesti. Per fare ciò, è necessario considerare quale caratteristica della lingua nazionale deve essere utilizzata per i pannelli. Una volta eseguita questa operazione, è possibile aggiornare il menu ISPF principale per le IBM MQ operazioni e i pannelli di controllo e modificare le impostazioni dei tasti funzionali.

- *È necessario eseguire questa attività una volta per ogni sistema z/OS in cui si desidera eseguire IBM MQ.*
- *Potrebbe essere necessario eseguire questa attività durante la migrazione da una versione precedente.*

Impostazione delle librerie

Attenersi alla seguente procedura per impostare le operazioni e i pannelli di controllo IBM MQ :

1. Assicurarsi che tutte le librerie contenute nelle concatenazioni siano nello stesso formato (F, FB, V, VB) e abbiano la stessa dimensione di blocco o siano in ordine decrescente di dimensioni di blocco. Altrimenti, potrebbero verificarsi dei problemi durante il tentativo di utilizzare questi pannelli.
2. Includere la libreria thlqual.SCSQEXEC nella concatenazione SYSEXEC o SYSPROC oppure attivarla utilizzando il comando TSO ALTLIB. Questa libreria, assegnata con un formato record 80 a blocco fisso durante l'installazione, contiene gli EXEC richiesti.

   È preferibile inserire la libreria nella concatenazione SYSEXEC. Tuttavia, se si desidera inserirlo in SYSPROC, la libreria deve avere una lunghezza record di 80 byte.
3. Aggiungere thlqual.SCSQAUTH e thlqual.SCSQANLx alla procedura di accesso TSO STEPLIB oppure attivarla utilizzando il comando TSO TSOLIB, se non si trova nell'elenco di link o nell'LPA.
4. È possibile aggiungere le librerie del pannello IBM MQ in modo permanente all'impostazione della propria libreria ISPF oppure consentirne l'impostazione dinamica quando vengono utilizzati i pannelli. Per la scelta precedente, è necessario effettuare le seguenti operazioni:
   a. Includere la libreria contenente le operazioni e le definizioni del pannello di controllo nella concatenazione ISPPLIB. Il nome è thlqual.SCSQPNLx, dove x è la lettera della lingua per la propria lingua nazionale.
   b. Includere la libreria che contiene le tabelle richieste nella concatenazione ISPTLIB. Il nome è thlqual.SCSQTBLx, dove x è la lettera della lingua per la tua lingua nazionale.
   c. Includere la libreria contenente i messaggi richiesti nella concatenazione ISPMLIB. Il nome è thlqual.SCSQMSGx, dove x è la lettera della lingua per la propria lingua nazionale.
   d. Includere la libreria contenente i moduli di caricamento richiesti nella concatenazione ISPLLIB. Il nome di questa libreria è thlqual.SCSQAUTH.
5. Verificare che sia possibile accedere ai pannelli IBM MQ dal pannello del processore comandi TSO. Questa è di solito l'opzione 6 nel menu Opzioni primarie ISPF/PDF. Il nome dell'EXEC eseguito è

CSQOREXX.Non esistono parametri da specificare se le librerie IBM MQ sono state inserite in modo permanente nella configurazione ISPF come nel passo 4. In caso contrario, utilizzare quanto segue:

```
CSQOREXX thlqual langletter
```

dove `langletter` è una lettera che identifica la lingua nazionale da utilizzare:

C
Cinese semplificato

E
U.S. Inglese (maiuscolo / minuscolo)

F
Franco francese

K
Giapponese

U
U.S. Inglese (maiuscolo)

Aggiornamento del menu ISPF

È possibile aggiornare il menu principale ISPF per consentire l'accesso alle operazioni IBM MQ e ai pannelli di controllo da ISPF. L'impostazione richiesta per & ZSEL è:

```
CMD(%CSQOREXX thlqual langletter)
```

Per informazioni su `thlqual` e `langletter`, consultare il passo “5” a pagina 874.

Per ulteriori dettagli, consultare il manuale *z/OS: ISPF Dialog Developer's Guide and Reference* .

Aggiornamento dei tasti funzione e delle impostazioni dei comandi

È possibile utilizzare le normali procedure ISPF per la modifica dei tasti funzionali e delle impostazioni dei comandi utilizzati dai pannelli. L'identificativo dell'applicazione è CSQO.

Tuttavia, ciò non è consigliato poiché le informazioni della guida non vengono aggiornate per riflettere le modifiche apportate.

Concetti correlati

“Includi il membro di formattazione del dump IBM MQ” a pagina 875
Per poter formattare i dump IBM MQ utilizzando IPCS (Interactive Problem Control System), è necessario aggiornare alcune librerie di sistema.

z/OS *Includi il membro di formattazione del dump IBM MQ*

Per poter formattare i dump IBM MQ utilizzando IPCS (Interactive Problem Control System), è necessario aggiornare alcune librerie di sistema.

- *È necessario eseguire questa attività una volta per ogni sistema z/OS in cui si desidera eseguire IBM MQ.*
- *È necessario eseguire questa attività quando si esegue la migrazione da una versione precedente.*

Per poter formattare i dump IBM MQ utilizzando IPCS (Interactive Problem Control System), copia il dataset thlqual.SCSQPROC(CSQ7IPCS) in SYS1.PARMLIB. Non è necessario modificare questo dataset.

Se è stata personalizzata la procedura TSO per IPCS, è possibile copiare thlqual.SCSQPROC(CSQ7IPCS) in qualsiasi libreria nella definizione IPCSPARM. Consultare il manuale *z/OS MVS IPCS Customization* per i dettagli su IPCSPARM.

È necessario inoltre includere la libreria thlqual.SCSQPNLA nella concatenazione ISPPLIB.

Per rendere disponibili i programmi di formattazione del dump per la sessione TSO o il lavoro IPCS, è necessario includere anche la libreria thlqual.SCSQAUTH nella concatenazione STEPLIB o attivarla utilizzando il comando TSO TSOLIB (anche se è già presente nell'elenco di collegamenti o LPA).

Concetti correlati

"Elimina messaggi informativi" a pagina 876
Il sistema IBM MQ potrebbe produrre un numero elevato di messaggi informativi. È possibile impedire che i messaggi selezionati vengano inviati alla console o al log della copia cartacea.

z/OS *Elimina messaggi informativi*

Il sistema IBM MQ potrebbe produrre un numero elevato di messaggi informativi. È possibile impedire che i messaggi selezionati vengano inviati alla console o al log della copia cartacea.

- *È necessario eseguire questa attività una volta per ogni sistema z/OS in cui si desidera eseguire IBM MQ.*
- *Non è necessario eseguire questa attività quando si esegue la migrazione da una versione precedente.*

Se il sistema IBM MQ è molto 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 della copia cartacea. Il bridge IBM MQ - IMS e il gestore buffer potrebbero anche produrre un numero elevato di messaggi informativi.

Se necessario, è possibile eliminare alcuni di questi messaggi della console utilizzando l'elenco di funzioni di elaborazione dei messaggi z/OS , specificato dai membri MPFLSTxx di SYS1.PARMLIB. I messaggi specificati vengono ancora visualizzati nella registrazione cartacea, ma non nella console.

L'esempio thlqual.SCSQPROC(CSQ4MPFL) mostra impostazioni consigliate per MPFLSTxx. Per ulteriori informazioni su MPFLSTxx, consultare il manuale *z/OS MVS Initialization and Tuning Reference* .

Se si desidera eliminare i messaggi informativi selezionati sul log cartaceo, è possibile utilizzare l'uscita di installazione di z/OS IEAVMXIT. È possibile impostare i seguenti bit switch su ON per i messaggi richiesti:

CTXTRDTM
Eliminare il messaggio.

Il messaggio non viene visualizzato sulle console o registrato in formato cartaceo.

CTXTESJL
Elimina dalla registrazione lavoro.

Il messaggio non va nella registrazione lavoro JES.

CTXTNWTP
Non eseguire l'elaborazione WTP.

Il messaggio non viene inviato a un terminale TSO o al dataset del messaggio di sistema di un lavoro batch.

Nota:

1. Per dettagli completi sugli altri parametri, consultare la documentazione Uscite di installazione MVS .
2. Si consiglia di non eliminare i messaggi diversi da quelli nell'elenco di soppressioni suggerito, CSQ4MPFL.

Inoltre, è possibile specificare il parametro aggiuntivo:

EXCLMSG
Specifica un elenco di messaggi da escludere da qualsiasi registrazione.

I messaggi in questo elenco non vengono inviati alla console z/OS e al log della copia cartacea. Per ulteriori informazioni, consultare EXCLMSG in "Utilizzo di CSQ6SYSP" a pagina 849 .

Attività correlate

"Test di un gestore code su z/OS" a pagina 892

Una volta personalizzato o migrato il gestore code, è possibile verificarlo eseguendo i programmi di verifica dell'installazione e alcune delle applicazioni di esempio fornite con IBM MQ for z/OS.

z/OS Configurazione del gruppo di condivisione code

Se si desidera utilizzare le code condivise per l'alta disponibilità, utilizzare questi argomenti come guida dettagliata per la configurazione del gruppo di condivisione code.

Una volta completati i passi in questa parte del processo per l'impostazione del sistema IBM MQ for z/OS , è necessario “Personalizzare il modulo dei parametri di sistema” a pagina 847 aggiungere i dati del gruppo di condivisione code. È necessario modificare CSQ6SYSP per specificare il parametro QSGDATA.

z/OS *Impostazione dell'ambiente Db2*

Se si utilizzano gruppi di condivisione code, è necessario creare gli oggetti Db2 richiesti personalizzando ed eseguendo un numero di lavori di esempio.

Impostazione dell'ambiente Db2

È necessario creare e collegare gli oggetti Db2 richiesti personalizzando ed eseguendo un numero di lavori di esempio.

- Ripetere questa attività per ciascun gruppo di condivisione dati Db2 .
- È necessario eseguire la procedura `bind` e `grant` quando si migra da una versione precedente.
- Omettere questa attività se non si utilizzano i gruppi di condivisione code.

  Se in seguito si desidera utilizzare i gruppi di condivisione code, eseguire questa attività in quel momento.

IBM MQ fornisce due serie equivalenti di lavori. Quelli con il prefisso CSQ45 sono per la compatibilità con le precedenti versioni di IBM MQ e per l'utilizzo con Db2 versione 11 e precedenti. Se si sta configurando un nuovo gruppo di condivisione dati con Db2 V12 o versioni successive, si consiglia di utilizzare i lavori con il prefisso CSQ4X , poiché questi lavori utilizzano le funzionalità Db2 più recenti per il dimensionamento dinamico e gli UTS (Universal Table Spaces)

È necessario stabilire un ambiente in cui IBM MQ possa accedere ed eseguire i piani Db2 utilizzati per i gruppi di condivisione code.

I seguenti passi devono essere eseguiti per ogni nuovo gruppo di condivisione dati Db2 . Tutti i JCL di esempio sono in thlqual.SCSQPROC.

1. Personalizzare ed eseguire il JCL di esempio CSQ45CSG V 9.1.0 (o CSQ4XCSG) per creare il gruppo di memoria da utilizzare per il database, gli spazi tabella e le tabelle IBM MQ .
2. Personalizzare ed eseguire il JCL di esempio CSQ45CDB V 9.1.0 (o CSQ4XCDB) per creare il database che deve essere utilizzato da tutti i gestori code che si collegano a questo gruppo di condivisione dati Db2 .
3. Personalizzare ed eseguire il JCL di esempio CSQ45CTS V 9.1.0 (o CSQ4XCTS) per creare gli spazi tabella che contengono le tabelle del gestore code e dell'iniziatore di canali utilizzate per i gruppi di condivisione code (da creare nel passo 1).
4. Personalizzare ed eseguire il JCL di esempio CSQ45CTB V 9.1.0 (o CSQ4XCTB) per creare le 12 tabelle Db2 e gli indici associati. Non modificare i nomi delle righe o gli attributi.
5. Personalizzare ed eseguire il JCL di esempio CSQ45BPL per collegare i piani Db2 per il gestore code, i programmi di utilità e l'iniziatore di canali.
6. Personalizzare ed eseguire il JCL di esempio CSQ45GEX per concedere l'autorizzazione di esecuzione ai piani per gli ID utente utilizzati dal gestore code, dai programmi di utilità e dall'iniziatore di canale. Gli ID utente per il gestore code e l'iniziatore di canali sono gli ID utente con cui vengono eseguite le procedure dell'attività avviata. Gli ID utente per i programmi di utilità sono gli ID utente con cui è possibile inoltrare i lavori batch.

I nomi dei piani appropriati sono mostrati nella seguente tabella per:

- LTS Long Term Support nella colonna LTS .
- CD Continuous Delivery nella colonna CD , dove n rappresenta la release CD .

  Ad ogni rilascio, n aumenta di uno. Ad esempio, in IBM MQ 9.0.3, CSQ5A90n è CSQ5A903.

Utente	Piani (LTS)	Piani (CD)
Gestore code	CSQ5A 910, CSQ5C 910, CSQ5D 910, CSQ5K 910, CSQ5L 910, CSQ5M 910, CSQ5P 910, CSQ5R 910, CSQ5S 910, CSQ5T 910, CSQ5U 910, CSQ5W 910	CSQ5A 91n, CSQ5C 91n, CSQ5D 91n, CSQ5K 91n, CSQ5L 91n, CSQ5M 91n, CSQ5P 91n, CSQ5R 91n, CSQ5S 91n, CSQ5T 91n, CSQ5U 91n, CSQ5W 91n
funzione SDEFS del programma di utilità batch CSQUTIL	CSQ52 910	CSQ52 91n
CSQ5PQSG e CSQJUCNV	CSQ5B 910	CSQ5B 91n
Programma di utilità del servizio CSQUZAP	CSQ5Z 910	CSQ5Z 91n

In caso di errore durante l'installazione di Db2 , è possibile personalizzare ed eseguire i seguenti lavori:

- CSQ45DTB per eliminare le tabelle e gli indici.
- CSQ45DTS V 9.1.0 (o CSQ4XDTS) per eliminare i tablespace.
- CSQ45DDB V 9.1.0 (o CSQ4XDDB) per eliminare il database.
- CSQ45DSG V 9.1.0 (o CSQ4XDSG) per eliminare il gruppo di memoria.

Nota: Se questi lavori hanno esito negativo a causa di un problema di blocco Db2 , probabilmente è dovuto al conflitto per una risorsa Db2 , soprattutto se il sistema è utilizzato in modo intensivo. Inoltrare nuovamente i lavori successivamente. È preferibile eseguire questi lavori quando il sistema è leggermente utilizzato o disattivato.

Consultare Db2 in *Db2 per z/OS 11.0.0* per ulteriori informazioni sull'impostazione di Db2.

Consultare Db2 Administration in *Db2 per z/OS 12.0.0* per ulteriori informazioni sull'impostazione di Db2.

Consultare Pianificazione su z/OS per informazioni sulle dimensioni delle tabelle Db2 .

Concetti correlati

“Impostazione della CF (coupling facility)” a pagina 879
Se si utilizzano i gruppi di condivisione code, definire le strutture CF (Coupling Facility) utilizzate dai gestori code nel gruppo di condivisione code (QSG) nel dataset della politica CFRM (Coupling Facility Resource Management), utilizzando IXCMIAPU.

z/OS *Impostazione della CF (coupling facility)*

Se si utilizzano i gruppi di condivisione code, definire le strutture CF (Coupling Facility) utilizzate dai gestori code nel gruppo di condivisione code (QSG) nel dataset della politica CFRM (Coupling Facility Resource Management), utilizzando IXCMIAPU.

- Ripetere questa attività per ogni gruppo di condivisione code.
- Potrebbe essere necessario eseguire questa attività quando si esegue la migrazione da una versione precedente.
- Omettere questa attività se non si utilizzano i gruppi di condivisione code.

  Se in seguito si desidera utilizzare i gruppi di condivisione code, eseguire questa attività in quel momento.

Tutte le strutture per il gruppo di condivisione code iniziano con il nome del gruppo di condivisione code. Definire le seguenti strutture:

- Una struttura amministrativa denominata *qsg - name* CSQ_ADMIN. Questa struttura è utilizzata dallo stesso IBM MQ e non contiene dati utente.
- Una struttura dell'applicazione di sistema denominata *qsg - name* CSQSYSAPPL. Questa struttura è utilizzata dalle code di sistema IBM MQ per memorizzare le informazioni sullo stato.
- Una o più strutture utilizzate per conservare i messaggi per le code condivise. Questi possono avere qualsiasi nome che si sceglie fino a 16 caratteri di lunghezza.
  - I primi quattro caratteri devono essere il nome del gruppo di condivisione code. (Se il nome del gruppo di condivisione code è inferiore a quattro caratteri, deve essere riempito con quattro caratteri con i simboli @.)
  - Il quinto carattere deve essere alfabetico e i caratteri successivi possono essere alfabetici o numerici. Questa parte del nome (senza il nome del gruppo di condivisione code) è quella specificata per il nome CFSTRUCT quando si definisce una coda condivisa o un oggetto struttura CF.

  È possibile utilizzare solo caratteri alfabetici e numerici nei nomi delle strutture utilizzate per contenere i messaggi per le code condivise, non è possibile utilizzare altri caratteri (ad esempio, il carattere _, utilizzato nel nome della struttura di gestione).

Le istruzioni di controllo di esempio per IXCMIAPI si trovano nel dataset thlqual.SCSQPROC(CSQ4CFRM). Personalizzare questi e aggiungerli al lavoro IXCMIAPU per la CF (coupling facility) ed eseguirli.

Una volta definite correttamente le strutture, attivare la politica CFRM utilizzata. Per eseguire questa operazione, immettere il seguente comando z/OS :

```
SETXCF START,POLICY,TYPE=CFRM,POLNAME= policy-name
```

Per informazioni sulla pianificazione delle strutture CF e le relative dimensioni, consultare Definizione delle risorse CF (coupling facility).

Concetti correlati

“Implementare i controlli di sicurezza ESM” a pagina 841
Implementare i controlli di sicurezza per gestori code e iniziatore di canali.

z/OS *Impostazione dell'ambiente SMDS*

Se si desidera utilizzare SMDS per scaricare i messaggi sulle code condivise, impostare l'ambiente di storage offload SMDS.

- *Eseguire questa attivit ... per ogni gestore code e struttura nel gruppo di condivisione code che si desidera configurare per scaricare i dati in SMDS.*
- *Se si desidera configurare ulteriori strutture per scaricare i dati su SMDS in un secondo momento, questa attività può essere eseguita nuovamente in quel momento.*

- *Ometti questa attività se non si utilizzano i gruppi di condivisione code.*

  Se successivamente si desidera utilizzare i gruppi di condivisione code, eseguire questa attività in quel momento.

Impostazione dell'ambiente SMDS

1. Stimare la struttura e i requisiti di spazio del dataset. Consultare Considerazioni sulla capacità del dataset del messaggio condiviso.
2. Allocare e preformattare i dataset. Consultare la sezione Creazione di un dataset di messaggi condiviso.
3. Quando si definisce la struttura CF per IBM MQ, assicurarsi di definire CFSTRUCT con CFLEVEL (5) e OFFLOAD (SMDS).

Concetti correlati

“Impostazione della CF (coupling facility)” a pagina 879
Se si utilizzano i gruppi di condivisione code, definire le strutture CF (Coupling Facility) utilizzate dai gestori code nel gruppo di condivisione code (QSG) nel dataset della politica CFRM (Coupling Facility Resource Management), utilizzando IXCMIAPU.

z/OS *Aggiungere le voci IBM MQ alle tabelle Db2*

Se si utilizzano i gruppi di condivisione code, eseguire il programma di utilità CSQ5PQSG per aggiungere le voci del gruppo di condivisione code e del gestore code alle tabelle IBM MQ nel gruppo di condivisione dati Db2 .

- *Ripetere questa attività per ogni gruppo di condivisione code IBM MQ e per ciascun gestore code*
- *Potrebbe essere necessario eseguire questa attività durante la migrazione da una versione precedente.*
- *Ometti questa attività se non si utilizzano i gruppi di condivisione code.*

  Se successivamente si desidera utilizzare i gruppi di condivisione code, eseguire questa attività in quel momento.

Eseguire CSQ5PQSG per ogni gruppo di condivisione code e per ogni gestore code che deve essere membro di un gruppo di condivisione code. (CSQ5PQSG è descritto in Amministrazione di IBM MQ for z/OS.)

Effettuare le seguenti azioni nell'ordine specificato:

1. Aggiungere una voce del gruppo di condivisione code nelle tabelle IBM MQ Db2 utilizzando la funzione ADD QSG del programma CSQ5PQSG . Un esempio viene fornito in thlqual.SCSQPROC(CSQ45AQS).

   Eseguire questa funzione una volta per ogni gruppo di condivisione code definito nel gruppo di condivisione dati Db2 . La voce del gruppo di condivisione code deve esistere prima di aggiungere le voci del gestore code che fanno riferimento al gruppo di condivisione code.
2. Aggiungere una voce del gestore code nelle tabelle IBM MQ Db2 utilizzando la funzione ADD QMGR del programma CSQ5PQSG . Un esempio è fornito in thlqual.SCSQPROC(CSQ45AQM).

   Eseguire questa funzione per ciascun gestore code che deve essere membro del gruppo di condivisione code.

   Nota:

   a. Un gestore code può essere solo un membro di un gruppo di condivisione code.

   b. È necessario disporre di RRS in esecuzione per poter utilizzare i gruppi di condivisione code.

Concetti correlati

“Personalizzare il modulo dei parametri di sistema” a pagina 847
Il modulo di parametri di sistema IBM MQ controlla gli ambienti di registrazione, archiviazione, traccia e connessione che IBM MQ utilizza nella sua operazione. Viene fornito un modulo predefinito. È necessario creare il proprio modulo dei parametri di sistema poiché alcuni parametri, ad esempio i nomi dei dataset, sono di solito specifici del sito.

z/OS *Implementare i controlli di sicurezza ESM per il gruppo di condivisione code*

Implementare i controlli di sicurezza per tutti i gestori code in un gruppo di condivisione code, per accedere a Db2 e alle strutture dell'elenco CF (Coupling Facility).

- *Ripetere questa attività per ogni IBM MQ gestore code in un gruppo di condivisione code*
- *Potrebbe essere necessario eseguire questa attività durante la migrazione da una versione precedente.*

Accertarsi che gli ID utente associati con il gestore code, l'iniziatore di canali e i programmi di utilità dispongano dell'autorizzazione per stabilire una connessione RRSAF a ciascun sottosistema Db2 con cui si desidera stabilire una connessione. Gli ID utente per il gestore code e l'iniziatore di canali sono gli ID utente con cui vengono eseguite le procedure dell'attività avviata.

Gli ID utente per i programmi di utilità sono gli ID utente con cui è possibile inoltrare i lavori batch. Il profilo RACF per il quale l'ID utente richiede l'accesso READ è `Db2ssid.RRSAF` nella classe di risorsa DSNR

Agli ID utente associati a ciascun gestore code in un gruppo di condivisione code deve essere concesso il livello appropriato di accesso alle strutture dell'elenco CF (Coupling Facility). La classe RACF è FACILITY.

I seguenti ID utente richiedono l'accesso ALTER:

- L'ID gestore code per il profilo `IXLSTR.structure-name`
- L'ID utente che esegue CSQ5PQSG

Concetti correlati

“Implementare i controlli di sicurezza ESM” a pagina 841
Implementare i controlli di sicurezza per gestori code e iniziatore di canali.

z/OS Configurazione di Advanced Message Security for z/OS

Utilizzare questi argomenti come guida dettagliata per la configurazione di Advanced Message Security (AMS).

Prima di iniziare

Prima di iniziare a configurare AMS, verificare che siano stati eseguiti i seguenti passi di configurazione del gestore code:

1. V 9.1.3 Da IBM MQ 9.1.3 in poi, ignorare questo passo.

   Per le versioni di IBM MQ for z/OS precedenti a IBM MQ 9.1.3, APF autorizza la libreria thqual.SDRQAUTH, come descritto in “L'APF autorizza le librerie di caricamento IBM MQ” a pagina 828.
2. Aggiungi il modulo CSQ0DRTM all'LPA, come descritto in “Aggiornare l'elenco di link z/OS e LPA” a pagina 830.
3. Aggiungere una voce per CSQ0DSRV alla tabella delle proprietà del programma z/OS (PPT), come descritto in “Aggiornare la tabella delle proprietà del programma z/OS” a pagina 833.
4. Includere il membro CSQ4INSM nella concatenazione CSQINP2 della procedura dell'attività avviata del gestore code, come descritto in “Personalizzazione dei dataset di input di inizializzazione” a pagina 842.
5. V 9.1.3 Per le versioni di IBM MQ for z/OS precedenti a IBM MQ 9.1.3, includere la libreria thqual.SDRQAUTH nella concatenazione STEPLIB del gestore code, come descritto in “Creare le procedure per il gestore code IBM MQ” a pagina 838.

   Da IBM MQ 9.1.3 in poi, è possibile abilitare AMS utilizzando l'attributo AMSPROD. Per ulteriori dettagli, consultare Registrazione dell'utilizzo del prodotto con i prodotti IBM MQ for z/OS.

Operazioni successive

Configurare le politiche per le code protette da AMS. Le politiche di sicurezza sono descritte in Gestione delle politiche di sicurezza Advanced Message Security.

Esistono esempi di configurazioni AMS in Configurazioni di esempio su z/OS.

z/OS *Crea procedure per Advanced Message Security .*

Ogni sottosistema IBM MQ che deve essere configurato per utilizzare Advanced Message Security (AMS) richiede una procedura catalogata per avviare lo spazio di indirizzi AMS . È possibile creare la propria libreria o utilizzare la libreria di procedure fornita da IBM.

Procedura

1. Copiare la procedura dell'attività avviata di esempio *thlqual*.SCSQPROC (CSQ4AMSM) in SYS1.PROCLIB o, se non si utilizza SYS1.PROCLIB, la libreria delle procedure. Denominare la procedura xxxxAMSM, dove xxxx è il nome del sottosistema IBM MQ . Ad esempio, CSQ1AMSM è la AMS procedura dell'attività avviata per il gestore code CSQ1.
2. Creare una copia per ogni sottosistema IBM MQ che si sta per utilizzare.
3. Adattare le procedure ai propri requisiti utilizzando le istruzioni nella procedura di esempio CSQ4AMSM. È anche possibile utilizzare parametri simbolici in JCL per consentire la modifica della procedura quando viene avviata.
4. Rivedere e facoltativamente modificare i parametri passati all'attività AMS utilizzando il file Language Environment ® _CEE_ENVFILE. L'esempio thlqual.SCSQPROC(CSQ40ENV) elenca i parametri supportati.
5. Ripetere i passi da 1 a 4 per ogni gestore code IBM MQ .

Operazioni successive

“Impostare l'ID utente dell'attività avviata Advanced Message Security” a pagina 882

z/OS *Impostare l'ID utente dell'attività avviata Advanced Message Security*

L'attività Advanced Message Security (AMS) richiede un ID utente che ne consenta la conoscenza come processo USS (UNIX System Services).

Informazioni su questa attività

Inoltre, gli utenti per cui l'attività funziona per conto di devono avere anche una definizione appropriata di UNIX UID (ID utente) e GID (ID gruppo) in modo che questi utenti siano noti come utenti UNIX System Services. Per ulteriori informazioni sulla definizione degli UID e dei GID di UNIX System Services, consultare *z/OS: Security Server RACF Security Administrator's Guide*.

z/OS: UNIX System Services Planning confronta la sicurezza UNIX tradizionale con quella z/OS . La differenza principale tra la sicurezza UNIX tradizionale e la sicurezza z/OS è che i servizi Kernel supportano due livelli di privilegi appropriati: livello UNIX e livello z/OS UNIX .

In base alla politica di sicurezza dell'installazione, l'attività Advanced Message Security può essere eseguita con l'autorizzazione superuser (uid (0)) o con la relativa identità RACF consentita per il BPX RACF FACILITY class BPX.DAEMON e BPX.SERVER , poiché questa attività deve essere in grado di assumere l'identit ... RACF dei relativi utenti.

Se viene utilizzato l'ultimo metodo o se è già stato attivato BPX.DAEMON o BPX.SERVER , il programma attività Advanced Message Security (thlqual.SCSQAUTH(CSQ0DSRV)) deve essere ubicato nelle librerie controllate dal programma RACF .

Consultare *z/OS: UNIX System Services Planning* per comprendere le differenze di sicurezza tra la sicurezza UNIX tradizionale e la sicurezza z/OS UNIX . Ciò consente di gestire l'attività Advanced Message Security in base alla propria politica di sicurezza dell'installazione per la distribuzione e l'esecuzione di processi UNIX System Services privilegiati.

Per riferimento, le pubblicazioni utili a questa recensione sono:

- *z/OS: UNIX Pianificazione dei servizi di sistema*
- *z/OS: Security Server RACF Security Administrator's Guide*

Nota: Scegliere attentamente l'ID utente per questa attività poiché i certificati del destinatario Advanced Message Security vengono caricati in un keyring associato a questo ID utente. Questa considerazione viene discussa in Utilizzo dei certificati su z/OS .

I passi riportati di seguito descrivono come impostare l'utente dell'attività avviata Advanced Message Security . La procedura utilizza i comandi RACF come esempi. Se si utilizza un gestore della sicurezza diverso, è necessario utilizzare comandi equivalenti.

Nota: Gli esempi in questa sezione presuppongono che sia stata attivata l'elaborazione del comando del profilo generico per le classi RACF STARTED, FACILITY e SURROGAT e la verifica del profilo generico. Per ulteriori informazioni su come RACF gestisce i profili generici, consultare *z/OS: Security Server RACF Command Language Reference*.

Procedura

1. Definire l'utente dell'attività avviata Advanced Message Security in RACF. Gli esempi in questa sezione utilizzano l'ID utente WMQAMSM.

   ```
   ADDUSER WMQAMSM NAME('AMS user') OMVS (UID(0)) DFLTGRP(group)
   ```

   Selezionare un 'gruppo ' predefinito in base agli standard di installazione.

   Nota: Se non si desidera concedere l'autorizzazione superutente USS (UID (0)), è necessario consentire l'ID utente Advanced Message Security al BPX BPX.DAEMON e BPX.SERVER :

   ```
   PERMIT BPX.DAEMON CLASS(FACILITY) ID(WMQAMSM) ACCESS(READ)
   ```

   e il programma attività Advanced Message Security (*thlqual*.SCSQAUTH (CSQ0DSRV)) deve essere ubicato in una libreria controllata dal programma RACF .

   Per controllare il proprio programma di libreria SCSQAUTH, è possibile utilizzare il seguente comando:

   ```
   RALTER PROGRAM * ADDMEM('thlqual.SCSQAUTH'//NOPADCHK) -or-
   RALTER PROGRAM ** ADDMEM('thlqual.SCSQAUTH'//NOPADCHK)
   SETROPTS WHEN(PROGRAM) REFRESH
   ```

   È inoltre necessario abilitare il controllo programma per la libreria della lingua nazionale (*thlqual*.SCSQANLx) utilizzata dall'attività Advanced Message Security .
2. Determinare se la classe RACF STARTED è attiva. In caso contrario, attivare la classe RACF STARTED:

   ```
   SETROPTS CLASSACT(STARTED)
   ```
3. Definire un profilo di classe avviato per le attività Advanced Message Security , specificando l'ID utente selezionato o creato al passo 1:

   ```
   RDEFINE STARTED qmgrAMSM.* STDATA(USER(WMQAMSM))
   ```

   dove *qmgr* è il prefisso del nome dell'attività avviata. Ad esempio, l'attività avviata può essere denominata CSQ1AMSM. In questo caso, sostituire *qmgr*AMSM.* con CSQ1AMSM.*.

   Le attività avviate AMS devono essere denominate *qmgr*AMSM.
4. Utilizzare il comando **SETROPTS** RACF per aggiornare i profili della classe RACLISTed STARTED nell'archivio:

```
SETROPTS RACLIST(STARTED) REFRESH
```

5. L'attività Advanced Message Security assume temporaneamente l'identità dell'ID utente host del richiedente durante l'elaborazione della protezione dei messaggi IBM MQ . Di conseguenza, è necessario definire i profili nella classe SURROGAT per ogni ID utente che può effettuare richieste.

   Se la classe RACF SURROGAT è attiva, la definizione di un singolo profilo generico consente all'attività Advanced Message Security di assumere l'identità di qualsiasi utente. Il controllo viene ignorato se la classe SURROGAT non è attiva. I profili SURROGAT necessari sono descritti in *z/OS: UNIX System Services Planning*.

   Per definire i profili nella classe SURROGAT:

   a) Attivare la classe RACF SURROGAT utilizzando il comando RACF SETROPTS:

   ```
   SETROPTS CLASSACT(SURROGAT)
   ```

   b) Attivare l'elaborazione del profilo generico per la classe SURROGAT RACF :

   ```
   SETROPTS GENERIC(SURROGAT)
   ```

   c) Attivare l'elaborazione del comando di profilo generico per la classe SURROGAT RACF :

   ```
   SETROPTS GENCMD(SURROGAT)
   ```

   d) Definire un profilo generico nella classe SURROGAT:

   ```
   RDEFINE SURROGAT BPX.SRV.* UACC(NONE)
   ```

   e) Consentire all'ID utente Advanced Message Security il profilo della classe SURROGAT generico:

   ```
   PERMIT BPX.SRV.* CLASS(SURROGAT) ID(WMQAMSM) ACCESS(READ)
   ```

   Nota: È possibile definire profili più specifici se si desidera limitare l'elaborazione di utenti specifici da parte dell'attività Advanced Message Security , come descritto in *z/OS: UNIX System Services Planning*.

   Ad esempio, un profilo denominato BPX.SRV.MQUSER1 controlla se l'attività AMS può assumere l'identità dell'ID utente MQUSER1.

   f) Consentire l'ID utente Advanced Message Security alla funzione BPX.SERVER (se non è già stato fatto in Creazione dei certificati e dei file di chiavi):

   ```
   PERMIT BPX.SERVER CLASS(FACILITY) ID(WMQAMSM) ACCESS(READ)
   ```

   g) Utilizzare il comando **SETROPTS** RACF per aggiornare i profili della classe avviata RACLISTed nello storage:

   ```
   SETROPTS RACLIST(SURROGAT) REFRESH
   SETROPTS RACLIST(FACILITY) REFRESH
   ```

6. L'attività Advanced Message Security utilizza le funzioni fornite dai servizi SSL di z/OS System per aprire i keyring gestiti da SAF. Il SAF (System Authorization Facility) sottostante che accede al contenuto dei file di chiavi è controllato da RACFo da un gestore della sicurezza equivalente.

   Questo servizio è il servizio richiamabile IRRSDL00 (R_datalib). Questo servizio richiamabile è protetto con gli stessi profili utilizzati per proteggere i comandi RACF RACDCERT definiti per la classe RACF FACILITY. Pertanto, l'ID utente Advanced Message Security deve essere consentito ai profili utilizzando questi comandi:

a) Se non è stato ancora fatto, definire un profilo generico RACF per la classe RACF FACILITY che protegge il comando RACDCERT e il servizio richiamabile IRRSDL00 :

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
SETROPTS RACLIST(FACILITY) REFRESH
```

b) Concedere l'autorizzazione all'ID utente dell'attività avviata al profilo generico RACF :

```
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID(WMQAMSM) ACC(READ)
```

In alternativa, è possibile concedere l'accesso READ al keyring dell'utente dell'attività di servizio dati nella classe RDATALIB nel modo seguente:

```
PERMIT WMQASMD.DRQ.AMS.KEYRING.LST CLASS(RDATALIB) ID(WMQAMSM) ACC(READ)
```

7. Configurare la sicurezza delle risorse:

a) L'utente dell'attività avviata Advanced Message Security richiede l'autorità per connettersi al gestore code come applicazione batch.

Se per il gestore code è abilitata la sicurezza della connessione, concedere l'autorizzazione dell'attività AMS per connettersi al gestore code con questo comando:

```
PERMIT hlq.BATCH CLASS(MQCONN) ID(WMQAMSM) ACC(READ)
```

dove *hlq* può essere il nome del gruppo di condivisione code del nome del gestore code.

Per ulteriori informazioni, consultare Profili di sicurezza della connessione per le connessioni batch.

b) L'utente dell'attività avviata Advanced Message Security richiede l'autorità per sfogliare il SISTEMA SYSTEM.PROTECTION.POLICY.QUEUE.

Se la sicurezza della coda è attiva sul gestore code, concedere all'utente AMS l'autorizzazione ad accedere alla coda con i seguenti comandi:

```
RDEFINE MQQUEUE hlq.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
PERMIT hlq.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE) ID(WMQAMSM) ACCESS(READ)
```

dove *hlq* può essere il nome del gruppo di condivisione code del nome del gestore code.

Se il gestore code utilizza profili con caratteri maiuscoli e minuscoli, definire invece il profilo nella classe MXQUEUE.

Per gestire le politiche di protezione AMS utilizzando il programma di utilità CSQ0UTIL , gli amministratori devono accedere per inserire i messaggi nel SISTEMA SYSTEM.PROTECTION.POLICY.QUEUE. Questa operazione viene eseguita concedendo l'accesso UPDATE al profilo che protegge la coda.

Per ulteriori informazioni, consultare Profili per la sicurezza della coda.

Operazioni successive

“Concedere le autorizzazioni RACDCERT all'amministratore della sicurezza per Advanced Message Security” a pagina 885

z/OS *Concedere le autorizzazioni RACDCERT all'amministratore della sicurezza per Advanced Message Security*

L'amministratore della sicurezza Advanced Message Security richiede l'autorità per utilizzare il comando RACDCERT per creare e gestire certificati digitali.

Procedura

- Identificare l'ID utente appropriato per questo ruolo e concedere l'autorizzazione per utilizzare il comando RACDCERT. Ad esempio:

```
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID(admin) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

  dove admin è l'ID utente dell'amministratore della sicurezza Advanced Message Security .

Operazioni successive

“Concedere agli utenti le autorizzazioni di risorsa per Advanced Message Security” a pagina 886

z/OS *Concedere agli utenti le autorizzazioni di risorsa per Advanced Message Security*

Gli utenti Advanced Message Security richiedono autorizzazioni di risorse rilevanti.

Informazioni su questa attività

Gli utenti Advanced Message Security , ossia gli utenti che stanno inserendo o ottenendo i messaggi protetti Advanced Message Security , richiedono:

- Un segmento OMVS associato al relativo id utente
- Autorizzazioni per IRR.DIGTCERT.LISTRING o RDATALIB
- Autorizzazioni per i profili CSFSERV e CSFKEYS della classe ICSF
- Autorizzazione per l'inserimento in SYSTEM.PROTECTION.ERROR.QUEUE

L'attività Advanced Message Security assume temporaneamente l'identità dei suoi client; ossia, l'attività funge da surrogato dell'ID utente z/OS degli utenti di Advanced Message Security durante l'elaborazione dei messaggi IBM MQ nelle code protette da Advanced Message Security.

Affinché l'attività assuma l'identità z/OS di un utente, l'ID utente z/OS del client deve avere un segmento OMVS definito associato al proprio profilo utente.

Come aiuto di gestione, RACF fornisce la possibilità di definire un segmento OMVS predefinito che può essere associato ai profili utente e gruppo RACF . Questo valore predefinito viene utilizzato se l'ID utente o il profilo gruppo z/OS non ha un segmento OMVS definito esplicitamente. Se si prevede di avere un numero elevato di utenti che utilizzano Advanced Message Security, è possibile scegliere di utilizzare questo valore predefinito piuttosto che definire esplicitamente il segmento OMVS per ciascun utente.

Il manuale *z/OS: Security Server RACF Security Administrator's Guide* contiene la procedura dettagliata per definire i segmenti OMVS predefiniti. Rivedere la procedura come descritto in questa pubblicazione per stabilire se la definizione dei segmenti OMVS predefiniti nei profili utente e gruppo RACF è appropriata per la propria installazione.

Procedura

1. Concedere l'autorizzazione READ all'IRR IRR.DIGTCERT.LISTRING nella classe FACILITY:
   - Per concedere l'autorizzazione READ a IRR.DIGTCERT.LISTRING profilo nella classe FACILITY per tutti gli utenti, immettere questo comando:

```
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(READ)
```

   - Per concedere l'autorizzazione READ a IRR.DIGTCERT.LISTRING profilo nella classe FACILITY per utente, immettere questo comando:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(userid) ACCESS(READ)
```

dove userid è il nome dell'utente Advanced Message Security .

- In alternativa, utilizzare la classe RDATALIB per concedere l'accesso a specifici keyring. Le autorizzazioni RDATALIB hanno la precedenza su IRR.DIGTCERT.LISTRING autorizzazioni. Ad esempio:

```
PERMIT user.DRQ.AMS.KEYRING.LST CLASS(RDATALIB) ID(user) ACC(READ)
```

2. Se si utilizzano i certificati gestiti da ICSF e le chiavi private, gli utenti Advanced Message Security richiedono l'accesso a determinati profili CSFSERV e CSFKEYS. Questo accesso è descritto nella seguente tabella:

Tabella 63. Accesso utente richiesto ai profili CSFSERV e CSFKEYS

Classe	**Profilo**	**Autorizzazione**
SERV CSF	CSFDSG	LETTURA
SERV CSF	CFPKE	LETTURA
SERV CSF	CFPKD	LETTURA
SERV CSF	CSFDSV	LETTURA
CSFCHIAVI	Etichetta ICSF PKDS	LETTURA

3. Le applicazioni che eseguono operazioni sulle code con politiche AMS definite devono accedere per inserire i messaggi in SYSTEM.PROTECTION.ERROR.QUEUE. Concedere l'accesso alla coda con i seguenti comandi:

```
RDEFINE MQQUEUE hlq.SYSTEM.PROTECTION.ERROR.QUEUE UACC(NONE)
PERMIT hlq.SYSTEM.PROTECTION.ERROR.QUEUE CLASS(MQQUEUE) ID(userId) ACCESS(UPDATE)
```

dove *hlq* può essere il nome del gruppo di condivisione code e *userID* è l'ID utente dell'applicazione.

Operazioni successive

“Creare portachiavi per Advanced Message Security” a pagina 887

z/OS *Creare portachiavi per Advanced Message Security*

I certificati utilizzati da Advanced Message Security (AMS) per la firma e la cifratura sono memorizzati nei keyring SAF z/OS . È necessario creare questi keyring e certificati prima di poter utilizzare AMS.

Informazioni su questa attività

Advanced Message Security accede ai certificati nei seguenti keyring:

- Un singolo keyring di proprietà dell'utente dello spazio di indirizzi AMS .
- File di chiavi di proprietà dei singoli utenti che inviano o ricevono messaggi sulle code con le politiche AMS definite.

Questi keyring devono essere tutti denominati `drq.ams.keyring`.

Ci sono ulteriori informazioni sui key ring e i certificati utilizzati da AMS, e uno scenario di esempio, in Utilizzo dei certificati su z/OS.

Attenersi alla seguente procedura per creare i file di chiavi richiesti da AMSe collegare i certificati ai file di chiavi. È necessario creare il keyring di proprietà dell'utente dello spazio di indirizzi AMS prima di avviare AMS. È possibile creare i key ring di proprietà degli utenti che inviano o ricevono messaggi in qualsiasi momento.

Procedura

1. Immettere il seguente comando per creare un keyring di proprietà dell'utente dello spazio di indirizzi AMS :

   ```
   RACDCERT ID(amsUser) ADDRING(drq.ams.keyring)
   ```

   dove *amsUser* è l'ID utente dello spazio di indirizzo AMS .
2. Creare un keyring per ogni utente che invia o riceve messaggi protetti da AMS immettendo il comando nel passo 1 per ogni ID utente.
3. Collegare il certificato CA (certificate authority) per l'emittente dei certificati utente al key ring di proprietà dell'ID utente spazio indirizzo AMS . Emetti il seguente comando:

   ```
   RACDCERT ID(amsUser) CONNECT(CERTAUTH LABEL('caLabel') RING(drq.ams.keyring))
   ```

   dove *amsUser* è l'ID utente dello spazio di indirizzi AMS e *caLabel* è l'etichetta del certificato CA.

   Se si utilizza RACF come CA e si deve creare un certificato CA (Certificate Authority), seguire l'esempio in Definizione di un certificato CA (Certificate Authority) locale.
4. Se si utilizzano le politiche di riservatezza o riservatezza per codificare i messaggi sulle code protette da AMS, connettere i certificati dei destinatari dei messaggi al key ring di proprietà dell'ID utente dello spazio di indirizzo AMS . Emetti il seguente comando:

   ```
   RACDCERT ID(amsUser) CONNECT(ID(userId) LABEL('certLabel')
   RING(drq.ams.keyring) USAGE(SITE))
   ```

   dove *amsUser* è l'ID utente dello spazio di indirizzo AMS , *userId* è il destinatario del messaggio e *certLabel* è l'etichetta del certificato dell'utente.

   L'attributo `USAGE(SITE)` impedisce l'accessibilità della chiave privata nel keyring.

   Se si stanno creando i propri certificati con RACF, seguire l'esempio in Creazione di un certificato digitale con una chiave privata per creare il certificato.
5. Connettere i certificati di ciascun utente che invia o riceve i messaggi protetti da AMS a un keyring di proprietà dell'utente. Il certificato deve essere connesso come certificato predefinito nel keyring. Emetti il seguente comando:

   ```
   RACDCERT ID(userId) CONNECT(ID(userId) LABEL('certLabel')
   RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
   ```

   dove *userId* è l'utente che sta inviando o ricevendo messaggi e *certLabel* è l'etichetta del certificato dell'utente.

Operazioni successive

“AbilitaAdvanced Message Security” a pagina 888

z/OS *AbilitaAdvanced Message Security*

La funzionalità della politica di sicurezza per un gestore code viene controllata dal parametro SPLCAP nel modulo dei parametri di sistema.

Informazioni su questa attività

Attenersi alla seguente procedura per abilitare Advanced Message Security (AMS) per un singolo gestore code.

Questa attività richiede di apportare una modifica al modulo dei parametri di sistema. Consultare “Personalizzare il modulo dei parametri di sistema” a pagina 847 per ulteriori informazioni sulla creazione e personalizzazione del modulo dei parametri di sistema.

Procedura

1. Impostare **SPLCAP** su YES in CSQ6SYSP. Consultare “Utilizzo di CSQ6SYSP” a pagina 849 per ulteriori informazioni sulla macro CSQ6SYSP .
2. V 9.1.3
   Impostare **AMSPROD** su AMS, ADVANCED o ADVANCEDVUE in base alla titolarità della licenza. Per ulteriori informazioni sulla macro CSQ6USGP , consultare Utilizzo di CSQ6USGP .
3. Ricompilare il modulo dei parametri di sistema.
4. Riavviare il Gestore code con il modulo dei parametri di sistema aggiornato. Lo spazio di indirizzo AMS viene avviato automaticamente all'avvio del gestore code.

z/OS V 9.1.0 Configurazione del server mqweb

Utilizzare questi argomenti come guida dettagliata per la configurazione del server mqweb.

Attività correlate

“Configurazione di IBM MQ Console e REST API” a pagina 760
Il server mqweb che ospita IBM MQ Console e REST API viene fornito con una configurazione predefinita. Per poter utilizzare uno di questi componenti è necessario completare una serie di attività di configurazione, come la configurazione della sicurezza per consentire agli utenti di accedere. Questo argomento descrive tutte le opzioni di configurazione disponibili.

z/OS V 9.1.0 *Creazione del server mqweb*

Se sono stati installati i componenti Web di IBM MQ for z/OS UNIX System Services e si desidera utilizzare MQ Console, o REST API, è necessario creare e personalizzare il server mqweb.

Prima di iniziare

È necessario creare il SISTEMA SYSTEM.REST.REPLY.QUEUE per utilizzare il server Liberty . Eseguire questa operazione utilizzando l'esempio **CSQ4INSG** più recente in “Personalizzazione dei dataset di input di inizializzazione” a pagina 842.

Attenzione: Quando si avvia il server mqweb, se viene visualizzato il messaggio di errore CWWKG0014E, come visualizzato nel seguente output:

```
     Launching mqweb (MQM MVS/ESA V9 R2.0/wlp...) (en_US)
               ÝAUDIT   ¨ CWWKE0001I: The server mqweb has been
launched.
               ÝWARNING ¨ CWWKF0009W: The server has not been configured to install any
features.
               ÝAUDIT   ¨ CWWKF0011I: The mqweb server is ready to run a smarter planet.
The mqweb server started in 6.348 seconds.
               ÝERROR   ¨ CWWKG0014E: The configuration parser detected an XML syntax
error while parsing the root of the configuration and the referenced configuration
documents.
                                 Error: An invalid XML character (Unicode: 0x4c) was found
in the prolog of the document.
                                  File: file:<your filepath>/servers/mqweb/server.xml Line:
1 Column: 1
```

è necessario controllare l'impostazione z/OS di AUTOCVT (convertire automaticamente i file da una serie di codici a un altro) e regolare il valore come richiesto effettuando una delle seguenti operazioni.

In un terminale USS:

Immettere il comando: echo **$_BPXK_AUTOCVT**per visualizzare il valore di questa variabile di ambiente. Se la variabile di ambiente non è definita, non viene visualizzato alcun valore.

Per impostare la variabile di ambiente, vedi _BPXK environment variables.

A livello di sistema:

L'esempio 6 in Visualizzazione dello stato di z/OS UNIX System Services (OMVS) mostra come visualizzare il valore dell'istruzione AUTOCVT del sistema in BPXPRMxx.

Per impostare la variabile di ambiente a livello di sistema, utilizzare l'istruzione AUTOCVT in BPXPRMxx.

Se la variabile di ambiente _BPeccedenze AUTOCVT è impostata in un terminale USS, sovrascrive l'impostazione a livello di sistema dell'istruzione AUTOCVT in BPXPRMxx.

Informazioni su questa attività

- È necessario eseguire questa attività una volta per ogni sistema z/OS in cui si desidera eseguire MQ Console o REST API.
- È necessario un server mqweb per ciascuna versione di IBM MQ in esecuzione.
- Potrebbe essere necessario aggiornare o modificare la configurazione del server quando si esegue la migrazione da una versione precedente.

MQ Console e REST API richiedono la creazione di un singolo server Liberty , denominato mqweb.

I file di log e di configurazione del server sono tutti memorizzati nella directory utente Liberty .

Attenzione: Consultare RACF profiles per alcuni esempi di esempi RDEFINE e nella sezione Profili utilizzati per controllare l'accesso alle risorse IBM MQ fare riferimento a Profili per gli elenchi nomi per informazioni sull'impostazione della sicurezza necessaria sul server.

Completare la seguente procedura per creare il server mqweb:

Procedura

1. Scegliere un percorso adatto per la directory utente Liberty .

   L'ID utente con cui viene eseguito il server mqweb, richiede l'accesso in lettura e scrittura a questa directory utente e al relativo contenuto. Poiché questa directory utente conterrà i file di log e la configurazione del server, è necessario creare questa directory in un file system separato.

   Nota: C'è una quantità significativa di I/O del disco all'avvio del server mqweb. Per ridurre il tempo impiegato per avviare il server mqweb, assicurarsi che sia il file system UNIX di IBM MQ installazione z/OS che il file system della directory utente Liberty siano sysplex-aware o montati localmente sul sistema su cui è in esecuzione il server mqweb.
2. In UNIX System Services, assicurarsi che la directory corrente sia `PathPrefix/web/bin`, immettendo il seguente comando:

   ```
   cd PathPrefix/web/bin
   ```

   `PathPrefix` è il IBM MQ percorso di installazione dei componenti di UNIX System Services.
3. Creare la directory utente Liberty , contenente la definizione del server mqweb modello, eseguendo lo script **crtmqweb** . Ad esempio, per creare la directory utente Liberty in `/var/mqm/mqweb`, immettere il comando:

   ```
   ./crtmqweb /var/mqm/mqweb
   ```

   Nota: Lo script **crtmqweb** accetta un parametro facoltativo - il nome della directory utente Liberty .

   Se non si fornisce un nome per la directory utente Liberty , viene utilizzato il valore predefinito `/var/mqm/web/installation1` .
4. Modificare la proprietà delle directory e file nella directory utente Liberty , in modo che appartengano all'ID utente e al gruppo con cui viene eseguito il server mqweb, utilizzando il comando:

   ```
   chown -R userid:group path
   ```

   Per fornire al gruppo l'accesso in scrittura al percorso, immettere il comando:

   ```
   chmod -R 770 path
   ```

Operazioni successive

“Creazione di una procedura per il server mqweb” a pagina 891

Attività correlate

“Configurazione di IBM MQ Console e REST API” a pagina 760

Il server mqweb che ospita IBM MQ Console e REST API viene fornito con una configurazione predefinita. Per poter utilizzare uno di questi componenti è necessario completare una serie di attività di configurazione, come la configurazione della sicurezza per consentire agli utenti di accedere. Questo argomento descrive tutte le opzioni di configurazione disponibili.

z/OS V 9.1.0 *Creazione di una procedura per il server mqweb*

Se sono stati installati i componenti Web di IBM MQ for z/OS Unix System Services e si desidera utilizzare MQ Consoleo REST API, è necessario creare una procedura catalogata per avviare il server mqweb. Il server mqweb è un server di Liberty che ospita MQ Console e REST API.

- È necessario eseguire questa attività una volta per ogni sistema z/OS in cui si desidera eseguire MQ Console o REST API.
- È necessario un server mqweb per ciascuna versione di IBM MQ in esecuzione. Ad esempio, un'attività avviata denominata MQWB0910 per gestori code in IBM MQ 9.1.0 e un'attività avviata denominata MQWB0905 per i gestori code in IBM MQ 9.0.5.

  Se si dispone di un solo gestore code sul sistema z/OS , è possibile eseguire una singola attività avviata del server Liberty e modificare le librerie utilizzate durante la migrazione del gestore code.
- Potrebbe essere necessario modificare la procedura catalogata durante la migrazione da una versione precedente.

Eseguire la seguente procedura per creare una procedura catalogata:

1. Copiare la procedura di attività avviata di esempio `thlqual.SCSQPROC(CSQ4WEBS)` nella libreria delle procedure.

   Denominare la procedura in base agli standard della propria azienda.

   Ad esempio, `MQWB0910`, indica che questa è la procedura catalogata per il server IBM MQ 9.1.0 mqweb.
2. Adattare la procedura ai propri requisiti utilizzando le istruzioni contenute nella procedura di esempio CSQ4WEBS.

   Si noti che la directory utente Liberty è la directory specificata quando è stato eseguito lo script **`crtmqweb`** per creare la definizione del server mqweb.

   Consultare “Creazione del server mqweb” a pagina 889 per i dettagli.

   Nota: Assicurarsi di specificare **Maiuscole disattivate** quando si modifica il membro, poiché il file contiene dati in minuscolo.
3. Autorizzare la procedura da eseguire con il gestore della sicurezza esterno.
4. Utilizzare IBM Workload Manager (WLM) per classificare questo spazio di indirizzo.

   Il server mqweb è un'applicazione IBM MQ e gli utenti interagiscono con questa applicazione. Non è necessario che l'applicazione abbia un'importanza elevata in WLM e una classe di servizi di **STCUSER** potrebbe essere adatta.

Cosa fare successivamente

Seguire i passi in “Configurazione di base per il server mqweb” a pagina 760 per terminare la configurazione del server mqweb.

Attività correlate

“Configurazione di IBM MQ Console e REST API” a pagina 760

Il server mqweb che ospita IBM MQ Console e REST API viene fornito con una configurazione predefinita. Per poter utilizzare uno di questi componenti è necessario completare una serie di attività

di configurazione, come la configurazione della sicurezza per consentire agli utenti di accedere. Questo argomento descrive tutte le opzioni di configurazione disponibili.

z/OS Test di un gestore code su z/OS

Una volta personalizzato o migrato il gestore code, è possibile verificarlo eseguendo i programmi di verifica dell'installazione e alcune delle applicazioni di esempio fornite con IBM MQ for z/OS.

Informazioni su questa attività

Una volta installato e personalizzato IBM MQ for z/OS, è possibile utilizzare il programma di verifica dell'installazione fornito, CSQ4IVP1, per verificare che IBM MQ for z/OS sia operativo.

Il programma di verifica dell'installazione di base CSQ4IVP1 verifica le code non condivise e verifica la IBM MQ di base senza utilizzare gli esempi C, COBOL o CICS .

Dopo aver eseguito la verifica di base dell'installazione, è possibile verificare le code condivise utilizzando CSQ4IVP1 con code diverse e verificare che Db2 e la CF siano impostati correttamente. Per confermare che l'accodamento distribuito è operativo, è possibile utilizzare il programma di verifica dell'installazione fornito, CSQ4IVPX,

CSQ4IVP1 viene fornito come modulo di caricamento e fornisce una serie di applicazioni di esempio procedurali come moduli di origine che dimostrano gli utilizzi tipici di MQI (Message Queue Interface). È possibile utilizzare questi moduli di origine per verificare diversi ambienti di linguaggio di programmazione. È possibile compilare e modificare i collegamenti degli altri esempi appropriati per l'installazione utilizzando il JCL di esempio fornito.

Procedura

- Per informazioni su come verificare il gestore code su z/OS, consultare i seguenti argomenti secondari:
  - “Esecuzione del programma di verifica dell'installazione di base” a pagina 892
  - “Verifica dei gruppi di condivisione code” a pagina 896
  - “Test per l'accodamento distribuito” a pagina 897
  - “Test per programmi C, C + +, COBOL, PL/I e CICS con IBM MQ for z/OS” a pagina 900

Concetti correlati

Concetti di IBM MQ for z/OS

Attività correlate

Pianificazione dell'ambiente IBM MQ su z/OS

“Configurazione dei gestori code su z/OS” a pagina 821
Utilizzare queste istruzioni per configurare i gestori code su IBM MQ for z/OS.

AmministrazioneIBM MQ for z/OS

z/OS Esecuzione del programma di verifica dell'installazione di base

Una volta installato e personalizzato IBM MQ, è possibile utilizzare il programma di verifica dell'installazione fornito, CSQ4IVP1, per verificare che IBM MQ sia operativo.

Il programma di verifica dell'installazione di base è un IVP dell'assembler batch che verifica IBM MQ di base senza utilizzare gli esempi C, COBOL o CICS .

Batch Assembler IVP è collegato - modificato da SMP/E e i moduli di carico vengono forniti nella libreria thlqual.SCSQLOAD.

Una volta completata la fase SMP/E APPLY e la fase di personalizzazione, eseguire l'IVP dell'Assembler batch.

Per ulteriori dettagli, consultare le sezioni riportate di seguito:

- Panoramica dell'applicazione CSQ4IVP1
- Preparazione all'esecuzione di CSQ4IVP1
- Esecuzione di CSQ4IVP1
- Verifica dei risultati di CSQ4IVP1

Panoramica dell'applicazione CSQ4IVP1

CSQ4IVP1 è un'applicazione batch che si collega al sottosistema IBM MQ ed esegue queste funzioni di base:

- Emette chiamate IBM MQ
- Comunica con il server dei comandi
- Verifica che il trigger sia attivo
- Genera ed elimina una coda dinamica
- Verifica l'elaborazione della scadenza del messaggio
- Verifica l'elaborazione del commit del messaggio

Preparazione all'esecuzione di CSQ4IVP1

Prima di eseguire CSQ4IVP1:

1. Verificare che le voci IVP si trovino nella concatenazione del dataset CSQINP2 nel programma di avvio del gestore code. Le voci IVP vengono fornite nel membro thlqual.SCSQPROC(CSQ4IVPQ). In caso contrario, aggiungere le definizioni fornite in thlqual.SCSQPROC(CSQ4IVPQ) alla concatenazione CSQINP2 . Se il gestore code è attualmente in esecuzione, è necessario riavviarlo in modo che queste definizioni abbiano effetto.
2. Il JCL di esempio, CSQ4IVPR, richiesto per eseguire il programma di verifica dell'installazione si trova nella libreria thlqual.SCSQPROC.

   Personalizzare il JCL CSQ4IVPR con il qualificatore di alto livello per le librerie IBM MQ , la lingua nazionale che si desidera utilizzare, il nome del gestore code IBM MQ di quattro caratteri e la destinazione per l'output del lavoro.
3. Aggiornare RACF per consentire a CSQ4IVP1 di accedere alle relative risorse se è attiva la sicurezza IBM MQ .

   Per eseguire CSQ4IVP1 quando la sicurezza IBM MQ è abilitata, è necessario un ID utente RACF con autorizzazione per accedere agli oggetti. Per i dettagli relativi alla definizione delle risorse in RACF, consultare Impostazione della sicurezza su z/OS . L'ID utente che esegue IVP deve disporre della seguente autorità di accesso:

Autorità	**Profilo**	**Classe**
LETTURA	ssid.DISPLAY.PROCESS	MQCMDS
AGGIORNA	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
AGGIORNA	ssid.SYSTEM.COMMAND.REPLY.MODEL	MQQUEUE
AGGIORNA	ssid.CSQ4IVP1.**	MQQUEUE
LETTURA	ssid.BATCH	MQCONN

   Questi requisiti presuppongono che tutta la sicurezza IBM MQ sia attiva. I comandi RACF per attivare la sicurezza IBM MQ sono mostrati in Figura 100 a pagina 894. Questo esempio presuppone che il nome gestore code sia CSQ1 e che l'ID utente della persona che esegue l'esempio CSQ4IVP1 sia TS101.

```
RDEFINE MQCMDS CSQ1.DISPLAY.PROCESS
PERMIT CSQ1.DISPLAY.PROCESS CLASS(MQCMDS) ID(TS101) ACCESS(READ)

RDEFINE MQQUEUE CSQ1.SYSTEM.COMMAND.INPUT
PERMIT CSQ1.SYSTEM.COMMAND.INPUT CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.COMMAND.REPLY.MODEL
PERMIT CSQ1.SYSTEM.COMMAND.REPLY.MODEL CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.CSQ4IVP1.**
PERMIT CSQ1.CSQ4IVP1.** CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQCONN CSQ1.BATCH
PERMIT CSQ1.BATCH CLASS(MQCONN) ID(TS101) ACCESS(READ)
```

Figura 100. Comandi RACF per CSQ4IVP1

Esecuzione di CSQ4IVP1

Una volta completata questa procedura, avviare il gestore code. Se il gestore code è già in esecuzione e si è modificato CSQINP2, è necessario arrestare il gestore code e riavviarlo.

IVP viene eseguito come lavoro batch. Personalizzare la scheda di lavoro per soddisfare i requisiti di inoltro della propria installazione.

Verifica dei risultati di CSQ4IVP1

L'IVP è suddiviso in 10 fasi; ogni fase deve essere completata con un codice di completamento zero prima dell'esecuzione della fase successiva. L'IVP genera un report, che elenca:

- Il nome del gestore code a cui si sta eseguendo la connessione.
- Un messaggio di una riga che mostra il codice di completamento e il codice motivo restituiti da ogni fase.
- Un messaggio informativo di una riga, dove appropriato.

Un report di esempio viene fornito in Figura 101 a pagina 896

z/OS Per una spiegazione dei codici di completamento e di motivo, consultare IBM MQ for z/OS messaggi, codici di completamento e di motivo.

Alcuni stage dispongono di più di una chiamata IBM MQ e, in caso di errore, viene emesso un messaggio che indica la chiamata IBM MQ specifica che ha restituito l'errore. Inoltre, per alcune fasi l'IVP inserisce informazioni esplicative e diagnostiche in un campo di commento.

Il lavoro IVP richiede il controllo esclusivo di alcuni oggetti del gestore code e pertanto deve essere a thread singolo attraverso il sistema. Tuttavia, non esiste alcun limite al numero di volte in cui l'IVP può essere eseguito sul gestore code.

Le funzioni eseguite da ogni fase sono:

Fase 1
Connettersi al gestore code emettendo la chiamata API MQCONN .

Stage 2
Determinare il nome della coda di immissione comandi di sistema utilizzata dal server dei comandi per richiamare i messaggi di richiesta. Questa coda riceve richieste di visualizzazione dalla fase 5.

A tale scopo, la sequenza di chiamate è:

1. Emettere una chiamata MQOPEN , specificando il nome del gestore code, per aprire l'oggetto gestore code.
2. Emettere una chiamata MQINQ per individuare il nome della coda di immissione del comando di sistema.

3. Emettere una chiamata MQINQ per informazioni su vari switch di eventi del gestore code.
4. Eseguire una chiamata MQCLOSE per chiudere l'oggetto gestore code.

Al completamento con esito positivo di questo stage, il nome della coda di input del comando di sistema viene visualizzato nel campo del commento.

Stage 3
Aprire una coda di avvio utilizzando una chiamata **MQOPEN** .

Questa coda viene aperta in questa fase in previsione di un messaggio di trigger, che arriva come risultato della risposta del server dei comandi alla richiesta dalla fase 5. La coda deve essere aperta perché l'input soddisfi i criteri di attivazione.

Stage 4
Creare una coda dinamica permanente utilizzando CSQ4IVP1.MODEL coda come modello. La coda dinamica ha gli stessi attributi del modello da cui è stata creata. Ciò significa che quando le risposte dalla richiesta del server dei comandi nella fase 5 vengono scritte in questa coda, viene scritto un messaggio trigger nella coda di iniziazione aperta nella fase 3.

Al completamento con esito positivo di questa fase, il nome della coda dinamica permanente viene indicato nel campo commento.

Stage 5
Emettere una richiesta MQPUT1 alla coda comandi del server dei comandi.

Un messaggio di tipo MQMT_REQUEST viene scritto nella coda di input del comando di sistema che richiede una visualizzazione del processo CSQ4IVP1. Il descrittore del messaggio specifica la coda dinamica permanente creata nella fase 4 come coda di risposta per la risposta del server dei comandi.

Fase 6
Emettere una richiesta **MQGET** dalla coda di iniziazione. In questa fase, viene emesso un comando GET WAIT con un intervallo di 1 minuto rispetto alla coda di avvio aperta nella fase 3. Si prevede che il messaggio restituito sia il messaggio trigger generato dai messaggi di risposta del server dei comandi scritti nella coda di risposta.

Fase 7
Eliminare la coda dinamica permanente creata nella fase 4. Poiché la coda contiene ancora messaggi, viene utilizzata l'opzione MQCO_PURGE_DELETE.

Fase 8

1. Aprire una coda dinamica.
2. MQPUT un messaggio con un intervallo di scadenza impostato.
3. Attendere la scadenza del messaggio.
4. Tentativo di MQGET del messaggio scaduto.
5. MQCLOSE la coda.

Fase 9

1. Aprire una coda dinamica.
2. MQPUT un messaggio.
3. Immettere MQCMIT per eseguire il commit dell'unità di lavoro corrente.
4. MQGET il messaggio.
5. Emettere MQBACK per eseguire il backout del messaggio.
6. MQGET lo stesso messaggio e verificare che il numero di backout sia impostato su 1.
7. Immettere MQCLOSE per chiudere la coda.

Fase 10
Disconnettersi dal gestore code utilizzando **MQDISC**.

Dopo aver eseguito IVP, è possibile eliminare tutti gli oggetti non più necessari.

Se l'IVP non viene eseguito correttamente, provare a eseguire manualmente ogni operazione per individuare la funzione non riuscita.

```
DATE : 2005.035                IBM MQ for z/OS - V6           PAGE : 0001
INSTALLATION VERIFICATION PROGRAM
PARAMETERS ACCEPTED. PROGRAM WILL CONNECT TO : CSQ1
,OBJECT QUALIFER : CSQ4IVP1
INSTALLATION VERIFICATION BEGINS :
STAGE 01 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR BRIDGE EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS EXCP FOR CHANNEL EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR SSL EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR INHIBITED EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR LOCAL EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR PERFORMENCE EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR REMOTE EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR START/STOP EVENTS
STAGE 02 COMPLETE. COMPCODE : 0000 REASON CODE : 0000 SYSTEM.COMMAND.INPUT
STAGE 03 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 04 COMPLETE. COMPCODE : 0000 REASON CODE : 0000 CSQ4IVP1.BAB9810EFEAC8980
STAGE 05 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 06 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 07 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 08 COMPLETE. COMPCODE : 0000 REASON CODE : 0000 CSQ4IVP1.BAB9810F0070E645
STAGE 09 COMPLETE. COMPCODE : 0000 REASON CODE : 0000 CSQ4IVP1.BAB9812BA8706803
STAGE 10 COMPLETE. COMPCODE : 0000 REASON CODE : 0000>>>>>>>>>>   END OF REPORT   <<<<<<<<<<
```

Figura 101. Report di esempio da CSQ4IVP1

z/OS Verifica dei gruppi di condivisione code

Il programma di verifica dell'installazione di base CSQ4IVP1 verifica le code non condivise.

CSQ4IVP1 può essere utilizzato anche se il gestore code è un membro di un gruppo di condivisione code. Dopo aver eseguito l'IVP di base, è possibile verificare le code condivise utilizzando il programma di verifica dell'installazione CSQ4IVP1 con code differenti. Inoltre, verifica che Db2 e la CF siano impostati correttamente.

Preparazione all'esecuzione di CSQ4IVP1 per un gruppo di condivisione code

Prima di eseguire CSQ4IVP1:

1. Aggiungere la struttura CF utilizzata da IVP al dataset della politica CFRM, come descritto in “Impostazione della CF (coupling facility)” a pagina 879. Gli esempi forniti utilizzano una struttura denominata APPLICATION1, ma è possibile modificarla se si desidera.
2. Verificare che le voci IVP si trovino nella concatenazione del dataset CSQINP2 nel programma di avvio del gestore code. Le voci IVP vengono fornite nel membro thlqual.SCSQPROC(CSQ4IVPG). In caso contrario, aggiungere le definizioni fornite in thlqual.SCSQPROC(CSQ4IVPG) alla concatenazione CSQINP2 . Se il gestore code è attualmente in esecuzione, è necessario riavviarlo in modo che queste definizioni abbiano effetto.
3. Modificare il nome della struttura CFS (coupling facility structure) utilizzata in thlqual.SCSQPROC(CSQ4IVPG), se necessario.
4. Il JCL di esempio, CSQ4IVPS, richiesto per eseguire il programma di verifica dell'installazione per un gruppo di condivisione code si trova nella libreria thlqual.SCSQPROC.

   Personalizzare il JCL CSQ4IVPS con il qualificatore di alto livello per le librerie IBM MQ , la lingua nazionale che si desidera utilizzare, il nome del gestore code IBM MQ di quattro caratteri e la destinazione per l'output del lavoro.
5. Aggiornare RACF per consentire a CSQ4IVP1 di accedere alle relative risorse se è attiva la sicurezza IBM MQ .

   Per eseguire CSQ4IVP1 quando la sicurezza IBM MQ è abilitata, è necessario un ID utente RACF con autorizzazione per accedere agli oggetti. Per i dettagli relativi alla definizione delle risorse in RACF, consultare Impostazione della sicurezza su z/OS . L'ID utente che esegue IVP deve avere la seguente autorizzazione di accesso in aggiunta a quella richiesta per eseguire l'IVP di base:

Autorità	Profilo	Classe
AGGIORNA	ssid.CSQ4IVPG.**	MQQUEUE

Questi requisiti presuppongono che tutta la sicurezza IBM MQ sia attiva. I comandi RACF per attivare la sicurezza IBM MQ sono mostrati in Figura 102 a pagina 897. Questo esempio presuppone che il nome gestore code sia CSQ1 e che l'ID utente della persona che esegue l'esempio CSQ4IVP1 sia TS101.

```
RDEFINE MQQUEUE CSQ1.CSQ4IVPG.**
PERMIT CSQ1.CSQ4IVPG.** CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)
```

Figura 102. Comandi RACF per CSQ4IVP1 per un gruppo di condivisione code

Esecuzione di CSQ4IVP1 per un gruppo di condivisione code

Una volta completata questa procedura, avviare il gestore code. Se il gestore code è già in esecuzione e si è modificato CSQINP2, è necessario arrestare il gestore code e riavviarlo.

IVP viene eseguito come lavoro batch. Personalizzare la scheda di lavoro per soddisfare i requisiti di inoltro della propria installazione.

Controllo dei risultati di CSQ4IVP1 per un gruppo di condivisione code

L'IVP per i gruppi di condivisione code funziona allo stesso modo dell'IVP di base, tranne per il fatto che le code create sono denominate CSQIVPG. *xx*. Seguire le istruzioni fornite in “Verifica dei risultati di CSQ4IVP1” a pagina 894 per controllare i risultati dell'IVP per i gruppi di condivisione code.

z/OS Test per l'accodamento distribuito

È possibile utilizzare il programma di verifica dell'installazione fornito, CSQ4IVPX, per verificare che l'accodamento distribuito sia operativo.

Panoramica del lavoro CSQ4IVPX

CSQ4IVPX è un lavoro batch che avvia l'iniziatore di canali ed emette il comando IBM MQ DISPLAY CHINIT. Ciò verifica che tutti gli aspetti principali dell'accodamento distribuito siano operativi, evitando la necessità di impostare le definizioni di canale e di rete.

Preparazione all'esecuzione di CSQ4IVPX

Prima di eseguire CSQ4IVPX:

1. Il JCL di esempio, CSQ4IVPX, richiesto per eseguire il programma di verifica dell'installazione si trova nella libreria thlqual.SCSQPROC.

   Personalizzare il JCL CSQ4IVPX con il qualificatore di alto livello per le librerie IBM MQ , la lingua nazionale che si desidera utilizzare, il nome del gestore code di quattro caratteri e la destinazione per l'output del lavoro.
2. Aggiornare RACF per consentire a CSQ4IVPX di accedere alle relative risorse se la sicurezza IBM MQ è attiva. Per eseguire CSQ4IVPX quando è abilitata la sicurezza IBM MQ , è necessario un ID utente di RACF con autorizzazione per accedere agli oggetti. Per i dettagli relativi alla definizione delle risorse in RACF, consultare Impostazione della sicurezza su z/OS . L'ID utente che esegue IVP deve disporre della seguente autorità di accesso:

Autorità	Profilo	Classe
CONTROL	ssid.START.CHINIT e ssid.STOP.CHINIT	MQCMDS
AGGIORNA	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
AGGIORNA	ssid.SYSTEM.CSQUTIL.*	MQQUEUE
LETTURA	ssid.BATCH	MQCONN
LETTURA	ssid.DISPLAY.CHINIT	MQCMDS

Questi requisiti presuppongono che il profilo di sicurezza della connessione ssid.CHIN sia stato definito (come mostrato in Profili di sicurezza della connessione per l'iniziatore di canali) e che tutta la sicurezza IBM MQ sia attiva. I comandi RACF per eseguire questa operazione sono riportati in Figura 103 a pagina 899. Questo esempio presuppone che:

- Il nome del gestore code è CSQ1
- L'ID utente della persona che esegue l'esempio CSQ4IVPX è TS101
- Lo spazio di indirizzo dell'iniziatore di canali è in esecuzione con l'ID utente CSQ1MSTR

3. Aggiornare RACF per consentire allo spazio di indirizzo dell'iniziatore di canali la seguente autorità di accesso:

Autorità	Profilo	Classe
LETTURA	ssid.CHIN	MQCONN
AGGIORNA	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
AGGIORNA	ssid.SYSTEM.CHANNEL.INITQ	MQQUEUE
AGGIORNA	ssid.SYSTEM.CHANNEL.SYNCQ	MQQUEUE
MODIFICA	ssid.SYSTEM.CLUSTER.COMMAND.QUEUE	MQQUEUE
AGGIORNA	ssid.SYSTEM.CLUSTER.TRANSMIT.QUEUE	MQQUEUE
MODIFICA	ssid.SYSTEM.CLUSTER.REPOSITORY.QUEUE	MQQUEUE
CONTROL	ssid.CONTEXT.**	MQADMIN

I comandi RACF per eseguire questa operazione sono riportati anche in Figura 103 a pagina 899.

```
RDEFINE MQCMDS CSQ1.DISPLAY.DQM
PERMIT CSQ1.DISPLAY.DQM CLASS(MQCMDS) ID(TS101) ACCESS(READ)

RDEFINE MQCMDS CSQ1.START.CHINIT
PERMIT CSQ1.START.CHINIT CLASS(MQCMDS) ID(TS101) ACCESS(CONTROL)

RDEFINE MQCMDS CSQ1.STOP.CHINIT
PERMIT CSQ1.STOP.CHINIT CLASS(MQCMDS) ID(TS101) ACCESS(CONTROL)

RDEFINE MQQUEUE CSQ1.SYSTEM.COMMAND.INPUT
PERMIT CSQ1.SYSTEM.COMMAND.INPUT CLASS(MQQUEUE) ID(TS101,CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.CSQUTIL.*
PERMIT CSQ1.SYSTEM.CSQUTIL.* CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQCONN CSQ1.BATCH
PERMIT CSQ1.BATCH CLASS(MQCONN) ID(TS101) ACCESS(READ)

RDEFINE MQCONN CSQ1.CHIN
PERMIT CSQ1.CHIN CLASS(MQCONN) ID(CSQ1MSTR) ACCESS(READ)

RDEFINE MQQUEUE CSQ1.SYSTEM.CHANNEL.SYNCQ
PERMIT CSQ1.SYSTEM.CHANNEL.SYNCQ CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.CLUSTER.COMMAND.QUEUE
PERMIT CSQ1.SYSTEM.CLUSTER.COMMAND.QUEUE CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(ALTER)

RDEFINE MQQUEUE CSQ1.SYSTEM.CLUSTER.TRANSMIT.QUEUE
PERMIT CSQ1.SYSTEM.CLUSTER.TRANSMIT.QUEUE CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.CLUSTER.REPOSITORY.QUEUE
PERMIT CSQ1.SYSTEM.CLUSTER.REPOSITORY.QUEUE CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(ALTER)

RDEFINE MQQUEUE CSQ1.SYSTEM.CHANNEL.INITQ
PERMIT CSQ1.SYSTEM.CHANNEL.INITQ CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQADMIN CSQ1.CONTEXT.**
PERMIT CSQ1.CONTEXT.** CLASS(MQADMIN) ID(CSQ1MSTR) ACCESS(CONTROL)
```

Figura 103. Comandi RACF per CSQ4IVPX

Esecuzione di CSQ4IVPX

Una volta completata questa procedura, avviare il gestore code.

IVP viene eseguito come lavoro batch. Personalizzare la scheda di lavoro per soddisfare i requisiti di inoltro della propria installazione.

Verifica dei risultati di CSQ4IVPX

CSQ4IVPX esegue il programma di utilità CSQUTIL IBM MQ per immettere tre comandi MQSC. Il dataset di output SYSPRINT dovrebbe essere simile a Figura 104 a pagina 900, anche se i dettagli potrebbero differire a seconda degli attributi del gestore code.

- Dovrebbero essere visualizzati i comandi **(1)** ciascuno seguito da diversi messaggi.
- L'ultimo messaggio da ciascun comando deve essere "CSQ9022I ... COMPLETAMENTO NORMALE" **(2)**.
- L'intero lavoro deve essere completato con codice di ritorno zero **(3)**.

```
CSQU000I CSQUTIL IBM MQ for z/OS - V6
CSQU001I CSQUTIL Queue Manager Utility - 2005-05-09 09:06:48
COMMAND
CSQU127I CSQUTIL Executing COMMAND using input from CSQUCMD data set
CSQU120I CSQUTIL Connecting to queue manager CSQ1
CSQU121I CSQUTIL Connected to queue manager CSQ1
CSQU055I CSQUTIL Target queue manager is CSQ1
START CHINIT
(1)
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000004
CSQM138I +CSQ1 CSQMSCHI CHANNEL INITIATOR STARTING
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000000
CSQ9022I +CSQ1 CSQXCRPS ' START CHINIT' NORMAL COMPLETION
(2)
DISPLAY CHINIT
(1)
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000004
CSQM137I +CSQ1 CSQMDDQM DISPLAY CHINIT COMMAND ACCEPTED
CSQN205I  COUNT=   12, RETURN=00000000, REASON=00000000
CSQX830I +CSQ1 CSQXRDQM Channel initiator active
CSQX002I +CSQ1 CSQXRDQM Queue sharing group is QSG1
CSQX831I +CSQ1 CSQXRDQM 8 adapter subtasks started, 8 requested
CSQX832I +CSQ1 CSQXRDQM 5 dispatchers started, 5 requested
CSQX833I +CSQ1 CSQXRDQM 0 SSL server subtasks started, 0 requested
CSQX840I +CSQ1 CSQXRDQM 0 channel connections current, maximum 200
CSQX841I +CSQ1 CSQXRDQM 0 channel connections active, maximum 200,
including 0 paused
CSQX842I +CSQ1 CSQXRDQM 0 channel connections starting,
0 stopped, 0 retrying
CSQX836I +CSQ1 Maximum channels - TCP/IP 200, LU 6.2 200
CSQX845I +CSQ1 CSQXRDQM TCP/IP system name is TCPIP
CSQX848I +CSQ1 CSQXRDQM TCP/IP listener INDISP=QMGR not started
CSQX848I +CSQ1 CSQXRDQM TCP/IP listener INDISP=GROUP not started
CSQX849I +CSQ1 CSQXRDQM LU 6.2 listener INDISP=QMGR not started
CSQX849I +CSQ1 CSQXRDQM LU 6.2 listener INDISP=GROUP not started
CSQ9022I +CSQ1 CSQXCRPS ' DISPLAY CHINIT' NORMAL COMPLETION
(2)
STOP CHINIT
(1)
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000004
CSQM137I +CSQ1 CSQMTCHI STOP CHINIT COMMAND ACCEPTED
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000000
CSQ9022I +CSQ1 CSQXCRPS ' STOP CHINIT' NORMAL COMPLETION
(2)
CSQU057I CSQUCMDS 3 commands read
CSQU058I CSQUCMDS 3 commands issued and responses received, 0 failed
CSQU143I CSQUTIL 1 COMMAND statements attempted
CSQU144I CSQUTIL 1 COMMAND statements executed successfully
CSQU148I CSQUTIL Utility completed, return code=0
(3)
```

Figura 104. Output di esempio da CSQ4IVPX

z/OS Test per programmi C, C + +, COBOL, PL/I e CICS con IBM MQ for z/OS

È possibile eseguire test per C, C + +, COBOL, PL/I o CICS, utilizzando le applicazioni di esempio fornite con IBM MQ.

IVP (CSQ4IVP1) viene fornito come modulo di caricamento e fornisce gli esempi come moduli di origine. È possibile utilizzare questi moduli di origine per verificare diversi ambienti di linguaggio di programmazione.

Per ulteriori informazioni sulle applicazioni di esempio, vedere Programmi di esempio per IBM MQ for z/OS .

z/OS Impostazione delle comunicazioni con altri gestori code su z/OS

Questa sezione descrive le preparazioni IBM MQ for z/OS che è necessario effettuare prima di poter iniziare a utilizzare l'accodamento distribuito.

Informazioni su questa attività

Per definire i requisiti di accodamento distribuito, è necessario definire i seguenti elementi:

- Le procedure e i dataset dell'iniziatore di canali
- Le definizioni di canale
- Le code e altri oggetti
- Sicurezza dell'accesso

Se si utilizzano gruppi di condivisione code, consultare Coda distribuita e gruppi di condivisione code.

Per ulteriori punti da considerare quando ci si prepara a configurare l'accodamento distribuito con IBM MQ for z/OS, consultare “Considerazioni per l'utilizzo dell'accodamento distribuito su z/OS” a pagina 901.

Procedura

Per abilitare l'accodamento distribuito, completare la seguente procedura:

- Personalizzare la funzionalità di accodamento distribuito e definire gli oggetti IBM MQ richiesti come descritto in Definizione degli oggetti di sistema e “Preparazione alla personalizzazione dei gestori code su z/OS” a pagina 822.
- Definire la sicurezza dell'accesso come descritto in Considerazioni sulla sicurezza per l'iniziatore di canali su z/OS .
- Impostare le comunicazioni come descritto in “Impostazione della comunicazione per z/OS” a pagina 922.

Concetti correlati

“Configurazione di IBM MQ for z/OS” a pagina 827
Utilizzare questo argomento come guida dettagliata per personalizzare il sistema IBM MQ for z/OS .

Attività correlate

“Configurazione dell'accodamento distribuito” a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

z/OS Considerazioni per l'utilizzo dell'accodamento distribuito su z/OS

Punti da considerare quando si sta preparando a utilizzare l'accodamento distribuito su z/OS.

Se si utilizzano gruppi di condivisione code, consultare Coda distribuita e gruppi di condivisione code.

Messaggi operatore

Poiché l'iniziatore di canali utilizza un numero di dispatcher che operano in modo asincrono, i messaggi dell'operatore potrebbero verificarsi nel log out della sequenza cronologica.

Comandi operazione canale

I comandi di operazione del canale generalmente coinvolgono due fasi. Una volta verificata la sintassi del comando e verificata l'esistenza del canale, viene inviata una richiesta all'iniziatore del canale. Il messaggio CSQM134I o CSQM137I viene inviato all'emittente del comando per indicare il completamento della prima fase. Quando l'iniziatore del canale ha elaborato il comando, ulteriori messaggi che indicano

l'esito positivo o meno vengono inviati all'emittente del comando insieme al messaggio CSQ9022I o CSQ9023E. Tutti i messaggi di errore generati potrebbero essere inviati anche alla console z/OS .

Tutti i comandi cluster tranne **DISPLAY CLUSQMGR**, tuttavia, funzionano in modo asincrono. I comandi che modificano gli attributi dell'oggetto aggiornano l'oggetto e inviano una richiesta all'iniziatore del canale. I comandi per gestire i cluster vengono controllati per la sintassi e viene inviata una richiesta all'iniziatore di canali. In entrambi i casi, il messaggio CSQM130I viene inviato all'emittente del comando che indica che è stata inviata una richiesta. Questo messaggio è seguito dal messaggio CSQ9022I per indicare che il comando è stato completato correttamente, in quanto è stata inviata una richiesta. Non indica che la richiesta cluster è stata completata correttamente. Le richieste inviate all'iniziatore del canale vengono elaborate in modo asincrono, insieme alle richieste cluster ricevute dagli altri membri del cluster. In alcuni casi, queste richieste devono essere inviate all'intero cluster per determinare se hanno esito positivo o meno. Tutti gli errori vengono notificati a z/OS sul sistema su cui è in esecuzione l'iniziatore di canali. Non vengono inviati all'emittente del comando.

Coda messaggi non recapitati

Un gestore di lettere non recapitate viene fornito con IBM MQ for z/OS. Per ulteriori informazioni, consultare Il programma di utilità gestore code di messaggi non instradabili (CSQUDLQH).

Code in uso

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

Modifiche di sicurezza

Se si modifica l'accesso di sicurezza per un ID utente, la modifica potrebbe non avere effetto immediatamente. Per ulteriori informazioni, consultare Considerazioni sulla sicurezza per l'iniziatore di canali su z/OS , Profili per la sicurezza della codae “Implementare i controlli di sicurezza ESM” a pagina 841.

Comunicazioni arrestate - TCP

Se TCP viene arrestato per qualche motivo e quindi riavviato, il listener TCP IBM MQ for z/OS in attesa su una porta TCP viene arrestato.

La riconnessione automatica del canale consente all'iniziatore del canale di rilevare che TCP/IP non è disponibile e di riavviare automaticamente il listener TCP/IP quando TCP/IP viene restituito. Questo riavvio automatico riduce la necessità per il personale operativo di notare il problema con TCP/IP e riavviare manualmente il listener. Mentre il listener non è attivo, l'iniziatore del canale può essere utilizzato anche per tentare nuovamente il listener all'intervallo specificato da LSTRTMR. Questi tentativi possono continuare fino a quando TCP/IP non ritorna e il listener viene riavviato automaticamente. Per ulteriori informazioni su LSTRTMR, consultare ALTER QMGR e Distributed queuing messages (CSQX ...).

Comunicazioni arrestate - LU6.2

Se APPC viene arrestato, viene arrestato anche il listener. Di nuovo, in questo caso, il listener tenta di nuovo automaticamente all'intervallo LSTRTMR in modo che, se l'APPC viene riavviato, anche il listener può essere riavviato.

Se Db2 ha esito negativo, i canali condivisi che sono già in esecuzione continuano l'esecuzione, ma tutte le nuove richieste di avvio del canale hanno esito negativo. Quando Db2 viene ripristinato, è possibile completare nuove richieste.

z/OS ARM (Automatic Restart Management)

ARM (Automatic Restart Management) è una funzione di ripristino z/OS che può migliorare la disponibilità di lavori batch specifici o di attività avviate (ad esempio, sottosistemi). Può quindi tradursi in una ripresa più rapida del lavoro produttivo.

Per utilizzare ARM, è necessario impostare i gestori code e gli iniziatori di canali in un modo particolare per riavviarli automaticamente. Per ulteriori informazioni, consultare Utilizzo di z/OS ARM (Automatic Restart Manager).

Concetti correlati

"Configurazione di IBM MQ for z/OS" a pagina 827
Utilizzare questo argomento come guida dettagliata per personalizzare il sistema IBM MQ for z/OS .

Attività correlate

"Configurazione dell'accodamento distribuito" a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

z/OS Definizione di oggetti IBM MQ

Utilizzare uno dei metodi di input del comando IBM MQ per definire gli oggetti IBM MQ . Per ulteriori dettagli sulla definizione di questi oggetti, fare riferimento alle informazioni contenute in questo argomento.

Fare riferimento a "Monitoraggio e controllo dei canali su z/OS" a pagina 904 per informazioni sulla definizione degli oggetti.

Code di trasmissione e canali di attivazione

Definire quanto segue:

- Una coda locale con l'utilizzo di XMITQ per ciascun canale di messaggi di invio.
- Definizioni di coda remota.

  Un oggetto coda remota ha tre utilizzi distinti, a seconda del modo in cui il nome e il contenuto vengono specificati:

  – Definizione di coda remota
  – Definizione alias del gestore code
  – Definizione alias coda di risposta

  Questi tre modi vengono mostrati in Tre modi di utilizzare l'oggetto definizione coda remota.

Utilizzare il campo TRIGDATA sulla coda di trasmissione per attivare il canale specificato. Ad esempio:

```
DEFINE QLOCAL(MYXMITQ) USAGE(XMITQ) TRIGGER +
INITQ(SYSTEM.CHANNEL.INITQ) TRIGDATA(MYCHANNEL)
DEFINE CHL(MYCHANNEL) CHLTYPE(SDR) TRPTYPE(TCP) +
XMITQ(MYXMITQ) CONNAME('9.20.9.30(1555)')
```

L'esempio fornito CSQ4INYD fornisce ulteriori esempi delle definizioni necessarie.

z/OS La perdita di connettività alla struttura CF in cui è definita la coda di sincronizzazione per i canali condivisi o problemi simili, potrebbe temporaneamente impedire l'avvio di un canale. Dopo la risoluzione del problema, se si utilizza un tipo di trigger FIRST e il canale non si avvia quando viene attivato, è necessario avviare il canale manualmente. Se si desidera avviare automaticamente i canali attivati dopo la risoluzione del problema, considerare l'impostazione dell'attributo TRIGINT del gestore code su un valore diverso da quello predefinito. L'impostazione dell'attributo TRIGINT su un valore diverso da quello predefinito fa sì che l'iniziatore del canale riprovi ad avviare il canale periodicamente mentre ci sono messaggi nella coda di trasmissione.

Coda di sincronizzazione

DQM richiede una coda da utilizzare con numeri di sequenza e LUWID (logical units of work identifier). È necessario assicurarsi che una coda sia disponibile con il nome SYSTEM.CHANNEL.SYNCQ (vedere Pianificazione su z/OS). Questa coda deve essere disponibile altrimenti l'iniziatore del canale non può essere avviato.

Assicurarsi di definire questa coda utilizzando INDXTYPE (MSGID). Questo attributo migliora la velocità con cui è possibile accedervi.

Code comandi canale

È necessario assicurarsi che esista una coda comandi del canale per il proprio sistema con il nome SYSTEM.CHANNEL.INITQ.

Se l'iniziatore di canali rileva un problema con SYSTEM.CHANNEL.INITQ, non è in grado di continuare normalmente fino a quando il problema non viene corretto. Il problema potrebbe essere uno dei seguenti:

- La coda è piena
- La coda non è abilitata per l'inserimento
- La serie di pagine su cui si trova la coda è piena
- L'iniziatore del canale non dispone dell'autorizzazione di protezione corretta per la coda

Se la definizione della coda viene modificata in GET (DISABLED) mentre l'iniziatore del canale è in esecuzione, l'iniziatore non è in grado di richiamare i messaggi dalla coda e termina.

Avvio dell'iniziatore di canali

L'attivazione è implementata utilizzando l'iniziatore di canali. Su IBM MQ for z/OS, l'iniziatore viene avviato con il comando MQSC `START CHINIT`.

Arresto dell'iniziatore di canali

L'iniziatore di canali viene arrestato automaticamente quando si arresta il gestore code. Se è necessario arrestare l'iniziatore di canali, ma non il gestore code, è possibile utilizzare il comando MQSC `STOP CHINIT`.

z/OS Monitoraggio e controllo dei canali su z/OS

Utilizzare i comandi e i pannelli DQM per creare, monitorare e controllare i canali dei gestori code remoti.

Ogni gestore code z/OS ha un programma DQM (l' *iniziatore di canali*) per il controllo delle interconnessioni ai gestori code remoti utilizzando le funzioni z/OS native.

L'implementazione di questi pannelli e comandi su z/OS è integrata nelle operazioni e nei pannelli di controllo e nei comandi MQSC. Non viene effettuata alcuna differenziazione nell'organizzazione di queste due serie di pannelli e comandi.

È anche possibile immettere comandi utilizzando i comandi PCF (Programmable Command Format). Consultare Automazione delle attività di gestione per informazioni sull'utilizzo di questi comandi.

Le informazioni in questa sezione si applicano in tutti i casi in cui l'iniziatore di canali viene utilizzato per l'accodamento distribuito. Si applica se si utilizzano i gruppi di condivisione code o l'accodamento all'interno del gruppo.

Funzione di controllo del canale DQM

Per una panoramica del modello di gestione code distribuite, consultare “Invio e ricezione di messaggi” a pagina 198.

La funzione di controllo del canale è costituita da pannelli, comandi e programmi, due code di sincronizzazione, code di comando del canale e definizioni di canale. Questo argomento è una breve descrizione dei componenti della funzione di controllo del canale.

- Le definizioni di canale vengono conservate come oggetti nella serie di pagine zero o in Db2, come altri oggetti IBM MQ in z/OS.
- Utilizzare le operazioni e i pannelli di controllo, i comandi MQSC o i comandi PCF per:
  - Creazione, copia, visualizzazione, modifica ed eliminazione di definizioni di canale
  - Avviare e arrestare i listener e gli iniziatori di canali
  - Avviare, arrestare e eseguire il ping dei canali, reimpostare 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
  - Visualizza informazioni su DQM

  In particolare, è possibile utilizzare il dataset di input di inizializzazione CSQINPX per emettere comandi MQSC. Questa serie può essere elaborata ogni volta che si avvia l'iniziatore di canali. Per ulteriori informazioni, consultare Comandi di inizializzazione.
- Esistono due code (SYSTEM.CHANNEL.SYNCQ e SYSTEM.QSG.CHANNEL.SYNCQ) utilizzato per la risincronizzazione del canale. Definire queste code con INDXTYPE (MSGID) per motivi di prestazione.
- La coda comandi del canale (SYSTEM.CHANNEL.INITQ) viene utilizzato per contenere i comandi per gli iniziatori di canali, i canali e i listener.
- Il programma della funzione di controllo del canale viene eseguito nel relativo spazio di indirizzo, separato dal gestore code e comprende l'iniziatore del canale, i listener, gli MCA, il controllo trigger e il gestore comandi.
- Per i gruppi di condivisione code e i canali condivisi, consultare Code condivise e gruppi di condivisione code.
- Per l'accodamento all'interno del gruppo, consultare Accodamento all'interno del gruppo

Gestione dei canali su z/OS

Utilizzare i collegamenti nella tabella seguente per informazioni su come gestire i canali, gli iniziatori di canali e i listener:

Tabella 64. Attività del canale

Attività da eseguire	**Comando MQSC**
Definire un canale	Definire il canale
Modifica di una definizione di canale	MODIFICA CANALE
Visualizzare una definizione di canale	VISUALIZZA CANALE
Eliminare una definizione di canale	Elimina canale
Avviare un iniziatore di canali	INIZIO STRINGA
Arrestare un iniziatore di canali	ARRESTARE CHINIT
Visualizza informazioni sull'iniziatore di canali	VISUALIZZA CHINIT
Avviare un listener del canale	Avvia listener
Arrestare un listener del canale	Arresto del listener
Avviare un canale	Avvio canale
Verifica un canale	Ping canale
Reimpostare i numeri di sequenza dei messaggi per un canale	Reimpostazione canale

Tabella 64. Attività del canale (Continua)	
Attività da eseguire	**Comando MQSC**
Risolvere i messaggi in dubbio su un canale	Risoluzione canale
Arresta un canale	Arresto canale
Visualizza stato canale	VISUALIZZA CHSTATUS
Visualizza canali cluster	VISUALIZZA CLUSQMGR

Concetti correlati

“Utilizzo dei riquadri e dei comandi” a pagina 906
È possibile utilizzare i comandi MQSC, i comandi PCF o le operazioni e i pannelli di controllo per gestire DQM.

“Configurazione di IBM MQ for z/OS” a pagina 827
Utilizzare questo argomento come guida dettagliata per personalizzare il sistema IBM MQ for z/OS .

“Impostazione della comunicazione per z/OS” a pagina 922
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. In questa sezione viene illustrato come definire una connessione.

“Preparazione di IBM MQ for z/OS per DQM con gruppi di condivisione code” a pagina 927
Utilizzare le istruzioni contenute in questa sezione per configurare l'accodamento distribuito con i gruppi di condivisione code su IBM MQ for z/OS.

“Impostazione della comunicazione per IBM MQ for z/OS utilizzando i gruppi di condivisione code” a pagina 931
Quando un canale di gestione dell'accodamento distribuito viene avviato, tenta di utilizzare la connessione specificata nella definizione del canale. Perché questo tentativo abbia esito positivo, è necessario che la connessione sia definita e disponibile.

Attività correlate

“Configurazione dell'accodamento distribuito” a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

“Impostazione delle comunicazioni con altri gestori code su z/OS” a pagina 901
Questa sezione descrive le preparazioni IBM MQ for z/OS che è necessario effettuare prima di poter iniziare a utilizzare l'accodamento distribuito.

z/OS *Utilizzo dei riquadri e dei comandi*

È possibile utilizzare i comandi MQSC, i comandi PCF o le operazioni e i pannelli di controllo per gestire DQM.

Per informazioni sui comandi MQSC, consultare Amministrazione utilizzando i comandi MQSC. Per informazioni sui comandi PCF, consultare Automazione della gestione mediante i comandi Programmable Command Formats.

Utilizzo del pannello iniziale

Per un'introduzione al richiamo delle operazioni e dei pannelli di controllo, utilizzando i tasti funzione e ottenendo assistenza, consultare Amministrazione di IBM MQ for z/OS.

Nota: Per utilizzare le operazioni e i pannelli di controllo, è necessario disporre dell'autorizzazione di protezione corretta; per ulteriori informazioni, consultare Amministrazione di IBM MQ for z/OS e gli argomenti secondari. Figura 105 a pagina 907 mostra il pannello visualizzato quando si avvia una sessione di pannello. Il testo dopo il pannello spiega le azioni eseguite in questo pannello.

```
IBM MQ for z/OS - Main Menu

Complete fields. Then press Enter.

Action . . . . . . . . . . 1   0. List with filter  4. Manage
1. List or Display  5. Perform
2. Define like    6. Start
3. Alter       7. Stop
8. Command
Object type . . . . . . . . CHANNEL    +
Name . . . . . . . . . . . . *
Disposition . . . . . . . . A Q=Qmgr, C=Copy, P=Private, G=Group,
S=Shared, A=All

Connect name . . . . . . . MQ25 - local queue manager or group
Target queue manager . . . MQ25
- connected or remote queue manager for command input
Action queue manager . . . MQ25 - command scope in group
Response wait time . . . . 10  5 - 999 seconds

(C) Copyright IBM Corporation 1993, 2024. All rights reserved.

Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F4=Prompt  F9=SwapNext F10=Messages
F12=Cancel
```

Figura 105. Pannello iniziale di operazioni e controlli

Da questo pannello, è possibile:

- Selezionare l'azione che si desidera eseguire immettendo il numero appropriato nel campo **Azione** .
- Specificare il tipo di oggetto che si desidera gestire. Premere F4 per un elenco di tipi di oggetto se non si è certi della loro natura.
- Visualizza un elenco di oggetti del tipo specificato. Immettere un asterisco (*) nel campo **Nome** e premere Invio per visualizzare un elenco di oggetti (del tipo specificato) già definiti su questo sottosistema. È quindi possibile selezionare uno o più oggetti da gestire in sequenza. Figura 106 a pagina 908 mostra un elenco di canali prodotti in questo modo.
- Specificare la disposizione nel gruppo di condivisione code degli oggetti che si desidera utilizzare nel campo **Disposizione** . La disposizione determina dove viene conservato l'oggetto e come si comporta l'oggetto.
- Scegliere il gestore code locale o il gruppo di condivisione code a cui si desidera connettersi nel campo **Nome connessione** . Se si desidera che i comandi vengano emessi su un gestore code remoto, scegliere il campo **Gestore code di destinazione** o il campo **Gestore code azioni** , a seconda che il gestore code remoto non sia o non sia un membro di un gruppo di condivisione code. Se il gestore code remoto non è un membro di un gruppo di condivisione code, scegliere il campo **Gestore code di destinazione** . Se il gestore code remoto è un membro di un gruppo di condivisione code, scegliere il campo **Gestore code azioni** .
- Scegliere il tempo di attesa per la ricezione delle risposte nel campo **Tempo di attesa risposta** .

```
List Channels - MQ25          Row 1 of 8

Type action codes, then press Enter. Press F11 to display connection status.
1=Display  2=Define like  3=Alter  4=Manage  5=Perform
6=Start   7=Stop

Name         Type     Disposition  Status
<> *           CHANNEL    ALL   MQ25
_  SYSTEM.DEF.CLNTCONN  CLNTCONN   QMGR  MQ25
_  SYSTEM.DEF.CLUSRCVR  CLUSRCVR   QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.CLUSSDR  CLUSSDR    QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.RECEIVER  RECEIVER   QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.REQUESTER REQUESTER   QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.SENDER   SENDER    QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.SERVER   SERVER    QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.SVRCONN  SVRCONN    QMGR  MQ25 INACTIVE
******** End of list ********



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F4=Filter  F5=Refresh  F7=Bkwd
F8=Fwd    F9=SwapNext F10=Messages F11=Status  F12=Cancel
```

Figura 106. Elenco dei canali

z/OS *Definizione di un canale su z/OS*

Su z/OS, è possibile definire un canale utilizzando i comandi MQSC o utilizzando le operazioni e i pannelli di controllo.

Per definire un canale utilizzando i comandi MQSC, utilizzare DEFINE CHANNEL.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	**Valore**
Azione	2 (Definisci come)
Tipo oggetto	tipo di canale (ad esempio SENDER) o CHANNEL
Nome	
Disposizione	L'ubicazione del nuovo oggetto.

Vengono visualizzati alcuni pannelli per completare le informazioni sul nome e gli attributi desiderati per il canale che si sta definendo. Vengono inizializzate con i valori di attributo predefiniti. Modificare le modifiche desiderate prima di premere Invio.

Nota: Se è stato immesso CHANNEL nel campo **`object type`** , viene visualizzato prima il pannello Seleziona un tipo di canale valido.

Se si desidera definire un canale con gli stessi attributi di un canale esistente, inserire il nome del canale che si desidera copiare nel campo **Name** del pannello iniziale. I pannelli vengono inizializzati con attributi dell'oggetto esistente.

Per informazioni sugli attributi del canale, consultare Attributi del canale

Nota:

1. Denominare in modo univoco tutti i canali nella rete. Come mostrato in Diagramma di rete che mostra tutti i canali, inclusi i nomi dei gestori code di origine e di destinazione nel nome del canale è un buon modo per eseguire questa denominazione.

Una volta definito il canale, è necessario proteggere il canale, consultare “Protezione di un canale” a pagina 910

z/OS *Modifica di una definizione di canale*

È possibile modificare una definizione di canale utilizzando i comandi MQSC o le operazioni e i pannelli di controllo.

Per modificare una definizione di canale utilizzando i comandi MQSC, utilizzare ALTER CHANNEL.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	3 (Modifica)
Tipo oggetto	tipo di canale (ad esempio SENDER) o CHANNEL
Nome	CHANNEL.TO.ALTER
Disposizione	L'ubicazione dell'oggetto memorizzato.

Vengono visualizzati alcuni pannelli contenenti informazioni sugli attributi correnti del canale. Modificare i campi non protetti che si desidera sovrascrivendo il nuovo valore, quindi premere Invio per modificare la definizione del canale.

Per informazioni sugli attributi del canale, consultare Attributi del canale.

z/OS *Visualizzazione di una definizione di canale*

È possibile visualizzare una definizione di canale utilizzando i comandi MQSC o utilizzando le operazioni e i pannelli di controllo.

Per visualizzare una definizione di canale utilizzando i comandi MQSC, utilizzare DISPLAY CHANNEL.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	1 (Elenco o Visualizzazione)
Tipo oggetto	tipo di canale (ad esempio SENDER) o CHANNEL
Nome	CHANNEL.TO.DISPLAY
Disposizione	La posizione dell'oggetto.

Vengono visualizzati alcuni pannelli che visualizzano le informazioni sugli attributi correnti del canale.

Per informazioni sugli attributi del canale, consultare Attributi del canale.

z/OS *Eliminazione di una definizione di canale*

È possibile eliminare una definizione di canale utilizzando i comandi MQSC o le operazioni e i pannelli di controllo.

Per eliminare una definizione di canale utilizzando i comandi MQSC, utilizzare DELETE CHANNEL.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	4 (Gestisci)
Tipo oggetto	tipo di canale (ad esempio SENDER) o CHANNEL
Nome	CHANNEL.TO.DELETE
Disposizione	La posizione dell'oggetto.

Viene visualizzato un altro pannello. Selezionare il tipo di funzione 1 su questo pannello.

Premere Invio per eliminare la definizione di canale; viene richiesto di confermare che si desidera eliminare la definizione di canale premendo nuovamente Invio.

Nota: L'iniziatore di canali deve essere in esecuzione prima che una definizione di canale possa essere eliminata (ad eccezione dei canali di connessione client).

z/OS *Visualizzazione delle informazioni sull'iniziatore di canali*

È possibile visualizzare informazioni sull'iniziatore di canali utilizzando i comandi MQSC o utilizzando le operazioni e i pannelli di controllo.

Per visualizzare informazioni sull'iniziatore di canali utilizzando i comandi MQSC, utilizzare DISPLAY CHINIT.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	1 (Visualizzazione)
Tipo oggetto	SYSTEM
Nome	Spazio

Viene visualizzato un altro pannello. Selezionare il tipo di funzione 1 su questo pannello.

Nota:

1. La visualizzazione delle informazioni sull'accodamento distribuito potrebbe richiedere del tempo se si dispone di molti canali.
2. L'iniziatore di canali deve essere in esecuzione prima di poter visualizzare le informazioni sull'accodamento distribuito.

z/OS *Protezione di un canale*

È possibile proteggere un canale utilizzando i comandi MQSC o utilizzando le operazioni e i pannelli di controllo.

Per proteggere un canale utilizzando i comandi MQSC, utilizzare SET CHLAUTH.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	8

Viene visualizzato un editor all'interno del quale è possibile fornire un comando MQSC, in questo caso un comando CHLAUTH, consultare Figura 107 a pagina 910. Una volta terminata l'immissione del comando, sono necessari i segni più (+). Immettere PF3 per uscire dall'editor e inoltrare il comando al server dei comandi.

```
****************************** Top of Data ******************************
000001 SET CHLAUTH(SYSTEM.DEF.SVRCONN) +
000002 TYPE(SSLPEERMAP) +
000003 SSLPEER('CN="John Smith"') +
000004 MCAUSER('PUBLIC')
****** ***************************** Bottom of Data ****************************

Command ===>                          Scroll ===> PAGE
F1=Help   F3=Exit   F4=LineEdit F12=Cancel
```

Figura 107. Voce comando

L'output del comando viene quindi presentato all'utente, consultare Figura 108 a pagina 911

```
****** ***************************** Top of Data ******************************
000001 CSQU000I CSQUTIL IBM MQ for z/OS V7.1.0
000002 CSQU001I CSQUTIL Queue Manager Utility - 2011-04-20 14:42:58
000003 COMMAND TGTQMGR(MQ23) RESPTIME(30)
000004 CSQU127I Executing COMMAND using input from CSQUCMD data set
000005 CSQU120I Connecting to MQ23
000006 CSQU121I Connected to queue manager MQ23
000007 CSQU055I Target queue manager is MQ23
000008 SET CHLAUTH(SYSTEM.DEF.SVRCONN) +
000009 TYPE(SSLPEERMAP) +
000010 SSLPEER('CN="John Smith"') +
000011 MCAUSER('PUBLIC')
000012 CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000000
000013 CSQ9022I !MQ23 CSQMSCA ' SET CHLAUTH' NORMAL COMPLETION
000014 CSQU057I 1 commands read
000015 CSQU058I 1 commands issued and responses received, 0 failed
000016 CSQU143I 1 COMMAND statements attempted
000017 CSQU144I 1 COMMAND statements executed successfully
000018 CSQU148I CSQUTIL Utility completed, return code=0
Command ===>                          Scroll ===> PAGE
F1=Help   F3=Exit   F5=Rfind   F6=Rchange  F9=SwapNext F12=Cancel
```

Figura 108. Output del comando

z/OS *Avvio di iniziatore di canali*

È possibile avviare un iniziatore di canali utilizzando i comandi MQSC o le operazioni e i pannelli di controllo.

Per avviare un iniziatore di canali utilizzando i comandi MQSC, utilizzare START CHINIT.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	**Valore**
Azione	6 (Inizia)
Tipo oggetto	SYSTEM
Nome	Spazio

Viene visualizzato il pannello Avvia una funzione di sistema. Il testo che segue il seguente pannello spiega quale azione intraprendere:

```
Start a System Function

Select function type, complete fields, then press Enter to start system
function.

Function type . . . . . _   1. Channel initiator
2. Channel listener
Action queue manager . . . : MQ25

Channel initiator
JCL substitution . . . . . ________________________________________________
________________________________________

Channel listener
Inbound disposition . . . Q G=Group, Q=Qmgr
Transport type . . . . . _ L=LU6.2, T=TCP/IP
LU name (LU6.2) . . . . . ________________
Port number (TCP/IP) . . . 1414
IP address (TCP/IP) . . . ________________________________________________



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Figura 109. Avvio di una funzione di sistema

Selezionare la funzione tipo 1 (iniziatore di canale) e premere Invio.

z/OS *Arresto di un iniziatore di canali*

È possibile arrestare un iniziatore di canali utilizzando i comandi MQSC o le operazioni e i pannelli di controllo.

Per arrestare un iniziatore di canali utilizzando i comandi di MQSC, utilizzare STOP CHINIT.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	**Valore**
Azione	7 (Arresta)
Tipo oggetto	SYSTEM
Nome	Spazio

Viene visualizzato il pannello Arresta una funzione di sistema. Il testo che segue il pannello spiega come utilizzare questo pannello:

```
Stop a System Function

Select function type, complete fields, then press Enter to stop system
function.

Function type . . . . . _   1. Channel initiator
2. Channel listener
Action queue manager . . . : MQ25

Channel initiator
Restart shared channels  Y Y=Yes, N=No

Channel listener
Inbound disposition . . . Q G=Group, Q=Qmgr
Transport type . . . . . _ L=LU6.2, T=TCP/IP

Port number (TCP/IP) . . . _____
IP address (TCP/IP) . . . ________________________________________________



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Figura 110. Arresto di un controllo funzione

Selezionare la funzione tipo 1 (iniziatore di canale) e premere Invio.

L'iniziatore di canali attende l'arresto di tutti i canali in esecuzione in modalità di sospensione prima di arrestarlo.

Nota: Se alcuni dei canali sono canali riceventi o richiedenti in esecuzione ma non attivi, una richiesta di arresto inoltrata all'iniziatore del canale ricevente o mittente ne determina l'arresto immediato.

Tuttavia, se i messaggi sono in flusso, l'iniziatore di canali attende il completamento del batch corrente di messaggi prima di arrestarlo.

z/OS *Avvio di un listener del canale*

È possibile avviare un listener del canale utilizzando i comandi MQSC o le operazioni e i pannelli di controllo.

Per avviare un listener del canale utilizzando i comandi MQSC, utilizzare START LISTENER.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	6 (Inizia)
Tipo oggetto	SYSTEM
Nome	Spazio

Viene visualizzato il pannello Avvia una funzione di sistema (consultare Figura 109 a pagina 912).

Selezionare il tipo di funzione 2 (listener del canale). Selezionare la disposizione in entrata. Selezionare Tipo di trasporto. Se il tipo di trasporto è L, selezionare il nome LU. Se il tipo di trasporto è T, selezionare il numero di porta e (facoltativamente) l'indirizzo IP. Premere il tasto Invio

Nota: Per il listener TCP/IP, è possibile avviare più combinazioni di porta e indirizzo IP.

z/OS *Arresto di un listener del canale*

È possibile arrestare un listener del canale utilizzando i comandi MQSC o utilizzando le operazioni e i pannelli di controllo.

Per arrestare un listener del canale utilizzando i comandi MQSC, utilizzare STOP LISTENER.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	7 (Arresta)
Tipo oggetto	SYSTEM
Nome	Spazio

Viene visualizzato il pannello Arresta una funzione di sistema (consultare Figura 110 a pagina 913).

Selezionare il tipo di funzione 2 (listener del canale). Selezionare la disposizione in entrata. Selezionare Tipo di trasporto. Se il tipo di trasporto è 'T ', selezionare il numero di porta e (facoltativamente) l'indirizzo IP. Premere il tasto Invio

Nota: Per un listener TCP/IP, è possibile arrestare specifiche combinazioni di porta e indirizzo IP oppure è possibile arrestare tutte le combinazioni.

z/OS *Avvio di un canale*

È possibile avviare un canale utilizzando i comandi MQSC o le operazioni e i pannelli di controllo.

Per avviare un canale utilizzando i comandi MQSC, utilizzare START CHANNEL.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	6 (Inizia)
Tipo oggetto	tipo di canale (ad esempio SENDER) o CHANNEL
Nome	CHANNEL.TO.USE
Disposizione	La disposizione dell'oggetto.

Viene visualizzato il pannello Avvia un canale. Il testo che segue il pannello spiega come utilizzare il pannello:

```
Start a Channel

Select disposition, then press Enter to start channel.


Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE


Disposition . . . . . P   P=Private on MQ25
S=Shared on MQ25
A=Shared on any queue manager









Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Figura 111. Avvio di un canale

Selezionare la disposizione dell'istanza del canale e su quale gestore code deve essere avviato.

Premere Invio per avviare il canale.

z/OS *Avvio di un canale condiviso*

Per avviare un canale condiviso e mantenerlo su un iniziatore di canale designato, utilizzare disposition = S (nel comando START CHANNEL, specificare CHLDISP (FIXSHARED)).

Ci può essere solo un'istanza del canale condiviso in esecuzione alla volta. I tentativi di avviare una seconda istanza del canale hanno esito negativo.

Quando si avvia un canale in questo modo, a tale canale si applicano le regole riportate di seguito:

- È possibile arrestare il canale da qualsiasi gestore code nel gruppo di condivisione code. È possibile arrestarlo anche se l'iniziatore di canali su cui è stato avviato non è in esecuzione al momento dell'emissione della richiesta di arresto del canale. Una volta arrestato il canale, è possibile riavviarlo specificando la disposizione = S (CHLDISP (FIXSHARED)) sullo stesso o su un altro iniziatore di canale. È inoltre possibile avviarlo specificando la disposizione = A (CHLDISP (SHARED)).
- Se il canale è in stato di avvio o di nuovo tentativo, è possibile riavviarlo specificando la disposizione = S (CHLDISP (FIXSHARED)) sullo stesso iniziatore di canale o su un altro iniziatore. È inoltre possibile avviarlo specificando la disposizione = A (CHLDISP (SHARED)).
- Il canale è idoneo per essere avviato quando passa allo stato inattivo. I canali condivisi avviati hanno sempre una disposizione condivisa (CHLDISP (SHARED)).
- Il canale può essere avviato con CHLDISP (FIXSHARED), su qualsiasi iniziatore di canale, quando passa allo stato inattivo. È inoltre possibile avviarlo specificando la disposizione = A (CHLDISP (SHARED)).
- Il canale non viene ripristinato da nessun altro iniziatore di canali attivo nel gruppo di condivisione code quando l'iniziatore di canali su cui è stato avviato viene arrestato con SHARED (RESTART) o quando l'iniziatore di canali termina in modo anomalo. Il canale viene ripristinato solo quando l'iniziatore di canali su cui è stato avviato viene riavviato. Questo arresta i tentativi di ripristino del canale non riusciti passati ad altri iniziatori di canali nel gruppo di condivisione code, che vengono aggiunti al carico di lavoro.

z/OS *Verifica di un canale*

È possibile verificare un canale utilizzando i comandi MQSC o utilizzando le operazioni e i pannelli di controllo.

Per verificare un canale utilizzando i comandi MQSC, utilizzare PING CHANNEL.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	5 (Esegui)
Tipo oggetto	SENDER, SERVER o CHANNEL
Nome	CHANNEL.TO.USE
Disposizione	La disposizione dell'oggetto canale.

Viene visualizzato il pannello Esegui una funzione del canale. Il testo che segue il pannello spiega come utilizzare il pannello:

```
Perform a Channel Function

Select function type, complete fields, then press Enter.


Function type . . . . . _   1. Reset  3. Resolve with commit
2. Ping  4. Resolve with backout

Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE


Disposition . . . . . P   P=Private on MQ25
S=Shared on MQ25
A=Shared on any queue manager

Sequence number for reset . . 1     1 - 999999999
Data length for ping . . . . 16   16 - 32768



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Figura 112. Verifica di un canale

Selezionare il tipo di funzione 2 (ping).

Selezionare la disposizione del canale per cui deve essere eseguita la prova e su quale gestore code deve essere verificata.

La lunghezza dei dati è inizialmente impostata su 16. Modificarla se si desidera e premere Invio.

z/OS *Reimpostazione dei numeri di sequenza dei messaggi per un canale*

È possibile reimpostare i numeri di sequenza dei messaggi per un canale utilizzando i comandi MQSC o le operazioni e i pannelli di controllo.

Per reimpostare i numeri di sequenza del canale utilizzando i comandi MQSC, utilizzare RESET CHANNEL.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	5 (Esegui)
Tipo oggetto	tipo di canale (ad esempio SENDER) o CHANNEL
Nome	CHANNEL.TO.USE

Campo	Valore
Disposizione	La disposizione dell'oggetto canale.

Viene visualizzato il pannello Esegui una funzione del canale (consultare Figura 112 a pagina 916).

Selezionare Tipo di funzione 1 (reimpostazione).

Selezionare la disposizione del canale per cui deve essere eseguita la reimpostazione e su quale gestore code deve essere eseguita.

Il campo **numero sequenza** è inizialmente impostato su uno. Modificare questo valore e premere Invio.

z/OS *Risoluzione dei messaggi in dubbio su un canale*

È possibile risolvere i messaggi in dubbio su un canale utilizzando i comandi MQSC o le operazioni e i pannelli di controllo.

Per risolvere i messaggi in dubbio su un canale utilizzando i comandi MQSC, utilizzare RESOLVE CHANNEL.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	5 (Esegui)
Tipo oggetto	SENDER, SERVER o CHANNEL
Nome	CHANNEL.TO.USE
Disposizione	La disposizione dell'oggetto.

Viene visualizzato il pannello Esegui una funzione del canale (consultare Figura 112 a pagina 916).

Selezionare la funzione di tipo 3 o 4 (risolvere con commit o backout). (Per ulteriori informazioni, consultare “Gestione dei canali in dubbio” a pagina 218 .)

Selezionare la disposizione del canale per il quale deve essere eseguita la risoluzione e su quale gestore code deve essere eseguita. Premere il tasto Invio

z/OS *Arresto di un canale*

È possibile arrestare un canale utilizzando comandi MQSC o utilizzando le operazioni e i pannelli di controllo.

Per arrestare un canale utilizzando i comandi MQSC, utilizzare STOP CHANNEL.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	Valore
Azione	7 (Arresta)
Tipo oggetto	tipo di canale (ad esempio SENDER) o CHANNEL
Nome	CHANNEL.TO.USE
Disposizione	La disposizione dell'oggetto.

Viene visualizzato il pannello Arresta un canale. Il testo che segue il pannello spiega come utilizzare il pannello:

```
Stop a Channel

Complete fields, then press Enter to stop channel.


Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE


Disposition . . . . . P   P=Private on MQ25
A=Shared on any queue manager

Stop mode . . . . . 1   1. Quiesce  2. Force
Stop status . . . . . 1   1. Stopped  2. Inactive

Queue manager . . . . . _________________________________________________
Connection name . . . . . _________________________________________________



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Figura 113. Arresto di un canale

Selezionare la disposizione del canale per cui deve essere eseguito l'arresto e su quale gestore code deve essere arrestato.

Scegliere la modalità di arresto richiesta:

Quiesce
Il canale si arresta quando il messaggio corrente viene completato e il batch viene terminato, anche se il valore della dimensione batch non è stato raggiunto e ci sono messaggi già in attesa nella coda di trasmissione. Non sono stati avviati nuovi batch. La modalità predefinita.

Forza
Il canale si arresta immediatamente. Se è in corso un batch di messaggi, può verificarsi una situazione 'in dubbio'.

Scegliere il gestore code e il nome connessione per il canale che si desidera arrestare.

Scegliere lo stato richiesto:

Arrestato
Il canale non viene riavviato automaticamente e deve essere riavviato manualmente. Questa modalità è quella predefinita se non viene specificato alcun gestore code o nome connessione. Se viene specificato un nome, non è consentito.

Inattivo/a
Il canale viene riavviato automaticamente quando richiesto. Questa modalità è quella predefinita se viene specificato un gestore code o un nome connessione.

Premere Invio per arrestare il canale.

Per ulteriori informazioni, consultare “Arresto e disattivazione dei canali” a pagina 216. Per informazioni sul riavvio dei canali arrestati, consultare “Riavvio dei canali arrestati” a pagina 217.

Nota: Se un canale condiviso è in uno stato di nuovo tentativo e l'iniziatore del canale su cui è stato avviato non è in esecuzione, viene emessa una richiesta STOP per il canale sul gestore code in cui è stato immesso il comando.

z/OS *Visualizzazione dello stato del canale*

È possibile visualizzare lo stato del canale utilizzando i comandi MQSC o utilizzando le operazioni e i pannelli di controllo.

Per visualizzare lo stato di un canale o di una serie di canali utilizzando i comandi MQSC, utilizzare DISPLAY CHSTATUS.

Nota: La visualizzazione delle informazioni sullo stato del canale può richiedere del tempo se si dispone di molti canali.

Utilizzando le operazioni e i pannelli di controllo sul pannello Elenca canale (consultare Figura 106 a pagina 908), viene visualizzato un riepilogo dello stato del canale per ogni canale nel modo seguente:

INACTIVE	Nessuna connessione attiva
stato	Una connessione è attiva
nnn stato	Più di una connessione è corrente e tutte le connessioni correnti hanno lo stesso stato
nnn CORRENTE	Più di una connessione è corrente e le connessioni correnti non hanno tutte lo stesso stato
Spazio	IBM MQ non è in grado di stabilire quante connessioni sono attive (ad esempio, perché l'iniziatore di canali non è in esecuzione) **Nota:** Per gli oggetti canale con la disposizione GROUP, non viene visualizzato alcuno stato.

dove *nnn* è il numero di connessioni attive e *status* è uno dei seguenti:

Inizializzazione	INIZIALIZZAZIONE
BIND	Binding
AVVIA	IN FASE DI AVVIO
ESEGUI	IN ESECUZIONE
ARRESTA	STOPPING o STOPPED
RETRY	Nuovo tentativo in corso
REQST	In fase di richiesta

Per visualizzare ulteriori informazioni sullo stato del canale, premere il tasto Stato (F11) sui pannelli Canale di elenco o Visualizzazione o Modifica canale per visualizzare il pannello Canali di elenco - Stato corrente (consultare Figura 114 a pagina 920).

```
List Channels - Current Status - MQ25      Row 1 of 16

Type action codes, then press Enter. Press F11 to display saved status.
1=Display current status

Channel name     Connection name                 State
Start time      Messages Last message time  Type   Disposition
<> *                           CHANNEL  ALL   MQ25

_ RMA0.CIRCUIT.ACL.F  RMA1                       STOP
_  2005-03-21 10.22.36 557735  2005-03-24 09.51.11 SENDER  PRIVATE MQ25
_ RMA0.CIRCUIT.ACL.N  RMA1
_  2005-03-21 10.23.09 378675  2005-03-24 09.51.10 SENDER  PRIVATE MQ25
_ RMA0.CIRCUIT.CL.F  RMA2
_  2005-03-24 01.12.51 45544   2005-03-24 09.51.08 SENDER  PRIVATE MQ25
_ RMA0.CIRCUIT.CL.N  RMA2
_  2005-03-24 01.13.55 45560   2005-03-24 09.51.11 SENDER  PRIVATE MQ25
_ RMA1.CIRCUIT.CL.F  RMA1
_  2005-03-21 10.24.12 360757  2005-03-24 09.51.11 RECEIVER PRIVATE MQ25
_ RMA1.CIRCUIT.CL.N  RMA1
_  2005-03-21 10.23.40 302870  2005-03-24 09.51.09 RECEIVER PRIVATE MQ25
******** End of list ********
Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F4=Filter  F5=Refresh  F7=Bkwd
F8=Fwd    F9=SwapNext F10=Messages F11=Saved  F12=Cancel
```

Figura 114. Elenco delle connessioni di canale

I valori per lo stato sono i seguenti:

Inizializzazione	INIZIALIZZAZIONE
BIND	Binding
AVVIA	IN FASE DI AVVIO
ESEGUI	IN ESECUZIONE
ARRESTA	STOPPING o STOPPED
RETRY	Nuovo tentativo in corso
REQST	In fase di richiesta
DUBBIO	STOPPED e INDOUBT (YES)

Per ulteriori informazioni, consultare “Stati del canale” a pagina 208.

È possibile premere F11 per visualizzare un elenco simile di connessioni del canale con stato salvato; premere F11 per tornare all'elenco corrente. Lo stato salvato non si applica fino a quando non viene trasmesso almeno un batch di messaggi sul canale.

Utilizzare il codice azione 1 o una barra (/) per selezionare una connessione e premere Invio. Vengono visualizzati i pannelli Display Channel Connection Current Status.

z/OS *Visualizzazione dei canali cluster*

È possibile visualizzare i canali del cluster utilizzando i comandi MQSC o utilizzando le operazioni e i pannelli di controllo.

Per visualizzare tutti i canali cluster che sono stati definiti (esplicitamente o utilizzando la definizione automatica), utilizzare il comando MQSC, DISPLAY CLUSQMGR.

Utilizzando le operazioni e i pannelli di controllo, a partire dal pannello iniziale, completare questi campi e premere Invio:

Campo	**Valore**
Azione	1 (Elenco o Visualizzazione)

Campo	Valore
Tipo oggetto	CLUSCHL
Nome	*

Viene visualizzato un pannello come la figura Figura 115 a pagina 921, in cui le informazioni per ciascun canale cluster occupano tre righe e includono i relativi nomi di canale, cluster e gestore code. Per i canali mittente del cluster, viene mostrato lo stato generale.

```
List Cluster queue manager Channels - MQ25    Row 1 of 9

Type action codes, then press Enter. Press F11 to display connection status.
1=Display  5=Perform  6=Start  7=Stop

Channel name     Connection name                State
Type     Cluster name                   Suspended
Cluster queue manager name            Disposition
<>   *                          -    MQ25
_ TO.MQ90.T      HURSLEY.MACH90.COM(1590)
_  CLUSRCVR   VJH01T                        N
_   MQ90                       -    MQ25
_ TO.MQ95.T      HURSLEY.MACH95.COM(1595)             RUN
_  CLUSSDRA   VJH01T                        N
_   MQ95                       -    MQ25
_ TO.MQ96.T      HURSLEY.MACH96.COM(1596)             RUN
_  CLUSSDRB   VJH01T                        N
_   MQ96                       -    MQ25
******** End of list ********


Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F4=Filter  F5=Refresh  F7=Bkwd
F8=Fwd    F9=SwapNext F10=Messages F11=Status  F12=Cancel
```

Figura 115. Elenco dei canali cluster

Per visualizzare informazioni complete su uno o più canali, immettere il codice azione 1 rispetto ai relativi nomi e premere Invio. Utilizzare i codici azione 5, 6 o 7 per eseguire funzioni (come ping, risoluzione e ripristino) e avviare o arrestare un canale cluster.

Per visualizzare ulteriori informazioni sullo stato del canale, premere il pulsante Stato (F11).

z/OS *Preparazione di IBM MQ for z/OS all'utilizzo della funzione zEnterprise Data Compression Express*

La funzione zEnterprise Data Compression (zEDC) Express è disponibile per determinati modelli di macchine IBM Z , a partire da IBM zEC12 GA2, utilizzando un z/OS livello minimo di z/OS 2.1.

Consultare zEnterprise Data Compression (zEDC) per ulteriori informazioni.

Prerequisiti

Per IBM z15 e versioni successive, la funzione zEnterprise Data Compression (zEDC) Express è stata spostata da una funzione facoltativa nel cassetto I/O PCIe del sistema hardware come Integrated Accelerator per zEDC. Con questa modifica, i prerequisiti di configurazione vengono aggiornati e dipendono dal sistema hardware.

IBM z15 o successive

Applicare una delle seguenti PTF in base al proprio livello di z/OS:

- z/OS 2.4: UJ00636
- z/OS 2.3: UJ00635

- z/OS 2.2: UJ00638
- z/OS 2.1: UJ00639

Non esistono requisiti hardware per z15 o sistemi successivi. La soluzione Integrated Accelerator for zEDC in questi sistemi fornisce l'accelerazione dei dati integrata, in modo che non sia più necessario un adattatore separato.

IBM zEC12 GA2 a IBM z14

Il sistema deve avere anche i requisiti seguenti:

- Un adattatore zEDC Express ®, installato nei cassetti I/O PCIe del sistema hardware.
- La funzionalità software zEDC (una funzione facoltativa a pagamento) deve essere abilitata in un membro parmlib IFAPRDxx.

Procedura

IBM zEC12 GA2 per IBM z14

Assicurarsi che l'ID utente iniziatore di canali disponga dell'autorità READ per FPZ.ACCELERATOR.COMPRESSION in RACF FACILITY CLASS o l'equivalente in ESM (external security manager) utilizzato dall'azienda.

Attenzione: Non richiesto per IBM z15 o versioni successive.

IBM zEnterprise zEC12 GA2 o successivo

Configurare il canale con COMPMSG (ZLIBFAST) sia all'estremità di invio che a quella di ricezione. Una volta configurata, la compressione zlib viene utilizzata per comprimere e decomprimere i messaggi che attraversano il canale.

La compressione viene eseguita in zEDC quando la dimensione dei dati da comprimere è superiore alla soglia minima. La soglia dipende dall'hardware IBM z utilizzato

- IBM zEC12 GA2 to IBM z14 ha una soglia minima di 4KB
- IBM z15 o successivo ha una soglia minima di 1KB

Per i messaggi al di sotto della dimensione della soglia, la compressione o l'inflazione vengono eseguite nel software.

z/OS Impostazione della comunicazione per z/OS

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. In questa sezione viene illustrato come definire una connessione.

DQM è una funzione di accodamento remoto per IBM MQ. Fornisce programmi di controllo del canale per il gestore code che formano l'interfaccia per i collegamenti di comunicazione. Questi collegamenti sono controllabili dall'operatore di sistema. Le definizioni di canale gestite dalla gestione dell'accodamento distribuito utilizzano queste connessioni.

Scegliere una delle due forme di protocollo di comunicazione che possono essere utilizzate per z/OS:

- “Definizione di un collegamento TCP su z/OS” a pagina 923
- “Definizione di una connessione LU6.2 per z/OS utilizzando APPC / MVS” a pagina 926

MQ Adv. CD V 9.1.4 Un canale messaggi che utilizza TCP/IP può essere puntato a IBM Aspera fasp.io Gateway, che utilizza un tunnel TCP/IP veloce, in grado di aumentare notevolmente la velocità di trasmissione della rete. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux. Consultare Definizione di una connessione Aspera gateway su Linux.

Ogni definizione di canale deve specificare solo un protocollo come attributo del protocollo di trasmissione (Tipo di trasporto). Un gestore code può utilizzare più di un protocollo per comunicare.

Potrebbe essere utile anche fare riferimento a Configurazione di esempio - IBM MQ for z/OS . Se si utilizzano gruppi di condivisione code, consultare “Impostazione della comunicazione per IBM MQ for z/OS utilizzando i gruppi di condivisione code” a pagina 931.

Concetti correlati

“Utilizzo dei riquadri e dei comandi” a pagina 906
È possibile utilizzare i comandi MQSC, i comandi PCF o le operazioni e i pannelli di controllo per gestire DQM.

“Configurazione di IBM MQ for z/OS” a pagina 827
Utilizzare questo argomento come guida dettagliata per personalizzare il sistema IBM MQ for z/OS .

“Monitoraggio e controllo dei canali su z/OS” a pagina 904
Utilizzare i comandi e i pannelli DQM per creare, monitorare e controllare i canali dei gestori code remoti.

“Preparazione di IBM MQ for z/OS per DQM con gruppi di condivisione code” a pagina 927
Utilizzare le istruzioni contenute in questa sezione per configurare l'accodamento distribuito con i gruppi di condivisione code su IBM MQ for z/OS.

“Impostazione della comunicazione per IBM MQ for z/OS utilizzando i gruppi di condivisione code” a pagina 931
Quando un canale di gestione dell'accodamento distribuito viene avviato, tenta di utilizzare la connessione specificata nella definizione del canale. Perché questo tentativo abbia esito positivo, è necessario che la connessione sia definita e disponibile.

Attività correlate

“Configurazione dell'accodamento distribuito” a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

“Impostazione delle comunicazioni con altri gestori code su z/OS” a pagina 901
Questa sezione descrive le preparazioni IBM MQ for z/OS che è necessario effettuare prima di poter iniziare a utilizzare l'accodamento distribuito.

z/OS *Definizione di un collegamento TCP su z/OS*

Per definire una connessione TCP, è necessario configurare diverse impostazioni.

Il nome dello spazio di indirizzo TCP deve essere specificato nel dataset dei parametri di sistema TCP, *tcpip*.TCPIP.DATA. Nel dataset, è necessario includere un'istruzione "TCPIPJOBNAME *TCPIP_proc*" .

Se si utilizza un Firewall, è necessario configurare le connessioni `allow` dall'iniziatore di canali agli indirizzi nei canali e dalle connessioni remote nel gestore code.

Di solito, la definizione per un firewall configura l'indirizzo IP di invio e la porta all'indirizzo IP di destinazione e alla porta:

- Un'immagine z/OS può avere più di un nome host e potrebbe essere necessario configurare il firewall con più indirizzi host come indirizzo di origine.

  È possibile utilizzare il comando NETSTAT HOME per visualizzare questi nomi e indirizzi.
- Un iniziatore di canali può disporre di più listener su porte differenti, quindi è necessario configurare queste porte.
- Se si utilizza una porta condivisa per un gruppo di condivisione code, è necessario configurare anche la porta condivisa.

Lo spazio di indirizzo dell'iniziatore di canali deve avere l'autorità per leggere il data set. Le tecniche seguenti possono essere utilizzate per accedere al TCPIP TCPIP.DATA , a seconda del prodotto TCP/IP e dell'interfaccia che si sta utilizzando:

- Variabile di ambiente, RESOLVER_CONFIG
- /etc/resolv.conf sul file system
- // istruzione SYSTCPD DD
- // istruzione SYSTCPDD DD
- *jobname/userid*.TCPIP.DATA
- SYS1.TCPPARMS(TCPDATA)
- *zapname*.TCPIP.DATA

È inoltre necessario prestare attenzione a specificare correttamente il qualificatore di alto livello per TCP/IP.

È necessario un server DNS (Domain Name System) configurato in modo appropriato, in grado di eseguire la conversione da nome a indirizzo IP e da indirizzo IP a nome.

Nota: Alcune modifiche alla configurazione del resolver richiedono un nuovo ciclo di applicazioni che lo utilizzano, ad esempio IBM MQ.

Per ulteriori informazioni, consultare quanto segue:

- Sistema TCP/IP di base
- z/OS UNIX System Services.

Ogni canale TCP quando viene avviato utilizza le risorse TCP; potrebbe essere necessario modificare i seguenti parametri nel proprio profilo PROFILE.TCPIP :

ACBPOOLSIZE
Aggiungi uno per canale TCP avviato, più uno

CCBPOOLSIZE
Aggiungere uno per canale TCP avviato, più uno per dispatcher DQM, più uno

DIMENSIONEPOOLBUFFER
Aggiungi due per canale TCP avviato, più uno

PROCFILEMAX
Controlla il numero di canali che ciascun dispatcher nell'iniziatore di canali può gestire.

Questo parametro viene specificato nel membro BPXPRMxx di SYSI.PARMLIB. Accertarsi di specificare un valore sufficientemente grande per le proprie esigenze.

Per impostazione predefinita, l'iniziatore di canali è in grado di eseguire il bind solo agli indirizzi IP associati con lo stack denominato nell'attributo del gestore code TCPNAME. Per consentire all'iniziatore di canali di comunicare utilizzando ulteriori stack TCP/IP sul sistema, modificare l'attributo del gestore code TCPSTACK in MULTIPLE.

MQ Adv. CD V 9.1.4 Un canale messaggi che utilizza TCP/IP può essere puntato a IBM Aspera fasp.io Gateway, che utilizza un tunnel TCP/IP veloce, in grado di aumentare notevolmente la velocità di trasmissione della rete. Un gestore code in esecuzione su qualsiasi piattaforma CD autorizzata può connettersi tramite un Aspera gateway. Il gateway stesso è distribuito su Red Hat o Ubuntu Linux. Consultare Definizione di una connessione Aspera gateway su Linux.

Concetti correlati

“Fine invio” a pagina 925
All'estremità di invio della connessione TCP/IP, vi sono diverse impostazioni da configurare.

“Ricezione su TCP” a pagina 925
All'estremità di ricezione della connessione TCP/IP, vi sono diverse impostazioni da configurare.

“Utilizzo dell'opzione backlog del listener TCP” a pagina 925
Quando si riceve su TCP/IP, viene impostato un numero massimo di richieste di connessione in sospeso. Queste richieste in sospeso possono essere considerate un *backlog* di richieste in attesa sulla porta TCP/IP affinché il listener accetti la richiesta.

z/OS *Fine invio*

All'estremità di invio della connessione TCP/IP, vi sono diverse impostazioni da configurare.

Il campo del nome della connessione (CONNAME) nella definizione del canale deve essere impostato sul nome host (ad esempio MVSHUR1) o sull'indirizzo di rete TCP della destinazione. L'indirizzo di rete TCP può essere in formato decimale puntato IPv4 (ad esempio, 127.0.0.1) o esadecimale IPv6 (ad esempio, 2001:DB8:0:0:0:0:0:0). Se il nome della connessione è un nome host, è necessario un server dei nomi TCP per convertire il nome host in un indirizzo host TCP. (Questo requisito è una funzione di TCP, non IBM MQ.)

All'estremità iniziale di una connessione (tipi di canale mittente, richiedente e server) è possibile fornire un numero di porta facoltativo per la connessione, ad esempio:

Nome connessione
192.0.2.0(1555)

In questo caso, l'estremità di inizializzazione tenta di collegarsi ad un programma ricevente in ascolto sulla porta 1555.

Nota: Il numero di porta predefinito 1414 viene utilizzato se non viene specificato un numero di porta facoltativo.

L'iniziatore di canali può utilizzare qualsiasi stack TCP/IP attivo e disponibile. Per impostazione predefinita, l'iniziatore del canale collega i propri canali in uscita all'indirizzo IP predefinito per lo stack TCP/IP denominato nell'attributo del gestore code TCPNAME. Per connettersi tramite uno stack differente, è necessario specificare il nome host o l'indirizzo IP dello stack nell'attributo LOCLADDR del canale.

z/OS *Ricezione su TCP*

All'estremità di ricezione della connessione TCP/IP, vi sono diverse impostazioni da configurare.

I programmi del canale ricevente vengono avviati in risposta a una richiesta di avvio dal canale mittente. Per fare ciò, è necessario avviare un programma listener per rilevare le richieste di rete in entrata e avviare il canale associato. Avviare questo programma listener con il comando START LISTENER oppure utilizzando le operazioni e i pannelli di controllo.

Per impostazione predefinita:

- Il programma TCP Listener utilizza la porta 1414 ed è in ascolto su tutti gli indirizzi disponibili per lo stack TCP.
- I listener TCP/IP possono collegarsi solo agli indirizzi associati allo stack TCP/IP denominato nell'attributo del gestore code TCPNAME.

Per avviare i listener per altri indirizzi o per tutti gli stack TCP disponibili, impostare l'attributo del gestore code TCPSTACK su 'MULTIPLE'.

È possibile avviare il programma listener TCP per ascoltare solo un indirizzo specifico o un nome host specificando IPADDR nel comando START LISTENER. Per ulteriori informazioni, consultare Listener.

z/OS *Utilizzo dell'opzione backlog del listener TCP*

Quando si riceve su TCP/IP, viene impostato un numero massimo di richieste di connessione in sospeso. Queste richieste in sospeso possono essere considerate un *backlog* di richieste in attesa sulla porta TCP/IP affinché il listener accetti la richiesta.

Il valore di backlog del listener predefinito su z/OS è 10000. Se il backlog raggiunge questi valori, la connessione TCP/IP viene rifiutata e il canale non è in grado di avviarsi.

Per i canali MCA, ciò fa sì che il canale entri in uno stato RETRY e ritenti la connessione in seguito.

Per le connessioni client, il client riceve un codice motivo MQRC_Q_MGR_NOT_AVAILABLE da MQCONN e può ritentare la connessione in un secondo momento.

z/OS *Definizione di una connessione LU6.2 per z/OS utilizzando APPC / MVS*

Per definire una connessione LU6.2 è necessario configurare una serie di impostazioni.

Impostazione APPC/MVS

Ogni istanza dell'iniziatore di canali deve avere il nome del LU che deve utilizzare definito per APPC/MVS, nel membro APPCPMxx di SYS1.PARMLIB, come nel seguente esempio:

```
LUADD ACBNAME( luname ) NOSCHED TPDATA(CSQ.APPCTP)
```

luname è il nome dell'unità logica da utilizzare. NOSCHED è obbligatorio; TPDATA non viene utilizzato. Non è necessaria alcuna aggiunta al membro ASCHPMxx o al dataset del profilo TP APPC/MVS.

Il dataset delle informazioni lato deve essere esteso per definire le connessioni utilizzate da DQM. Consultare l'esempio fornito CSQ4SIDE per dettagli su come eseguire questa operazione utilizzando il programma di utilità APPC ATBSDFMU. Per i dettagli dei valori TPNAME da utilizzare, consultare la seguente tabella per informazioni:

Tabella 65. Impostazioni sul sistema z/OS locale per una piattaforma del gestore code remoto

Piattaforma remota	**TPNAME**
z/OS o MVS	Lo stesso di TPNAME nelle informazioni laterali corrispondenti sul gestore code remoto.
IBM i	Uguale al valore di confronto nella specifica di instradamento sul sistema IBM i .
Sistemi UNIX and Linux	Lo stesso di TPNAME nelle informazioni laterali corrispondenti sul gestore code remoto.
Windows	Come specificato nel comando Windows Esegui listener o nel programma di transazione richiamabile definito utilizzando TpSetup su Windows.

Se si dispone di più di un gestore code sulla stessa macchina, verificare che i nomi TP nelle definizioni di canale siano univoci.

Consultare il manuale *Multiplatform APPC Configuration Guide* anche per informazioni sulle definizioni VTAM che potrebbero essere richieste.

In un ambiente in cui il gestore code comunica utilizzando APPC con un gestore code sullo stesso o su un altro sistema z/OS , verificare che la definizione VTAM per la LU di comunicazione specifichi SECACPT (ALREADYV) o che esista un profilo RACF APPCLU per la connessione tra LU, che specifica CONVSEC (ALREADYV).

Il comando z/OS VARY ACTIVE deve essere emesso per entrambe le LU di base e listener prima di tentare di avviare le comunicazioni in entrata o in uscita.

Attenzione: Oltre alla configurazione APPC, è necessario immettere il seguente comando:

```
ALTER QMGR LUNAME(luname)
```

e riavviare l'iniziatore del canale.

Per ulteriori informazioni, consultare LUNAME .

Concetti correlati

“Connessione a LU 6.2” a pagina 927
Per connettersi alla LU 6.2, è necessario configurare una serie di impostazioni.

“Ricezione su LU 6.2” a pagina 927
Per ricevere su LU 6.2, è necessario configurare un determinato numero di impostazioni.

z/OS *Connessione a LU 6.2*

Per connettersi alla LU 6.2, è necessario configurare una serie di impostazioni.

Il campo del nome della connessione (CONNAME) nella definizione di canale deve essere impostato sul nome di destinazione simbolico, come specificato nel dataset delle informazioni laterali per APPC / MVS.

Il nome LU da utilizzare (definito per APPC/MVS come descritto precedentemente) deve essere specificato anche nei parametri dell'iniziatore di canali. Deve essere impostato sulla stessa LU utilizzata per la ricezione dal listener.

L'iniziatore di canali utilizza l'opzione "SECURITY (SAME)" APPC/MVS, quindi è l'ID utente dello spazio di indirizzo dell'iniziatore di canali utilizzato per le trasmissioni in uscita e viene presentato al destinatario.

z/OS *Ricezione su LU 6.2*

Per ricevere su LU 6.2, è necessario configurare un determinato numero di impostazioni.

Gli MCA di ricezione vengono avviati in risposta a una richiesta di avvio dal canale di invio. Per fare ciò, è necessario avviare un programma listener per rilevare le richieste di rete in entrata e avviare il canale associato. Il programma listener è un server APPC / MVS. Avviarlo con il comando START LISTENER o utilizzando le operazioni e i pannelli di controllo. È necessario specificare il nome LU da utilizzare con un nome di destinazione simbolico definito nel dataset delle informazioni lato. La LU locale così identificata deve essere la stessa utilizzata per le trasmissioni in uscita, come impostata nei parametri dell'iniziatore di canali.

z/OS Preparazione di IBM MQ for z/OS per DQM con gruppi di condivisione code

Utilizzare le istruzioni contenute in questa sezione per configurare l'accodamento distribuito con i gruppi di condivisione code su IBM MQ for z/OS.

Per una configurazione di esempio utilizzando i gruppi di condivisione code, vedere Configurazione di esempio - IBM MQ for z/OS utilizzo dei gruppi di condivisione code. Per un esempio di pianificazione del canale dei messaggi utilizzando i gruppi di condivisione code, consultare Esempio di pianificazione del canale dei messaggi per z/OS utilizzo dei gruppi di condivisione code.

È possibile creare e configurare i seguenti componenti per abilitare l'accodamento distribuito con i gruppi di condivisione code:

- LU 6.2 e listener TCP/IP
- Code di trasmissione e trigger
- Agente canale dei messaggi (MCA, message channel agent)
- Coda di sincronizzazione

Una volta creati i componenti necessari per configurare le comunicazioni, consultare “Impostazione della comunicazione per IBM MQ for z/OS utilizzando i gruppi di condivisione code” a pagina 931.

Per informazioni su come monitorare e controllare i canali quando si utilizzano i gruppi di condivisione code, consultare “Monitoraggio e controllo dei canali su z/OS” a pagina 904.

Consultare le seguenti sezioni per i concetti e i vantaggi del gruppo di condivisione code.

Classe di servizio

Una coda condivisa è un tipo di coda locale che offre una diversa classe di servizio. I messaggi su una coda condivisa vengono memorizzati in una CF (coupling facility), che consente a tutti i gestori code nel gruppo di condivisione code di accedervi. Un messaggio su una coda condivisa deve essere un messaggio di lunghezza non superiore a 100 MB.

Interfaccia generica

Un gruppo di condivisione code ha un'interfaccia generica che permette alla rete di visualizzare il gruppo come una singola entità. Questa vista si ottiene con un singolo indirizzo generico che può essere utilizzato per connettersi a qualsiasi gestore code all'interno del gruppo.

Ogni gestore code nel gruppo di condivisione code è in attesa di richieste di sessione in ingresso su un indirizzo logicamente correlato all'indirizzo generico. Per ulteriori informazioni, fare riferimento a "Listener LU 6.2 e TCP/IP per i gruppi di condivisione code" a pagina 929.

Avvio canale con bilanciamento del carico

Una coda di trasmissione condivisa può essere servita da un canale in uscita in esecuzione su qualsiasi iniziatore di canale nel gruppo di condivisione code. L'avvio del canale con bilanciamento del carico determina la destinazione di un comando di avvio del canale. Viene scelto un iniziatore di canali appropriato che abbia accesso al sottosistema di comunicazioni necessario. Ad esempio, un canale definito con TRPTYPE (LU6.2) non può essere avviato su un iniziatore di canali che ha accesso solo ad un sottosistema TCP/IP.

La scelta dell'iniziatore di canali dipende dal carico del canale e dalla capacità dell'iniziatore di canali. Il carico del canale è il numero di canali attivi come una percentuale del numero massimo di canali attivi consentiti come definiti nei parametri dell'iniziatore del canale. L'headroom è la differenza tra il numero di canali attivi e il numero massimo consentito.

I canali condivisi in entrata possono essere bilanciati in base al carico nel gruppo di condivisione code utilizzando un indirizzo generico, come descritto in "Listener LU 6.2 e TCP/IP per i gruppi di condivisione code" a pagina 929.

Ripristino canale condiviso

La seguente tabella mostra i tipi di errore del canale condiviso e la modalità di gestione di ciascun tipo.

Tipo di errore	**Cosa succede:**
Errore del sottosistema delle comunicazioni dell'iniziatore di canali	I canali dipendenti dal sottosistema di comunicazioni immettono un nuovo tentativo di canale e vengono riavviati su un iniziatore di canale del gruppo di condivisione code appropriato da un comando di avvio con bilanciamento del carico.
Errore iniziatore canale	L'iniziatore del canale non riesce, ma il gestore code associato rimane attivo. Il gestore code controlla l'errore e avvia l'elaborazione del recupero.
Errore del gestore code	Il gestore code ha esito negativo (errore dell'iniziatore di canali associato). Altri gestori code nel gruppo di condivisione code controllano l'evento e avviano il recupero peer.
Errore di stato condiviso	Le informazioni sullo stato del canale sono memorizzate in Db2, quindi una perdita di connessione a Db2 diventa un errore quando si verifica una modifica dello stato del canale. I canali in esecuzione possono continuare l'esecuzione senza accedere alle risorse. In caso di accesso non riuscito a Db2, il canale immette un nuovo tentativo.

L'elaborazione del ripristino del canale condiviso per conto di un sistema non riuscito richiede la connettività a Db2 per essere disponibile sul sistema che gestisce il ripristino per recuperare lo stato del canale condiviso.

Canali client

I canali di connessione client possono beneficiare dell'alta disponibilità dei messaggi nei gruppi di condivisione code connessi all'interfaccia generica invece di essere connessi a un gestore code specifico. Per ulteriori informazioni, vedi Canali di connessione client.

Concetti correlati

Code condivise e gruppi di condivisione code

"Configurazione di IBM MQ for z/OS" a pagina 827
Utilizzare questo argomento come guida dettagliata per personalizzare il sistema IBM MQ for z/OS .

"Cluster e gruppi di condivisione code" a pagina 931
È possibile rendere la coda condivisa disponibile per un cluster in una singola definizione. Per eseguire questa operazione, specificare il nome del cluster quando si definisce la coda condivisa.

"Canali e serializzazione" a pagina 931
Durante il ripristino peer della coda condivisa, gli agent canale dei messaggi che elaborano i messaggi sulle code condivise serializzano il loro accesso alle code.

Accodamento all'interno del gruppo

Attività correlate

"Configurazione dell'accodamento distribuito" a pagina 176
Questa sezione fornisce informazioni più dettagliate sull'intercomunicazione tra installazioni IBM MQ , incluse la definizione della coda, la definizione del canale, il trigger e le procedure del punto di sincronizzazione

"Impostazione delle comunicazioni con altri gestori code su z/OS" a pagina 901
Questa sezione descrive le preparazioni IBM MQ for z/OS che è necessario effettuare prima di poter iniziare a utilizzare l'accodamento distribuito.

z/OS *Listener LU 6.2 e TCP/IP per i gruppi di condivisione code*

Il gruppo LU 6.2 e i listener TCP/IP sono in ascolto su un indirizzo collegato logicamente all'indirizzo generico.

Per il listener LU 6.2 , il LUGROUP specificato viene associato alla risorsa generica VTAM associata al gruppo di condivisione code. Per un esempio di impostazione di questa tecnologia, consultare "Definizione di una connessione LU6.2 per z/OS utilizzando APPC / MVS" a pagina 926.

Per il listener TCP/IP, la porta specificata può essere connessa all'indirizzo generico in uno dei seguenti modi:

- Per un router front - end come IBM Network Dispatcher, le richieste di connessione in entrata vengono inoltrate dal router ai membri del gruppo di condivisione code.
- Per il distributore Sysplex TCP/IP, a ogni listener in esecuzione e in ascolto su un particolare indirizzo impostato come DVIPA distribuito viene assegnata una proporzione delle richieste in entrata. Per un esempio di impostazione di questa tecnologia, consultare Utilizzo del distributore Sysplex

z/OS *Code di trasmissione e trigger per i gruppi di condivisione code*

Una coda di trasmissione condivisa viene utilizzata per memorizzare i messaggi prima che vengano spostati dal gruppo di condivisione code alla destinazione.

Si tratta di una coda condivisa ed è accessibile a tutti i gestori code del gruppo di condivisione code.

Triggering

Una coda condivisa attivata può generare più di un messaggio trigger per una condizione trigger soddisfatta. Esiste un messaggio trigger generato per ogni coda di iniziazione locale definita su un gestore code nel gruppo di condivisione code associato alla coda condivisa attivata.

Per l'accodamento distribuito, ogni iniziatore di canali riceve un messaggio trigger per una condizione di trigger della coda di trasmissione condivisa soddisfatta. Tuttavia, solo un iniziatore di canali elabora effettivamente l'avvio attivato e gli altri hanno esito negativo in modo sicuro. Il canale attivato viene

quindi avviato con un avvio bilanciato del carico (consultare “Preparazione di IBM MQ for z/OS per DQM con gruppi di condivisione code” a pagina 927) che viene attivato per avviare il canale QSG.TO.QM2. Per creare una coda di trasmissione condivisa, utilizzare i comandi IBM MQ (MQSC) come mostrato nel seguente esempio:

```
DEFINE QLOCAL(QM2) DESCR('Transmission queue to QM2') +
USAGE(XMITQ) QSGDISP(SHARED) +
CFSTRUCT(APPLICATION1) INITQ(SYSTEM.CHANNEL.INITQ) +
TRIGGER TRIGDATA(QSG.TO.QM2)
```

Nota: Se una coda condivisa è impostata per l'attivazione e la connessione alla CF (Coupling Facility) che ospita la coda condivisa viene persa, è possibile che venga generato un evento trigger e che venga inserito un messaggio nella coda di iniziazione. Ciò può verificarsi anche quando nessun messaggio è stato inserito nella configurazione della coda condivisa originale per l'attivazione. Ciò è causato dalla sovraindicazione dei bit da parte della macro IXLVECTR come documentato in Il vettore di notifica elenco.

z/OS *Agent canale dei messaggi per i gruppi di condivisione code*

Un canale può essere avviato su un iniziatore di canali solo se ha accesso a una definizione di canale per un canale con quel nome.

Un MCA (message channel agent) è un programma IBM MQ che controlla l'invio e la ricezione di messaggi. Gli agenti del canale dei messaggi spostano i messaggi da un gestore code ad un altro; esiste un agente del canale dei messaggi ad ogni estremità di un canale.

Una definizione di canale può essere definita come privata per un gestore code o memorizzata nel repository condiviso e disponibile ovunque (una definizione di gruppo). Ciò significa che un canale definito dal gruppo è disponibile su qualsiasi iniziatore di canali nel gruppo di condivisione code.

Nota: La copia privata della definizione del gruppo può essere modificata o eliminata.

Per creare definizioni di canali di gruppo, utilizzare i comandi IBM MQ (MQSC) come mostrato nei seguenti esempi:

```
DEFINE CHL(QSG.TO.QM2) CHLTYPE(SDR) +
TRPTYPE(TCP) CONNAME(QM2.MACH.IBM.COM) +
XMITQ(QM2) QSGDISP(GROUP)
```

```
DEFINE CHL(QM2.TO.QSG) CHLTYPE(RCVR) TRPTYPE(TCP) +
QSGDISP(GROUP)
```

Esistono due prospettive da cui esaminare gli agent del canale messaggi utilizzati per l'accodamento distribuito con i gruppi di condivisione code:

In entrata

Un canale in entrata è un canale condiviso se è connesso al gestore code tramite il listener del gruppo. Viene connesso tramite l'interfaccia generica al gruppo di condivisione code, quindi viene indirizzato a un gestore code all'interno del gruppo o viene indirizzato alla porta del gruppo di un gestore code specifico o al nome luname utilizzato dal listener del gruppo.

In uscita

Un canale in uscita è un canale condiviso se sposta i messaggi da una coda di trasmissione condivisa. Nei comandi di esempio, il canale mittente QSG.TO.QM2 è un canale condiviso poiché la relativa coda di trasmissione, QM2 è definita con QSGDISP (SHARED).

z/OS *Coda di sincronizzazione per i gruppi di condivisione code*

I canali condivisi hanno la propria coda di sincronizzazione condivisa denominata SYSTEM.QSG.CHANNEL.SYNCQ.

Questa coda di sincronizzazione è accessibile a qualsiasi membro del gruppo di condivisione code. (I canali privati continuano a utilizzare la coda di sincronizzazione privata. Consultare “Definizione di oggetti IBM MQ” a pagina 903). Ciò significa che il canale può essere riavviato su un gestore code e un'istanza dell'iniziatore di canali diversi all'interno del gruppo di condivisione code in caso di malfunzionamento del sottosistema di comunicazioni, dell'iniziatore di canali o del gestore code. Per ulteriori informazioni, fare riferimento a “Preparazione di IBM MQ for z/OS per DQM con gruppi di condivisione code” a pagina 927.

DQM con gruppi di condivisione code richiede che una coda condivisa sia disponibile con il nome SYSTEM.QSG.CHANNEL.SYNCQ. Questa coda deve essere disponibile affinché un listener di gruppo possa essere avviato correttamente.

Se un listener di gruppo ha esito negativo perché la coda non era disponibile, è possibile definire la coda e riavviare il listener senza riavviare l'iniziatore del canale. I canali non condivisi non sono interessati.

Assicurarsi di definire questa coda utilizzando INDXTYPE (MSGID). Questa definizione migliora la velocità con cui è possibile accedere ai messaggi sulla coda.

z/OS *Cluster e gruppi di condivisione code*

È possibile rendere la coda condivisa disponibile per un cluster in una singola definizione. Per eseguire questa operazione, specificare il nome del cluster quando si definisce la coda condivisa.

Gli utenti nella rete vedono la coda condivisa come ospitata da ciascun gestore code all'interno del gruppo di condivisione code. (La coda condivisa non viene indicata come ospitata dal gruppo di condivisione code). I client possono avviare sessioni con tutti i membri del gruppo di condivisione code per inserire i messaggi nella stessa coda condivisa.

Per ulteriori informazioni, consultare “Configurazione di un cluster di gestore code” a pagina 275.

z/OS *Canali e serializzazione*

Durante il ripristino peer della coda condivisa, gli agent canale dei messaggi che elaborano i messaggi sulle code condivise serializzano il loro accesso alle code.

Se un gestore code in un gruppo di condivisione code ha esito negativo mentre un agent del canale dei messaggi sta gestendo messaggi senza commit su una o più code condivise, il canale e l'iniziatore del canale associato termineranno e il ripristino peer della coda condivisa avrà luogo per il gestore code.

Poiché il ripristino peer della coda condivisa è un'attività asincrona, il ripristino del canale peer potrebbe tentare di riavviare simultaneamente il canale in un'altra parte del gruppo di condivisione code prima del completamento del ripristino peer della coda condivisa. Se si verifica questo evento, i messaggi di cui è stato eseguito il commit potrebbero essere elaborati prima dei messaggi ancora in fase di recupero. Per assicurarsi che i messaggi non vengano elaborati fuori sequenza in questo modo, gli agent del canale dei messaggi che elaborano i messaggi sulle code condivise serializzano il proprio accesso a queste code.

Un tentativo di avviare un canale per il quale è ancora in corso il ripristino peer della coda condivisa potrebbe causare un errore. Viene emesso un messaggio di errore che indica che il ripristino è in corso e che il canale è in stato di nuovo tentativo. Una volta completato il ripristino peer del gestore code, il canale può essere riavviato al momento del successivo tentativo.

Un tentativo di RESOLVE, PING o DELETE di un canale può non riuscire per lo stesso motivo.

z/OS *Impostazione della comunicazione per IBM MQ for z/OS utilizzando i gruppi di condivisione code*

Quando un canale di gestione dell'accodamento distribuito viene avviato, tenta di utilizzare la connessione specificata nella definizione del canale. Perché questo tentativo abbia esito positivo, è necessario che la connessione sia definita e disponibile.

Scegli una delle due forme di protocollo di comunicazione che possono essere utilizzate:

- TCP
- LU 6.2 tramite APPC / MVS

Potrebbe essere utile fare riferimento a Configurazione di esempio - IBM MQ for z/OS utilizzando i gruppi di condivisione code.

z/OS *Definizione di una connessione TCP per i gruppi di condivisione code*

Per definire una connessione TCP per un gruppo di condivisione code, è necessaria la configurazione di alcuni attributi sull'estremità di invio e ricezione.

Per informazioni sull'impostazione del TCP, consultare “Definizione di un collegamento TCP su z/OS” a pagina 923.

Fine invio

Il campo del nome della connessione (CONNAME) nella definizione del canale per connettersi al gruppo di condivisione code deve essere impostato sull'interfaccia generica del gruppo di condivisione code (consultare Gruppi di condivisione code). Per ulteriori dettagli, fare riferimento a Utilizzo del distributore Sysplex.

Ricezione su TCP utilizzando un gruppo di condivisione code

I programmi di ricezione del canale condiviso vengono avviati in risposta a una richiesta di avvio dal canale mittente. Per fare ciò, è necessario avviare un listener per rilevare le richieste di rete in entrata e avviare il canale associato. Questo programma listener viene avviato con il comando START LISTENER, utilizzando la disposizione in entrata del gruppo o utilizzando le operazioni e i pannelli di controllo.

Tutti i listener di gruppo nel gruppo di condivisione code devono essere in ascolto sulla stessa porta. Se si dispone di più di un iniziatore di canali in esecuzione su una singola immagine MVS, è possibile definire indirizzi IP virtuali e avviare il programma listener TCP per ascoltare solo un indirizzo specifico o un nome host specificando IPADDR nel comando START LISTENER. (Per ulteriori informazioni, consultare START LISTENER.)

z/OS *Definizione di una connessione LU 6.2 su z/OS*

Per definire una connessione LU 6.2 per un gruppo di condivisione code, è necessaria la configurazione di alcuni attributi sull'estremità di invio e ricezione.

Per informazioni sull'impostazione di APPC/MVS, consultare Impostazione della comunicazione per z/OS .

Connessione a APPC/MVS (LU 6.2)

Il campo del nome della connessione (CONNAME) nella definizione del canale per la connessione al gruppo di condivisione code deve essere impostato sul nome di destinazione simbolico, come specificato nel dataset di informazioni lato per APPC/MVS. La LU partner specificata in questa destinazione simbolica deve essere il nome risorsa generico. Per ulteriori dettagli, vedi Definizione di te stesso sulla rete utilizzando risorse generiche.

Ricezione su LU 6.2 utilizzando un'interfaccia generica

La ricezione di MCA condivisi viene avviata in risposta a una richiesta di avvio dal canale di invio. Per fare ciò, è necessario avviare un programma listener di gruppo per rilevare le richieste di rete in entrata e avviare il canale associato. Il programma listener è un server APPC / MVS. Avviarlo con il comando START LISTENER, utilizzando un gruppo di disposizione in entrata o utilizzando le operazioni e i pannelli di controllo. È necessario specificare il nome LU per utilizzare un nome di destinazione simbolico definito nel dataset delle informazioni lato. Per ulteriori dettagli, vedi Definizione di te stesso sulla rete utilizzando risorse generiche.

z/OS Utilizzo di IBM MQ con IMS

L'adattatore IBM MQ -IMS e il bridge IBM MQ - IMS sono i due componenti che consentono a IBM MQ di interagire con IMS.

Per configurare IBM MQ e IMS per l'utilizzo congiunto, è necessario completare le seguenti attività:

- “Impostazione dell'adattatore IMS” a pagina 933
- “Impostazione del bridge IMS” a pagina 939

Concetti correlati

IBM MQ e IMS

“Utilizzo di IBM MQ con CICS” a pagina 941
Per utilizzare IBM MQ con CICS, è necessario configurare l'adattatore IBM MQ CICS e, facoltativamente, i componenti IBM MQ CICS bridge .

“Utilizzo delle uscite OTMA in IMS” a pagina 943
Utilizzare questo argomento se si desidera utilizzare le uscite IMS Open Transaction Manager Access con IBM MQ for z/OS.

Applicazioni bridge IMS e IMS su IBM MQ for z/OS

Attività correlate

“Configurazione dei gestori code su z/OS” a pagina 821
Utilizzare queste istruzioni per configurare i gestori code su IBM MQ for z/OS.

Riferimenti correlati

“Aggiornamento e applicazione del servizio a Language Environment o z/OS Callable Services” a pagina 941
Le azioni che è necessario eseguire variano a seconda che si utilizzi CALLLIBS o LINK e la versione di SMP/E.

z/OS Impostazione dell'adattatore IMS

Per utilizzare IBM MQ all'interno di IMS è necessario l'adattatore IBM MQ - IMS (generalmente indicato come adattatore IMS).

Questo argomento indica come rendere l'adattatore IMS disponibile per il proprio sottosistema IMS . Se non si ha dimestichezza con la personalizzazione di un sottosistema IMS , consultare le *IMS informazioni in IBM Documentation*.

Per rendere l'adattatore IMS disponibile per le applicazioni IMS , effettuare le seguenti operazioni:

1. Definire IBM MQ in IMS come sottosistema esterno utilizzando l'ESAF (external subsystem attach facility) IMS .

   Consultare “Definizione di IBM MQ in IMS” a pagina 935.
2. Includere la IBM MQ libreria di caricamento thlqual.SCSQAUTH nella concatenazione JOBLIB o STEPLIB nel JCL per la propria regione di controllo IMS e per qualsiasi regione dipendente che si connette a IBM MQ (se non si trova nell'elenco LPA o link). Se JOBLIB o STEPLIB non è autorizzato, includerlo anche nella concatenazione DFS dopo la libreria che contiene i moduli IMS (di solito IMS RESLIB).

   Includere anche thlqual.SCSQANLx (dove x è la lettera della lingua).

   Se DFSESL è presente, SCSQAUTH e SCSQANLx devono essere inclusi nella concatenazione o aggiunti a LNKLIST. L'aggiunta alla concatenazione STEPLIB o JOBLIB nel JCL non è sufficiente.
3. Copiare il programma assembler IBM MQ CSQQDEFV da thlqual.SCSQASMS in una libreria utente.
4. Il programma fornito, CSQQDEFV, contiene un nome sottosistema CSQ1 identificato come predefinito con un LIT (language interface token) IMS di MQM1. È possibile conservare questo nome per il test e la verifica dell'installazione.

   Per i sottosistemi di produzione, modificare NAME=CSQ1 con il proprio nome sottosistema oppure utilizzare CSQ1. È possibile aggiungere ulteriori definizioni di sottosistema come richiesto. Consultare “Definizione di gestori code IBM MQ sull'adattatore IMS” a pagina 938 per ulteriori informazioni sui LIT.

5. Assemblare e collegare il programma per produrre il modulo di caricamento CSQQDEFV. Per l'assembly, includere la libreria thlqual.SCSQMACS nella concatenazione SYSLIB; utilizzare il parametro link - edit RENT. Ciò viene mostrato nel JCL di esempio in thlqual.SCSQPROC(CSQ4DEFV).
6. Includere la libreria utente contenente il modulo CSQQDEFV creato nella concatenazione JOBLIB o STEPLIB nel JCL per qualsiasi regione dipendente che si connette a IBM MQ. Inserire questa libreria prima di SCSQAUTH perché SCSQAUTH ha un modulo di caricamento predefinito. Se non si esegue questa operazione, si riceverà una fine anomala dell'utente 3041 da IMS.
7. Se l'adattatore IMS rileva un errore IBM MQ imprevisto, emette un dump SNAP z/OS nel nome DD CSQSNAP ed emette il codice motivo MQRC_UNEXPECTED_ERROR per l'applicazione. Se l'istruzione CSQSNAP DD non si trovava nel JCL della regione dipendente IMS , non viene eseguito alcun dump. In questo caso, è possibile includere l'istruzione CSQSNAP DD nel JCL ed eseguire nuovamente l'applicazione. Tuttavia, poiché alcuni problemi potrebbero essere intermittenti, si consiglia di includere l'istruzione CSQSNAP DD per catturare il motivo dell'errore nel momento in cui si verifica.
8. Se si desidera utilizzare le chiamate IBM MQ dinamiche (descritte in Chiamata dinamica dello IBM MQ stub), creare lo stub dinamico, come mostrato in Figura 116 a pagina 934.
9. Se si desidera utilizzare il controllo trigger IMS , definire l'applicazione di controllo trigger IMS CSQQTRMN ed eseguire PSBGEN e ACBGEN. Consultare “Impostazione del controllo dei trigger IMS” a pagina 939.
10. Se si utilizza RACF per proteggere le risorse nella classe OPERCMDS, assicurarsi che l'id utente associato allo spazio di indirizzo del gestore code IBM MQ disponga dell'autorizzazione per emettere il comando MODIFY su qualsiasi sistema IMS a cui potrebbe connettersi.

```
//DYNSTUB EXEC PGM=IEWL,PARM='RENT,REUS,MAP,XREF'
//SYSPRINT DD  SYSOUT=*
//ACSQMOD  DD  DISP=SHR,DSN=thlqual.SCSQLOAD
//IMSLIB   DD  DISP=SHR,DSN=ims.reslib
//SYSLMOD  DD  DISP=SHR,DSN=private.load¹
//SYSUT1   DD  UNIT=SYSDA,SPACE=(CYL,1)
//SYSLIN   DD  *
  INCLUDE ACSQMOD(CSQQSTUB)
  INCLUDE IMSLIB(DFSLI000)
  ALIAS MQCONN,MQCONNX,MQDISC             MQI entry points
  ALIAS MQGET,MQPUT,MQPUT1                MQI entry points
  ALIAS MQOPEN,MQCLOSE                    MQI entry points
  ALIAS MQBACK,MQCMIT                     MQI entry points
  ALIAS CSQBBAK,CSQBCMT                   MQI entry points
  ALIAS MQINQ,MQSET                       MQI entry points
  ALIAS DFSPLI,PLITDLI                    IMS entry points
  ALIAS DFSCOBOL,CBLTDLI                  IMS entry points
  ALIAS DFSFOR,FORTDLI                    IMS entry points
  ALIAS DFSASM,ASMTDLI                    IMS entry points
  ALIAS DFSPASCL,PASTDLI                  IMS entry points
  ALIAS DFHEI01,DFHEI1                    IMS entry points
  ALIAS DFSAIBLI,AIBTDLI                  IMS entry points
  ALIAS DFSESS,DSNWLI,DSNHLI              IMS entry points
  ALIAS MQCRTMH,MQDLTMH,MQDLTMP           IMS entry points
  ALIAS MQINQMP,MQSETMP,MQMHBUF,MQBUFMH   IMS entry points
  MODE AMODE(31),RMODE(24)                Note RMODE setting
  NAME CSQQDYNS(R)
/*

¹Specify the name of a library accessible to IMS applications that
want to make dynamic calls to IBM MQ.
```

Figura 116. JCL di esempio per collegare - modificare lo stub della chiamata dinamica

Concetti correlati

IBM MQ e IMS

“Impostazione del bridge IMS” a pagina 939

Il bridge IBM MQ - IMS è un componente facoltativo che abilita IBM MQ all'input e all'output da e verso programmi e transazioni esistenti che non sono abilitati a IBM MQ.

z/OS *Definizione di IBM MQ in IMS*

IBM MQ deve essere definito nella regione di controllo IMS e in ogni regione dipendente che accede a tale gestore code IBM MQ . A tale scopo, è necessario creare un membro del sottosistema (SSM) in IMS.PROCLIB e identificare l'SSM per le regioni IMS applicabili.

Inserimento della voce del membro del sistema secondario in IMS.PROCLIB

Ogni voce SSM in IMS.PROCLIB definisce una connessione da una regione IMS a un gestore code differente.

Per denominare un SSM, concatenare il valore (da uno a quattro caratteri alfanumerici) del campo ID IMSdella macro IMS IMSCTRL con qualsiasi nome (da uno a quattro caratteri alfanumerici) definito dal proprio sito.

Un SSM può essere condiviso da tutte le regioni IMS , oppure è possibile definire un membro specifico per ciascuna regione. Questo membro contiene tante voci quante sono le connessioni ai sottosistemi esterni. Ogni voce è un record di 80 caratteri.

Parametri di posizione

I campi in questa voce sono:

```
SSN,LIT,ESMT,RTT,REO,CRC
```

dove:

SSN
Specifica il nome del gestore code IBM MQ . È obbligatorio e deve contenere da uno a quattro caratteri.

LIT
Specifica il LIT (language interface token) fornito a IMS. Questo campo è obbligatorio, il suo valore deve corrispondere ad uno nel modulo CSQQDEFV.

ESMT
Specifica la tabella ESMT (external subsystem module table). Questa tabella specifica quali moduli allegati devono essere caricati da IMS. CSQQESMT è il valore richiesto per questo campo.

RTT
Questa opzione non è supportata da IBM MQ.

REO
Specifica l'opzione di errore della regione (REO) da utilizzare se un'applicazione IMS fa riferimento a un sottosistema esterno non operativo o se le risorse non sono disponibili al momento della creazione del thread. Questo campo è facoltativo e contiene un singolo carattere, che può essere:

R
Inoltra un codice di ritorno all'applicazione, indicando che la richiesta per i servizi IBM MQ non è riuscita.

Q
Termina l'applicazione con un codice di abend U3051, ripristina l'attività all'ultimo punto di commit, esegue un PSTOP della transazione e riaccoda il messaggio di input. Questa opzione si applica solo quando un'applicazione IMS tenta di fare riferimento a un sottosistema esterno non operativo o se le risorse non sono disponibili al momento della creazione del thread.

I codici di completamento e di errore IBM MQ vengono restituiti all'applicazione se il problema IBM MQ si verifica mentre IBM MQ sta elaborando la richiesta; vale a dire, dopo che l'adattatore ha inoltrato la richiesta a IBM MQ.

A

Termina l'applicazione con un codice di interruzione U3047 ed elimina il messaggio di input. Questa opzione si applica solo quando un'applicazione IMS fa riferimento a un sistema secondario esterno non operativo o se le risorse non sono disponibili al momento della creazione del thread.

I codici di completamento e di errore IBM MQ vengono restituiti all'applicazione se il problema IBM MQ si verifica mentre IBM MQ sta elaborando la richiesta; vale a dire, dopo che l'adattatore ha inoltrato la richiesta a IBM MQ.

CRC

Questa opzione può essere specificata ma non è utilizzata da IBM MQ.

Nota: Per i dettagli completi di tutti i parametri posizionali, fare riferimento a Modalità di specifica dei sottosistemi esterni in IMS.

Una voce SSM di esempio è:

```
CSQ1,MQM1,CSQQESMT,,R,
```

dove:

CSQ1	Il nome del sottosistema predefinito fornito con IBM MQ. È possibile modificarlo per adattarlo alla propria installazione.
MQM1	La LIT predefinita fornita in CSQQDEFV.
CSQQESMT	Il nome del modulo del sottosistema esterno. È necessario utilizzare questo valore.
R	Opzione REO.

Parametri parola chiave

I parametri IBM MQ possono essere specificati in formato parola chiave. Il parametro SST può avere un valore di DB2 o MQ. Il supporto per il valore MQ è stato aggiunto in IMS 14. L'utilizzo di MQ aiuta la chiarezza e il comando del sottosistema IMS ora include il valore SST, ma in caso contrario non ha alcun effetto significativo. Se necessario, è ancora possibile utilizzare il valore DB2 . Altri parametri sono quelli descritti in Parametri posizionalie mostrati nel seguente esempio:

```
SST=MQ,SSN=SYS3,LIT=MQM3,ESMT=CSQQESMT
```

dove:

SYS3	Il nome del sottosistema
MQM3	La LIT fornita in CSQQDEFV
CSQQESMT	Il nome del modulo del sottosistema esterno

Specifica del parametro EXEC SSM

Specificare il parametro SSM EXEC nella procedura di avvio della control region IMS . Questo parametro specifica il nome del membro del sottosistema da un carattere a quattro caratteri (SSM).

Se si specifica l'SSM per la control region IMS , qualsiasi regione dipendente in esecuzione nella control region può collegarsi al gestore code IBM MQ denominato in IMS.Membro PROCLIB specificato dal parametro SSM. Il IMS.Il nome del membro PROCLIB è l'ID IMS (IMSID= *xxxx*) concatenato con uno o quattro caratteri specificati nel parametro EXEC SSM. L'ID IMS è il parametro ID IMSdella macro di generazione IMSCTRL.

IMS consente di definire il numero di connessioni del sottosistema esterno richiesto. È possibile definire più di una connessione per gestori code IBM MQ differenti. Tutte le connessioni IBM MQ devono trovarsi nello stesso sistema z/OS . Per una regione dipendente, è possibile specificare un SSM della regione dipendente oppure utilizzare quello specificato per la regione di controllo. È possibile specificare diverse opzioni di errore regione (REO) nell'SSM della regione dipendente e nell'SSM della regione di controllo. Tabella 66 a pagina 937 mostra le diverse possibilità delle specifiche SSM.

Tabella 66. Opzioni specifiche SSM

SSM per control region	**SSM per la regione dipendente**	**Azione**	**Commenti**
No	No	Nessuno	Non è possibile collegare alcun sottosistema esterno.
No	Sì	Nessuno	Non è possibile collegare alcun sottosistema esterno.
Sì	No	Utilizza SSM (control region)	Le applicazioni pianificate nella regione possono accedere ai sottosistemi esterni identificati nella regione di controllo SSM. Le uscite e i blocchi di controllo per ciascun collegamento vengono caricati nella control region e negli spazi di indirizzo della region dipendente.
Sì	Sì (vuoto)	Non viene utilizzato alcun SSM per la regione dipendente	Le applicazioni pianificate in questa regione possono accedere solo ai database DL/I. Le uscite e i blocchi di controllo per ogni allegato vengono caricati nello spazio di indirizzo della control region.
Sì	Sì (non vuoto)	Controllare l'SSM della regione dipendente con l'SSM della regione di controllo	Le applicazioni pianificate in questa regione possono accedere solo ai sottosistemi esterni identificati in entrambi gli SSM. Le uscite e i blocchi di controllo per ciascun collegamento vengono caricati nella control region e negli spazi di indirizzo della region dipendente.

Non esiste alcun parametro specifico per controllare il numero massimo di possibilità di specifica SSM.

Precaricamento dell'adattatore IMS

Le prestazioni dell'adattatore IMS possono essere migliorate se è precaricato da IMS. Il precaricamento è controllato dal membro DFSMPLxx di IMS.PROCLIB: consultare " IMS Guida all'amministrazione: Sistema " per ulteriori informazioni. I nomi modulo IBM MQ da specificare sono:

CSQACLST	CSQAMLST	CSQAPRH	CSQAVICM	SSQFSALM	CSQQDEFV
CSQQCONN	DISCOQSQC	CSQQTERM	CSQQINIT	CSQQBACK	CSQQCMMT
CSQQESMT	CSQQPREP	CSQQTTHD	ATTESQSQC	CSQQNORM	CSQQSSOF
CSQQSSON	CSQFSTAB	CSQQRESV	CSQQSNOP	CSQQCMND	CSQQCVER
IDTMQSQC	CSQQTRGI	CSQQCON2	CSQBPAPI	CSQBCRMH	CSQBAPPL

Per ulteriori informazioni sull'utilizzo di IBM MQ classes for JMS, consultare Utilizzo di IBM MQ classes for JMS in IMS IMS.

Le release correnti dei moduli IMS supportano il precaricamento IBM MQ dalle librerie di formato PDS-E solo nelle regioni MPP, BMP, IFP, JMP e JBP. Qualsiasi altro tipo di regione IMS non supporta il

precaricamento dalle librerie PDS - E. Se il precaricamento è richiesto per qualsiasi altro tipo di regione, i moduli IBM MQ forniti devono essere copiati in una libreria in formato PDS.

z/OS *Definizione di gestori code IBM MQ sull'adattatore IMS*

I nomi dei gestori code IBM MQ e i relativi LIT (language interface token) corrispondenti devono essere definiti nella tabella di definizione del gestore code.

Utilizzare la macro CSQQDEFX fornita per creare il modulo di caricamento CSQQDEFV. Figura 117 a pagina 938 mostra la sintassi di questa macro assembler.

```
CSQQDEFX TYPE=ENTRY|DEFAULT,NAME=qmgr-name,LIT=token
or
CSQQDEFX TYPE=END
```

Figura 117. Sintassi macro CSQQDEFX

Parametri

TIPO=VOCE | PREDEFINITO
Specificare TYPE=ENTRY o TYPE=DEFAULT come segue:

TIPO=VOCE
Specifica che deve essere generata una voce di tabella che descrive un gestore code IBM MQ disponibile per un'applicazione IMS . Se questa è la prima voce, viene generata anche l'intestazione della tabella, inclusa un'istruzione CSECT CSQQDEFV.

TIPO=PREDEFINITO
Come per TYPE=ENTRY. Il gestore code specificato è il gestore code predefinito da utilizzare quando MQCONN o MQCONNX specifica un nome che è vuoto. Nella tabella deve essere presente una sola voce di questo tipo.

NAME= *nome - qmg*
Specifica il nome del gestore code, come specificato con **MQCONN** o **MQCONNX**.

LIT = token
Specifica il nome della LIT (language interface token) che IMS utilizza per identificare il gestore code.

Una chiamata MQCONN o MQCONNX associa il parametro di input *name* e il parametro di output *hconn* con l'etichetta del nome e, quindi, la LIT nella voce CSQQDEFV. Ulteriori chiamate IBM MQ che passano il parametro *hconn* utilizzano la LIT dalla voce CSQQDEFV identificata nella chiamata MQCONN o MQCONNX per indirizzare le chiamate al gestore code IBM MQ definito nel membro IMS SSM PROCLIB con la stessa LIT.

In sintesi, il parametro **name** sulla chiamata a MQCONN o MQCONNX identifica una LIT in CSQQDEFV e la stessa LIT nel membro SSM identifica un gestore code IBM MQ . (Per informazioni sulla chiamata MQCONN , fare riferimento a MQCONN - Connetti gestore code. Per informazioni sulla chiamata MQCONNX , consultare MQCONNX - Connect queue manager (extended).)

TIPO=FINE
Specifica che la tabella è completa. Se questo parametro viene omesso, viene assunto TYPE=ENTRY.

Utilizzo della macro CSQQDEFX

Figura 118 a pagina 939 mostra il layout generale di una tabella di definizione del gestore code.

```
CSQQDEFX NAME=subsystem1,LIT=token1
CSQQDEFX NAME=subsystem2,LIT=token2,TYPE=DEFAULT
CSQQDEFX NAME=subsystem3,LIT=token3
...
CSQQDEFX NAME=subsystemN,LIT=tokenN
CSQQDEFX TYPE=END
END
```

Figura 118. Layout di una tabella di definizione del gestore code

z/OS *Impostazione del controllo dei trigger IMS*

È possibile impostare un programma IMS batch - oriented per monitorare una coda di iniziazione IBM MQ .

Definire l'applicazione per IMS utilizzando il Modello CSQQTAPL nella libreria thlqual.SCSQPROC (consultare Esempio di definizione della transazione per CSQQTRMN).

Generare PSB e ACB utilizzando il modello CSQQTPSB nella libreria thlqual.SCSQPROC (consultare Esempio di definizione PSB per CSQQTRMN).

```
*  This is the application definition *
*  for the IMS Trigger Monitor BMP    *

APPLCTN PSB=CSQQTRMN,
PGMTYPE=BATCH,
SCHDTYP=PARALLEL
```

Figura 119. Definizione di transazione di esempio per CSQQTRMN

```
PCB  TYPE=TP,      ALTPCB for transaction messages
MODIFY=YES,        To "triggered" IMS transaction
PCBNAME=CSQQTRMN
PCB  TYPE=TP,      ALTPCB for diagnostic messages
MODIFY=YES,        To LTERM specified or "MASTER"
PCBNAME=CSQQTRMG,
EXPRESS=YES
PSBGEN LANG=ASSEM,
PSBNAME=CSQQTRMN,  Runs program CSQQTRMN
CMPAT=YES
```

Figura 120. Definizione PSB di esempio per CSQQTRMN

Per ulteriori informazioni sull'avvio e l'arresto del controllo trigger IMS , consultare Controllo del controllo trigger IMS.

z/OS Impostazione del bridge IMS

Il bridge IBM MQ - IMS è un componente facoltativo che abilita IBM MQ all'input e all'output da e verso programmi e transazioni esistenti che non sono abilitati a IBM MQ.

Questo argomento descrive le operazioni da effettuare per personalizzare il bridge IBM MQ - IMS .

Definire i parametri XCF e OTMA per IBM MQ.

Questo passo definisce il gruppo XCF e i nomi dei membri per il proprio sistema IBM MQ e altri parametri OTMA. IBM MQ e IMS devono appartenere allo stesso gruppo XCF. Utilizzare la parola chiave OTMACON della macro CSQ6SYSP per adattare questi parametri nel modulo di caricamento dei parametri di sistema.

Per ulteriori informazioni, consultare Utilizzo di CSQ6SYSP .

Definire i parametri XCF e OTMA in IMS.
Questa fase definisce il gruppo XCF e i nomi dei membri per il sistema IMS . IMS e IBM MQ devono appartenere allo stesso gruppo XCF.

Aggiungere i seguenti parametri al proprio elenco di parametri IMS , nel proprio JCL o nel membro DFSPBxxx in IMS PROCLIB:

OTMA=Y
Questo avvia automaticamente OTMA quando IMS viene avviato. (È facoltativo, se si specifica OTMA=N è anche possibile avviare OTMA immettendo il comando IMS /START OTMA.)

GRNAME=
Questo parametro fornisce il nome del gruppo XCF.

È uguale al nome del gruppo specificato nella definizione della classe di memoria (vedere il passo successivo) e nel parametro **Group** della parola chiave OTMACON della macro CSQ6SYSP .

OTMANM=
Questo parametro fornisce il nome del membro XCF del sistema IMS .

È uguale al nome del membro specificato nella definizione della classe di memoria (consultare il passo successivo).

Comunicare a IBM MQ il gruppo XCF e il nome del membro del sistema IMS .
Viene specificato dalla classe di memoria di una coda. Se si desidera inviare messaggi attraverso il bridge IBM MQ - IMS , è necessario specificarlo quando si definisce la classe di memoria per la coda. Nella classe di memorizzazione, è necessario definire il gruppo XCF e il nome membro del sistema IMS di destinazione. Per effettuare questa operazione, utilizzare le operazioni IBM MQ e i pannelli di controllo oppure utilizzare i comandi IBM MQ come descritto in Introduzione ai formati di comando programmabili.

Impostare la protezione richiesta.
Il comando /SECURE OTMA IMS determina il livello di sicurezza da applicare a **ogni** IBM MQ gestore code che si connette a IMS tramite OTMA. Per ulteriori informazioni, consultare Considerazioni sulla sicurezza per l'utilizzo di IBM MQ con IMS .

Aggiunta di una connessione IMS aggiuntiva allo stesso gestore code

Per aggiungere una connessione IMS allo stesso gestore code, è necessario:

- Definire una seconda classe di archiviazione STGCLASS per puntare al nuovo IMS; per ulteriori informazioni, consultare DEFINE STGCLASS .
- Aggiungere una nuova coda locale per puntare alla seconda classe di memoria.

Importante:

- Una coda locale non può puntare a due classi di memoria.
- Una classe di memoria non può puntare a due bridge IMS .
- IBM MQ e IMS devono appartenere allo stesso gruppo XCF. Utilizzare la parola chiave OTMACON della macro CSQ6SYSP per adattare questi parametri nel modulo di caricamento dei parametri di sistema.

  Per ulteriori informazioni, consultare Utilizzo di CSQ6SYSP .

Concetti correlati
IBM MQ e IMS
“Impostazione dell'adattatore IMS” a pagina 933
Per utilizzare IBM MQ all'interno di IMS è necessario l'adattatore IBM MQ - IMS (generalmente indicato come adattatore IMS).

Applicazioni bridge IMS e IMS su IBM MQ for z/OS

z/OS Utilizzo di IBM MQ con CICS

Per utilizzare IBM MQ con CICS, è necessario configurare l'adattatore IBM MQ CICS e, facoltativamente, i componenti IBM MQ CICS bridge .

Per ulteriori informazioni sulla configurazione dell'adattatore IBM MQ CICS e dei componenti di IBM MQ CICS bridge , consultare la sezione Configurazione delle connessioni a MQ della documentazione di CICS .

Concetti correlati

IBM MQ e CICS

“Utilizzo di IBM MQ con IMS” a pagina 932

L'adattatore IBM MQ -IMS e il bridge IBM MQ - IMS sono i due componenti che consentono a IBM MQ di interagire con IMS.

Riferimenti correlati

“Aggiornamento e applicazione del servizio a Language Environment o z/OS Callable Services” a pagina 941

Le azioni che è necessario eseguire variano a seconda che si utilizzi CALLLIBS o LINK e la versione di SMP/E.

z/OS Aggiornamento e applicazione del servizio a Language Environment o z/OS Callable Services

Le azioni che è necessario eseguire variano a seconda che si utilizzi CALLLIBS o LINK e la versione di SMP/E.

Le seguenti tabelle mostrano cosa è necessario fare per IBM MQ for z/OS se si aggiorna il proprio livello o si applica il servizio ai seguenti prodotti:

- Ambiente del linguaggio
- z/OS Servizi richiamabili (APPC e RRS, ad esempio)

Tabella 67. Il servizio è stato applicato o il prodotto è stato aggiornato a una nuova release

Prodotto	**Azione se si utilizzano CALLLIBS e SMP/E V3r2 o successive** **Nota: Non è necessario eseguire lavori separati per Language Environment e servizi richiamabili. Un lavoro sarà sufficiente.**	**Azione se si utilizza LINK**
Ambiente del linguaggio	1. Impostare il limite sul lavoro SMP/E sulla zona di destinazione. 2. Sulla scheda SMPCNTL specificare LINK LMODS CALLLIBS. È anche possibile specificare altri parametri come CHECK, RETRY (YES) e RC. Per ulteriori informazioni, vedere *SMP/E per z/OS: Comandi* . 3. Eseguire il lavoro SMP/E.	Non è richiesta alcuna azione se le zone SMP/E sono state impostate per il ricollegamento automatico e il lavoro CSQ8SLDQ è stato eseguito.

Tabella 67. Il servizio è stato applicato o il prodotto è stato aggiornato a una nuova release (Continua)

Prodotto	**Azione se si utilizzano CALLLIBS e SMP/E V3r2 o successive** **Nota: Non è necessario eseguire lavori separati per Language Environment e servizi richiamabili. Un lavoro sarà sufficiente.**	**Azione se si utilizza LINK**
Servizi richiamabili	1. Impostare il limite sul lavoro SMP/E sulla zona di destinazione. 2. Sulla scheda SMPCNTL specificare LINK LMODS CALLLIBS. È anche possibile specificare altri parametri come CHECK, RETRY (YES) e RC. Per ulteriori informazioni, vedere *SMP/E per z/OS: Comandi* . 3. Eseguire il lavoro SMP/E.	Non è richiesta alcuna azione se le zone SMP/E sono state impostate per il ricollegamento automatico e il lavoro CSQ8SLDQ è stato eseguito.

Tabella 68. Uno dei prodotti è stato aggiornato ad una nuova versione in un nuovo ambiente e librerie SMP/E

Prodotto	**Azione se si utilizzano CALLLIBS e SMP/E V3r2 o successive** **Nota: Non è necessario eseguire tre lavori separati per Language Environment e servizi richiamabili. Un lavoro sarà sufficiente per entrambi i prodotti.**	**Azione se si utilizza LINK**
Ambiente del linguaggio	1. Modificare le DDDEF per SCEELKED e SCEESPC per puntare alla nuova libreria. 2. Impostare il limite sul lavoro SMP/E sulla zona di destinazione. 3. Sulla scheda SMPCNTL specificare LINK LMODS CALLLIBS. È anche possibile specificare altri parametri come CHECK, RETRY (YES) e RC. Per ulteriori informazioni, vedere *SMP/E per z/OS: Comandi* . 4. Eseguire il lavoro SMP/E.	1. Eliminare le voci secondarie XZMOD per le seguenti voci LMOD nella zona di destinazione IBM MQ for z/OS : CMQXDCST, CMQXRCTL, CMQXSUPR, CSQCBE00, CSQCBE30, CSQCBP00, CSQCBP10, CSQCBR00, CSQUCVX, CSQUDLQH, CSQVXPCB, CSQVXSPT, CSQXDCST, CSQXRCTL, CSQXSUPR, CSQXTCMI, CSQXTCP, CSQXTNSV, CSQ7DRPS, IMQB23IC, IMQB23IM, IMQB23IR, IMQS23IC, IMQS23IM, IMQS23IR 2. Impostare le ZONEINDEX appropriate tra le zone IBM MQ e le zone Language Environment. 3. Adattare CSQ8SLDQ in modo che faccia riferimento alla nuova zona sul parametro FROMZONE dei comandi LINK. CSQ8SLDQ si trova nella libreria SCSQINST. 4. Eseguire CSQ8SLDQ.

Tabella 68. Uno dei prodotti è stato aggiornato ad una nuova versione in un nuovo ambiente e librerie SMP/E (Continua)

Prodotto	Azione se si utilizzano CALLLIBS e SMP/E V3r2 o successive **Nota: Non è necessario eseguire tre lavori separati per Language Environment e servizi richiamabili. Un lavoro sarà sufficiente per entrambi i prodotti.**	Azione se si utilizza LINK
Servizi richiamabili	1. Modificare il DDDEF per CSSLIB in modo che punti alla nuova libreria 2. Impostare il limite sul lavoro SMP/E sulla zona di destinazione. 3. Sulla scheda SMPCNTL specificare LINK LMODS CALLLIBS. È anche possibile specificare altri parametri come CHECK, RETRY (YES) e RC. Per ulteriori informazioni, vedere *SMP/E per z/OS: Comandi* . 4. Eseguire il lavoro SMP/E.	1. Eliminare le voci secondarie XZMOD per le seguenti voci LMOD nella zona di destinazione IBM MQ for z/OS : CMQXRCTL, CMQXSUPR, CSQBSR, CSQILPLM, CSQXJST, CSQXRCTL, CSQXSUPR, CSQ3AMGP, CSQ3EPX, CSQ3REPL 2. Impostare le ZONEINDEX appropriate tra le zone IBM MQ e le zone Callable Services. 3. Adattare CSQ8SLDQ in modo che faccia riferimento alla nuova zona sul parametro FROMZONE dei comandi LINK. CSQ8SLDQ si trova nella libreria SCSQINST. 4. Eseguire CSQ8SLDQ.

Per un esempio di lavoro per ricollegare i moduli quando si utilizza CALLLIBS, consultare "Esecuzione di un lavoro LINK CALLLIBS" a pagina 943.

z/OS Esecuzione di un lavoro LINK CALLLIBS

Un lavoro di esempio per ricollegare moduli quando si utilizza CALLLIBS.

Il seguente è un esempio del lavoro per ricollegare i moduli quando si utilizzano CALLLIBs su un sistema SMP/E V3r2 . È necessario fornire JOBCARD e il nome del dataset SMP/E CSI che contiene IBM MQ for z/OS.

```
//*********************************************************************
//* RUN LINK CALLLIBS.
//*********************************************************************
//CALLLIBS EXEC PGM=GIMSMP,REGION=4096K
//SMPCSI  DD DSN=your.csi
//       DISP=SHR
//SYSPRINT DD SYSOUT=*
//SMPCNTL DD *
SET BDY(TZONE).
LINK LMODS CALLLIBS .
/*
```

Figura 121. Lavoro SMP/E LINK CALLLIBS di esempio

z/OS Utilizzo delle uscite OTMA in IMS

Utilizzare questo argomento se si desidera utilizzare le uscite IMS Open Transaction Manager Access con IBM MQ for z/OS.

Se si desidera inviare l'output da una transazione IMS a IBM MQe tale transazione non ha avuto origine in IBM MQ, è necessario codificare una o più uscite OTMA IMS .

Allo stesso modo, se si desidera inviare l'output a una destinazione non OTMA e la transazione ha avuto origine in IBM MQ, è necessario codificare anche una o più IMS uscite OTMA.

Le seguenti uscite sono disponibili in IMS per consentire di personalizzare l'elaborazione tra IMS e IBM MQ:

- Un'uscita di preinstradamento OTMA
- Un'uscita DRU (destination resolution user)

Nomi uscita OTMA

È necessario denominare l'uscita di preinstradamento DFSYPRX0. È possibile denominare qualsiasi uscita DRU, purché non sia in conflitto con un nome modulo già presente in IMS.

Specifica del nome dell'uscita utente di risoluzione di destinazione

È possibile utilizzare il parametro *Druexit* della parola chiave OTMACON della macro CSQ6SYSP per specificare il nome dell'exit DRU OTMA che deve essere eseguita da IMS.

Per semplificare l'identificazione dell'oggetto, prendere in considerazione l'adozione di una convenzione di denominazione di DRU0xxxx, dove xxxx è il nome del gestore code IBM MQ .

Se non si specifica il nome di un'uscita DRU nel parametro OTMACON, il valore predefinito è DFSYDRU0. Per ulteriori informazioni, consultare DFSYDRU0 .

Convenzione di denominazione per la destinazione IMS

È necessaria una convenzione di denominazione per la destinazione a cui si invia l'output dal proprio programma IMS . Questa è la destinazione impostata nella chiamata CHNG della tua applicazione IMS o preimpostata nel PSB IMS .

Uno scenario di esempio per un'uscita OTMA

Utilizzare i seguenti argomenti per un esempio di uscita di pre - instradamento e di uscita di instradamento di destinazione per IMS:

- “L'uscita di pre - instradamento DFSYPRX0” a pagina 944
- “L'uscita utente della risoluzione di destinazione” a pagina 946

Per semplificare l'identificazione, rendere il nome di destinazione OTMA simile al nome del gestore code IBM MQ , ad esempio il nome del gestore code IBM MQ ripetuto. In questo caso, se il nome del gestore code IBM MQ è " **VCPE** ", la destinazione impostata dalla chiamata CHNG è" **VCPEVCPE** ".

Concetti correlati

IBM MQ e IMS

“Utilizzo di IBM MQ con IMS” a pagina 932

L'adattatore IBM MQ -IMS e il bridge IBM MQ - IMS sono i due componenti che consentono a IBM MQ di interagire con IMS.

Applicazioni bridge IMS e IMS su IBM MQ for z/OS

z/OS L'uscita di pre - instradamento DFSYPRX0

Questo argomento contiene un'uscita di pre - instradamento di esempio per OTMA in IMS.

È necessario prima codificare un'uscita di preinstradamento DFSYPRX0. Consultare OTMA Destination Resolution user exit (DFSYPRX0 e altre uscite di tipo OTMAYPRX) per parametri passati a questa routine da IMS.

Questa uscita verifica se il messaggio è destinato a una destinazione OTMA nota (nell'esempio VCPEVCPE). In questo caso, l'exit deve verificare se la transazione che invia il messaggio ha avuto origine

in OTMA. Se il messaggio ha avuto origine in OTMA, avrà un'intestazione OTMA, quindi è necessario uscire da DFSYPRX0 con il registro 15 impostato su zero.

- Se la transazione che invia il messaggio non ha avuto origine in OTMA, è necessario impostare il nome client in modo che sia un client OTMA valido. Questo è il nome - membro XCF del gestore code IBM MQ a cui si desidera inviare il messaggio. Impostare il nome client (nel parametro OTMACON della macro CSQ6SYSP) sul nome del gestore code. Questa è l'opzione predefinita. È quindi necessario uscire da DFSYPRX0 impostando il registro da 15 a 4.
- Se la transazione che invia il messaggio ha avuto origine in OTMA e la destinazione non è OTMA, è necessario impostare il registro da 15 a 8 ed uscire.
- In tutti gli altri casi, è necessario impostare il registro 15 su zero.

Se si imposta il nome client OTMA su uno sconosciuto a IMS, la chiamata CHNG o ISRT dell'applicazione restituisce un codice di stato A1 .

Per un sistema IMS che comunica con più di un gestore code IBM MQ , è necessario ripetere la logica per ciascun gestore code IBM MQ .

Il codice assembler di esempio viene mostrato in Figura 122 a pagina 946:

```
TITLE 'DFSYPRX0: OTMA PRE-ROUTING USER EXIT'
DFSYPRX0 CSECT
DFSYPRX0 AMODE 31
DFSYPRX0 RMODE ANY
*
SAVE (14,12),,DFSYPRX0&SYSDATE&SYSTIME
SPACE 2
LR  R12,R15        MODULE ADDRESSABILITY
USING DFSYPRX0,R12
*
L   R2,12(,R1)      R2 -> OTMA PREROUTE PARMS
*
LA  R3,48(,R2)      R3 AT ORIGINAL OTMA CLIENT (IF ANY)
CLC  0(16,R3),=XL16'00'  OTMA ORIG?
BNE  OTMAIN        YES, GO TO THAT CODE
*
NOOTMAIN DS 0H            NOT OTMA INPUT
LA  R5,8(,R2)       R5 IS AT THE DESTINATION NAME
CLC  0(8,R5),=C'VCPEVCPE' IS IT THE OTMA UNSOLICITED DEST?
BNE  EXIT0         NO, NORMAL PROCESSING
*
L   R4,80(,R2)      R4 AT ADDR OF OTMA CLIENT
MVC  0(16,R4),=CL16'VCPE' CLIENT OVERRIDE
B   EXIT4         AND EXIT
*
OTMAIN  DS 0H           OTMA INPUT
LA  R5,8(,R2)       R5 IS AT THE DESTINATION NAME
CLC  0(8,R5),=C'VCPEVCPE' IS IT THE OTMA UNSOLICITED DEST?
BNE  EXIT8         NO, NORMAL PROCESSING
```

```
*
EXIT0  DS 0H
LA  R15,0         RC = 0
B   BYEBYE
*
EXIT4  DS 0H
LA  R15,4         RC = 4
B   BYEBYE
*
EXIT8  DS 0H
LA  R15,8         RC = 8
B   BYEBYE
*
BYEBYE  DS 0H
RETURN (14,12),,RC=(15)   RETURN WITH RETURN CODE IN R15
SPACE 2
REQUATE
SPACE 2
END
```

Figura 122. Esempio di assembler uscita di pre - instradamento OTMA

z/OS L'uscita utente della risoluzione di destinazione

Questo argomento contiene una user exit di risoluzione di destinazione di esempio per IMS.

Se sono stati impostati i registri da 15 a 4 in DFSYPRX0, o se l'origine della transazione era OTMA ***e*** si imposta il Registro 15 su zero, viene richiamata l'uscita DRU. In questo esempio, il nome dell'uscita DRU è DRU0VCPE.

L'uscita DRU controlla se la destinazione è VCPEVCPE. Se lo è, imposta i dati utente OTMA (nel prefisso OTMA) come segue:

Offset
Dati utente OTMA

(decimale)

0
Lunghezza dati utente OTMA (in questo esempio, 334)

2
MQMD

326
Rispondi al formato

Questi offset sono i punti in cui il bridge IBM MQ - IMS si aspetta di trovare queste informazioni.

L'uscita DRU dovrebbe essere il più semplice possibile. Pertanto, in questo esempio, tutti i messaggi che hanno origine in IMS per un particolare gestore code IBM MQ vengono inseriti nella stessa coda IBM MQ .

Se il messaggio deve essere persistente, IMS deve utilizzare un pipe di transazioni sincronizzato. Per fare ciò, l'uscita DRU deve impostare l'indicatore OUTPUT. Per ulteriori informazioni, consultare Specifica dei tpipe sincronizzati per IBM MQ .

Scrivere un'applicazione IBM MQ per elaborare questa coda e utilizzare le informazioni dalla struttura MQMD, la struttura MQIIH (se presente) o i dati utente per instradare ciascun messaggio alla relativa destinazione.

Un'uscita DRU assembler di esempio viene mostrata in Figura 123 a pagina 947.

```
TITLE 'DRU0VCPE: OTMA DESTINATION RESOLUTION USER EXIT'
DRU0VCPE CSECT
DRU0VCPE AMODE 31
DRU0VCPE RMODE ANY
*
SAVE (14,12),,DRU0VCPE&SYSDATE&SYSTIME
SPACE 2
LR  R12,R15            MODULE ADDRESSABILITY
USING DRU0VCPE,R12
*
L   R2,12(,R1)           R2 -> OTMA DRU PARMS
*
L   R5,88(,R2)           R5 ADDR OF OTMA USERDATA
LA  R6,2(,R5)           R6 ADDR OF MQMD
USING MQMD,R6            AS A BASE
*
LA  R4,MQMD_LENGTH+10       SET THE OTMA USERDATA LEN
STH  R4,0(,R5)           = LL + MQMD + 8
*                       CLEAR REST OF USERDATA
MVI  0(R6),X'00'          ...NULL FIRST BYTE
MVC  1(255,R6),0(R6)        ...AND PROPAGATE IT
MVC  256(MQMD_LENGTH-256+8,R6),255(R6) ...AND PROPAGATE IT
*
VCPE   DS  0H
CLC  44(16,R2),=CL16'VCPE'     IS DESTINATION VCPE?
BNE  EXIT4             NO, THEN DEST IS NON-OTMA
MVC  MQMD_REPLYTOQ,=CL48'IMS.BRIDGE.UNSOLICITED.QUEUE'
MVC  MQMD_REPLYTOQMGR,=CL48'VCPE'  SET QNAME AND QMGRNAME
MVC  MQMD_FORMAT,MQFMT_IMS     SET MQMD FORMAT NAME
MVC  MQMD_LENGTH(8,R6),MQFMT_IMS_VAR_STRING
*                       SET REPLYTO FORMAT NAME
B   EXIT0
*
EXIT0  DS  0H
LA  R15,0             SET RC TO OTMA PROCESS
B   BYEBYE             AND EXIT
*
EXIT4  DS  0H
LA  R15,4             SET RC TO NON-OTMA
B   BYEBYE             AND EXIT
*
BYEBYE  DS  0H
RETURN (14,12),,RC=(15)       RETURN CODE IN R15
SPACE 2
REQUATE
SPACE 2
CMQA  EQUONLY=NO
CMQMDA DSECT=YES
SPACE 2
END
```

Figura 123. Uscita DRU assembler di esempio

z/OS V 9.1.0 Utilizzo di IBM z/OSMF per automatizzare IBM MQ

IBM z/OS Management Facility (z/OSMF) fornisce funzioni di gestione del sistema in un'interfaccia utente basata sul browser Web, orientata alle attività, con assistenza utente integrata, in modo da poter gestire più facilmente le operazioni quotidiane e la gestione dei propri sistemi mainframe z/OS .

Semplificando alcune attività tradizionali e automatizzandone altre, z/OSMF può aiutare a semplificare alcune aree della gestione del sistema z/OS .

È possibile eseguire il provisioning o l'annullamento del provisioning delle risorse, facendo clic su un pulsante, da un portale fornito dall'utente. z/OSMF fornisce API REST di supporto per questa attività.

Il portale marketplace di esempio fornito con z/OSMF può essere utilizzato anche per il provisioning e l'annullamento del provisioning delle risorse. In alternativa, gli utenti più esperti possono utilizzare la WUI (Web User Interface) z/OSMF .

Questa sezione presuppone che tu comprenda z/OSMF, ma se non hai dimestichezza con z/OSMF dovresti leggere Introduzione a z/OSMF . In alternativa, è possibile accedere a questa sezione dalla guida in linea di z/OSMF WUI.

Dovresti familiarizzare con la configurazione di z/OS Cloud, ovvero:

- Provisioning cloud - Resource Management Services
- Gestione del carico di lavoro - consultare IBM z/OS Management Facility Programming Guide per ulteriori informazioni.
- Introduzione - consultare *Esercitazione introduttiva - Cloud*

z/OSMF 2.2 introduce le attività e le attività basate sui ruoli, per cui è importante comprendere concetti quali:

domini
amministratori
Responsabili approvazione
Tenant
modelli
istanze
flussi di lavoro

e così via.

I flussi di lavoro IBM MQ z/OSMF di esempio e i file associati vengono forniti e possono essere installati come parte della funzione Componenti dei servizi di sistema IBM MQ for z/OS UNIX . Il processo di installazione per questa funzione e la struttura di directory e file sono descritti in IBM MQ for z/OS Program Directory. Program Directory for IBM MQ for z/OS può essere scaricato da Centro pubblicazioni IBM (consultare File PDF diIBM MQ for z/OS Program Directory).

I flussi di lavoro di esempio sono scritti in XML e illustrano come automatizzare il provisioning (creazione) o l'annullamento del provisioning (distruzione) di gestori code IBM MQ , iniziatori di canali e code locali e come eseguire azioni sulle risorse IBM MQ di cui è stato eseguito il provisioning. I passi all'interno dei flussi di lavoro inoltrano lavori (JCL), eseguono exec REXX, elaborano script Shell o emettono chiamate REST API .

Gli esempi sono progettati per illustrare i tipi di funzione che è possibile ottenere utilizzando z/OSMF. Si prevede che i flussi di lavoro z/OSMF verranno generalmente utilizzati per eseguire il provisioning delle risorse e le azioni come put o get message verranno, in sostanza, eseguite utilizzando le applicazioni IBM MQ .

È possibile eseguire i flussi di lavoro di esempio come forniti, purché le proprietà della variabile del flusso di lavoro siano state impostate (come descritto nelle seguenti sezioni) oppure è possibile personalizzarli come richiesto. È possibile che si preferisca scrivere i propri flussi di lavoro per eseguire ulteriori funzioni. Prima di eseguire i flussi di lavoro di esempio, consultare:

- “Prerequisiti per z/OSMF” a pagina 949

- “Impostazioni di sicurezza” a pagina 950
- “Limitazioni” a pagina 953

Le applicazioni del flusso di lavoro di esempio sono fornite per:

- “Automatizzare il provisioning o l'annullamento del provisioning dei gestori code IBM MQ ed eseguire azioni sui gestori code di cui è stato eseguito il provisioning” a pagina 954
- “Automatizzare il provisioning o l'annullamento del provisioning delle code locali IBM MQ ed eseguire azioni sulle code di cui è stato eseguito il provisioning” a pagina 955.

Concetti correlati

“Configurazione di IBM MQ for z/OS” a pagina 827
Utilizzare questo argomento come guida dettagliata per personalizzare il sistema IBM MQ for z/OS .

z/OS V 9.1.0 Prerequisiti per z/OSMF

I prerequisiti richiesti per eseguire IBM z/OS Management Facility (z/OSMF) con IBM MQ

I flussi di lavoro IBM MQ forniti in IBM MQ 9.1.0 utilizzano la nuova funzione in z/OSMF, fornita tramite APAR su z/OS 2.1 e 2.2. Ulteriori dettagli sono forniti nel seguente testo.

1. IBM z/OS Management Facility 2.2 è stato installato e configurato correttamente. Se si sta eseguendo con la sicurezza abilitata, assicurarsi che tutte le impostazioni di sicurezza documentate da z/OSMF siano state configurate.
2. Sono stati installati i seguenti APAR per:

   z/OS 2.1

   - PI71068
   - PI71079
   - PI71082
   - PI71084
   - OA50130

   z/OS 2.2

   - PI70526
   - PI70521
   - PI70527
   - PI67839
   - PI70767
   - PI46315
   - OA49081
   - OA49802
   - OA50130
3. Il processo angel z/OSMF (se richiesto) e i processi server sono stati configurati.
4. L'ambiente z/OS Cloud è stato configurato (come descritto in precedenza e documentato da z/OSMF)
5. IBM MQ for z/OS 9.0.1 è stato installato e le librerie di caricamento del prodotto sono disponibili.
6. Sono state eseguite le seguenti attività di personalizzazione del gestore code IBM MQ :

Attività	Descrizione
1	Identificare i parametri di sistema z/OS
2	L'APF autorizza le librerie di caricamento IBM MQ
3	Aggiornare l'elenco di link z/OS e LPA

Attività	Descrizione
4	Aggiornare la tabella delle proprietà del programma z/OS

7. I flussi di lavoro di esempio e i file associati vengono installati in una directory USS (UNIX System Services for z/OS) adatta.
8. La directory USS **'/tmp'** è disponibile, poiché il flusso di lavoro provision.xml potrebbe creare un file temporaneo in questa directory. Se viene creato un file, il flusso di lavoro, in generale, elimina il file dopo l'utilizzo.
9. Il file `deprovision.xml` contiene passi che richiamano le esecuzioni CSQ4ZWS1.rexx e CSQ4ZWS2.rexx REXX. Questi execs attendono l'arresto del gestore code e dei sottosistemi iniziatore di canali; gli execs richiamano il comando USS 'SLEEP' come una chiamata di sistema.

   A seconda della configurazione USS, è possibile che il comando 'SLEEP' non funzioni come codificato. Se, durante l'elaborazione, si verifica un errore che indica che non è possibile trovare il comando 'SLEEP', è possibile provare a sostituire le seguenti righe in execs CSQ4ZWS1.rexx e CSQ4ZWS2.rexx:

```
CALL SYSCALLS('ON')             /* Enable USS calls    */
ADDRESS SYSCALL
"SLEEP" 10                           /* Sleep for 10 seconds */
CALL SYSCALLS 'OFF'             /* Disable USS calls    */
```

   indicando

```
'sleep' 10
```

   Quindi, immettere il comando OMVS (Open MVS) **env** per controllare l'impostazione delle variabili di ambiente PATH. Assicurarsi che la directory che contiene il comando **`sleep`** sia definita in PATH. Notare che il comando **`sleep`** si trova di solito nella directory `/bin` .
10. Assicurarsi che z/OSMF sia stato avviato.

    Entrambi i processi angel e server z/OSMF devono essere avviati e la WUI (Web User Interface) z/OSMF deve essere attiva e in esecuzione. Per ulteriori dettagli, consultare Liberty profile: Process types on z/OS.

    Anche se si intende guidare i flussi di lavoro utilizzando REST API, è necessario avviare z/OSMF WUI. z/OSMF WUI può essere utile per il monitoraggio della creazione e dell'esecuzione di flussi di lavoro.

Concetti correlati

“Utilizzo di IBM z/OSMF per automatizzare IBM MQ” a pagina 948
IBM z/OS Management Facility (z/OSMF) fornisce funzioni di gestione del sistema in un'interfaccia utente basata sul browser Web, orientata alle attività, con assistenza utente integrata, in modo da poter gestire più facilmente le operazioni quotidiane e la gestione dei propri sistemi mainframe z/OS .

z/OS V 9.1.0 Impostazioni di sicurezza

Le impostazioni di sicurezza richieste per eseguire z/OSMF.

Le proprietà della variabile ID utente riportate di seguito sono definite nel file delle proprietà. Per ulteriori dettagli, consulta “Esecuzione dei flussi di lavoro” a pagina 958.

Proprietà ID utente	Descrizione
IDUSER_CSQ	ID utente utilizzato per eseguire i passi del workflow. Tenere presente, tuttavia, che le fasi selezionate (che generalmente richiedono un livello elevato di autorizzazione) verranno eseguite con ID utente diversi in base alle impostazioni degli ID utente **`CSQ_ADMIN_*`** elencati nel seguente testo. L'ID utente in uso viene identificato dalla proprietà **`runAsUser`** nel rispettivo passo nei flussi di lavoro.

Proprietà ID utente	Descrizione
IDERO_APF_ADMIN_CSQ	ID utente da utilizzare quando APF autorizza la libreria di caricamento che contiene il modulo dei parametri di sistema del gestore code.
ID_APPROVAL_CSQ_APF	L'ID di approvazione utilizzato per consentire agli utenti di eseguire la fase di autorizzazione APF del dataset come utente CSQ_ADMIN_APF_USERID.
IDUTENTE_CONSOLE_ADMIN_CSQL	L'ID utente utilizzato durante l'esecuzione dei passi nell'esecuzione che immettono i comandi della console z/OS .  **Attenzione:** A questo ID utente deve essere consentito l'accesso UPDATE al profilo attività avviata (MVS.START.STC. *) nella classe OPERCMDS. Per ulteriori informazioni, consultare Controllo dell'utilizzo dei comandi dell'operatore nella documentazione di z/OS .
ID_APPROVAZIONE_CONSOLE_CQ	L'ID approvazione utilizzato per consentire agli utenti di eseguire i passi che immettono i comandi della console z/OS nell'esecuzione come utente CSQ_ADMIN_CONSOLE_USERID.
IDUSER_SAF_SQ_ADMIN_CSQ	ID utente da utilizzare quando si immettono comandi SAF.
ID_APPROVAL_SAF_CSQ	L'ID approvazione utilizzato per consentire agli utenti di eseguire i passi del comando SAF nell'esecuzione come utente CSQ_ADMIN_SAF_USERID.
CSQ_ADMIN_SSI_USERID	ID utente da utilizzare quando si immette il comando SETSSI per identificare il sottosistema sottoposto a provisioning in z/OS.
ID_APPROVAL_CSQ_SSI_ID	L'ID approvazione utilizzato per consentire agli utenti di eseguire il passo del comando SETSSI sotto l'esecuzione come utente CSQ_ADMIN_SSI_USERID.

Nota: L'ID utente utilizzato per eseguire i flussi di lavoro di provisioning e di annullamento provisioning deve disporre di autorizzazioni sufficienti, come indicato di seguito:

1. I flussi di lavoro di provisioning e annullamento provisioning del gestore code utilizzano il comando SETPROG per autorizzare i dataset APF. L'ID utente è impostato nella proprietà CSQ_ADMIN_APF_USERID oppure l'ID utente utilizzato per eseguire i flussi di lavoro deve essere autorizzato a immettere questo comando. È possibile ottenere ciò immettendo il seguente comando:

```
PERMIT MVS.SETPROG CLASS(OPERCMDS) ID(value of CSQ_ADMIN_APF_USERID) ACCESS(UPDATE)
```

   Nota: Il comando SETPROG potrebbe non persistere in un IPL di un sistema z/OS , pertanto potrebbe essere necessario immettere manualmente il seguente comando SETPROG dopo un IPL:

```
SETPROG APF,ADD,DSN=value of CSQ_AUTH_LIB_HLQ.value of CSQ_SSID.APF.LOAD,SMS
```

   Per ulteriori dettagli sul comando SETPROG, consultare Utilizzo di RACF per controllare gli elenchi APF.

   Inoltre, potrebbe essere stata abilitata la classe FACILITY per controllare quali librerie possono essere autorizzate APF, quindi potrebbe essere necessario immettere il comando:

```
PERMIT CSVAPF.libname CLASS(FACILITY) ID(value of CSQ_ADMIN_APF_USERID)
       ACCESS(UPDATE)
```

2. Un passo nel flusso di lavoro di provisioning del gestore code immette il comando SETSSI per identificare il sottosistema IBM MQ in z/OS. L'ID utente impostato nella proprietà

CSQ_ADMIN_SSI_USERID deve essere consentito per utilizzare questo comando. È possibile ottenere ciò immettendo il seguente comando:

```
PERMIT MVS.SETSSI.ADD CLASS(OPERCMDS) ID(value of CSQ_ADMIN_SSI_USERID)
        ACCESS(CONTROL)
```

Nota: I sottosistemi che sono stati identificati in z/OS tramite il comando SETSSI non persistono in un IPL di un sistema z/OS . Quindi, potrebbe essere necessario immettere manualmente il seguente comando SETSSI dopo un IPL:

```
SETSSI  ADD,S='value of CSQ_SSID',I=CSQ3INI,
       P='CSQ3EPX,value of CSQ_CMD_PFX,S'
```

Per ulteriori dettagli sul comando SETSSI, consultare: Comando SETSSI.

3. I flussi di lavoro emettono i comandi del gestore code, quindi se si intende abilitare la sicurezza, l'ID utente impostato nella proprietà CSQ_ADMIN_RACF_USERID (o l'ID utente utilizzato per eseguire i flussi di lavoro) deve disporre dell'autorizzazione CLAUTH (autenticazione client) per MQADMIN o la classe MXADMIN (a seconda della classe utilizzata). Ciò consente a questo ID utente di definire i profili di sicurezza per queste classi. È possibile ottenere ciò immettendo il seguente comando:

```
ALTUSR value of CSQ_ADMIN_RACF_USERID CLAUTH(MQADMIN)
```

Per ulteriori dettagli su **CLAUTH** , consultare L'attributo CLAUTH (autorizzazione classe).

4. Il flusso di lavoro deprovision.xml emette comandi z/OS , ad esempio, i lavori DISPLAY ACTIVE, i sottosistemi CANCEL o FORCE, quindi l'ID utente impostato nella proprietà CSQ_ADMIN_CONSOLE_USERID (o l'ID utente utilizzato per eseguire i flussi di lavoro) deve disporre dell'autorizzazione appropriata per emettere tali comandi.
5. Gli utenti che richiedono un'istanza del gestore code, utilizzando la tabella dei modelli dell'attività Servizi software, devono disporre delle autorizzazioni per accedere a z/OSMF e a Configuration Assistant, come definito da z/OSMF.
6. L'ID utente del consumer che esegue il provisioning di un gestore code richiede l'autorità per aggiungere ed eliminare i membri dal dataset PROCLIB definito con la variabile CSQ_PROC_LIB.
7. È necessario eseguire il provisioning di un gestore code prima delle code di provisioning.
8. Per utilizzare i flussi di lavoro `queueLoad.xml` e `queueOffload.xml` , i dataset utilizzati devono essere definiti in anticipo. Inoltre, l'ID utente utilizzato per eseguire questi flussi di lavoro deve disporre dell'autorizzazione UPDATE per i dataset.
9. Un passo nel flusso di lavoro del gestore code `provision.xml` attualmente disabilita la sicurezza del sottosistema. È possibile modificare il lavoro `csq4znse.jcl` per abilitare la sicurezza del sottosistema aggiungendo i comandi di sicurezza appropriati per la protezione delle risorse IBM MQ . Tuttavia, tenere presente che se si aggiungono ulteriori comandi, è necessario aggiungere anche i comandi per eliminare le autorizzazioni di protezione in `csq4dse.jcl`, inoltrato dal flusso di lavoro deprovision.xml .

   Nota: Questo passo emette i comandi di sicurezza RACF . Se si sta utilizzando un prodotto di sicurezza alternativo, è necessario modificare questa operazione per immettere i comandi appropriati per il proprio prodotto di sicurezza.

Requisiti di rete

Quando si aggiunge un modello di gestore code e le relative risorse, è necessario fare clic su **Crea pool di risorse di rete**. Questo crea un pool di risorse con risorse di rete per questo modello.

Utilizzando Assistente di configurazione, l'amministratore di rete deve completare questa definizione del pool di risorse di rete definendo un limite per il numero di porte che devono essere assegnate per questo modello.

Per ogni istanza del modello, il flusso di lavoro `provision.xml` assegna una porta nell'intervallo e avvia un listener per l'ascolto su tale porta.

Classificazione con IBM Workload Manager

Se si desidera classificare il gestore code e gli spazi di indirizzo dell'iniziatore di canali con WLM, è necessario specificarlo quando si aggiunge un modello per il provisioning di un gestore code.

Se classificare o meno, è controllato dagli indicatori **CSQ_DEFINE_MSTR_WLM_RULE** e **CSQ_DEFINE_CHIN_WLM_RULE**, impostati nel file `workflow_variables.properties`.

Per ulteriori informazioni sulla classificazione con WLM, fare riferimento al manuale *z/OSMF Configuration Guide*.

Concetti correlati

“Prerequisiti per z/OSMF” a pagina 949
I prerequisiti richiesti per eseguire IBM z/OS Management Facility (z/OSMF) con IBM MQ

z/OS V 9.1.0 Limitazioni

Limitazioni quando si utilizza z/OSMF con IBM MQ.

1. Il flusso di lavoro `provision.xml` attualmente automatizza le attività di personalizzazione dei gestori code evidenziate riportate di seguito:

Attività	Descrizione
1	Identificare i parametri di sistema z/OS
2	L'APF autorizza le IBM MQ librerie di caricamento **(provision.xml autorizza APF alcune librerie)**
3	Aggiornare l'elenco di link z/OS e LPA
4	Aggiornare la tabella delle proprietà del programma z/OS
5	**Definizione del sottosistema IBM MQ in z/OS**
6	**Creare procedure per il gestore code IBM MQ**
7	**Creare procedure per l'iniziatore di canali**
8	**Definire il sistema secondario IBM MQ in una z/OS classe di servizi WLM**
9	Selezionare e configurare l'ambiente di archiviazione CF (Coupling Facility)
10	Impostazione della CF (coupling facility)
11	Implementare i controlli di sicurezza ESM
12	Aggiornare SYS1.PARMLIB
13	**Personalizzazione dei dataset di input di inizializzazione**
14	**Creazione dei dataset bootstrap e log**
15	**Definire le serie di pagine**
16	Aggiungere le voci IBM MQ al gruppo di condivisione dati Db2
17	**Adattare i moduli dei parametri di sistema (alcuni)**
18	**Personalizzare i parametri dell'iniziatore di canali (alcuni)**
19	Impostazione di adattatori Batch, TSO e RRS
20	Impostare le operazioni e i pannelli di controllo

Attività	Descrizione
21	Includi il membro di formattazione del dump IBM MQ
22	Elimina messaggi informativi
23	Aggiornare il membro DIAG di sistema per Advanced Message Security
24	Crea procedure per Advanced Message Security .
25	Configurare l'utente dell'attività avviata Advanced Message Security
26	Concedere le autorizzazioni RACDCERT all'amministratore della sicurezza per Advanced Message Security
27	Concedere agli utenti le autorizzazioni di risorsa per Advanced Message Security

2. Le attività di personalizzazione non evidenziate in grassetto devono essere eseguite manualmente, se necessario.
3. I membri INP1 e INP2 di esempio sono attualmente utilizzati così come sono. Se necessario, è possibile definire ulteriori proprietà per controllare le risorse definite da questi membri.
4. I commenti relativi a specifiche proprietà elencate nel file delle proprietà indicano eventuali limitazioni nell'utilizzo di tali proprietà. Per ulteriori dettagli, consulta "Esecuzione dei flussi di lavoro" a pagina 958.

Concetti correlati

"Impostazioni di sicurezza" a pagina 950
Le impostazioni di sicurezza richieste per eseguire z/OSMF.

z/OS V 9.1.0 Automatizzare il provisioning di oggetti IBM MQ

Gli esempi vengono forniti per automatizzare il provisioning dei gestori code e delle code locali.

Automatizzare il provisioning o l'annullamento del provisioning dei gestori code IBM MQ ed eseguire azioni sui gestori code di cui è stato eseguito il provisioning

Vengono forniti i seguenti flussi di lavoro z/OSMF di esempio specifici del gestore code:

Nome flusso di lavoro	Descrizione
provision.xml	Provisioning di un gestore code IBM MQ for z/OS Questo flusso di lavoro di esempio: • Esegue il provisioning delle risorse di sistema necessarie per un gestore code. • Esegue il provisioning delle risorse di sistema richieste per un iniziatore di canali. • Avvia il gestore code (che avvia anche l'iniziatore di canali e il listener TCP/IP) • Esegue il programma di verifica dell'installazione del gestore code di esempio. È possibile impostare una proprietà di ambiente per controllare il provisioning di gestori code con caratteristiche differenti. Per ulteriori informazioni, consultare "Esecuzione dei flussi di lavoro" a pagina 958. **Nota:** Viene fornito un file manifest (`provision.mf`) per assistere l'aggiunta di un template per questo workflow. Questo file contiene un riferimento al file **qaas_readme.pdf** che contiene ulteriori informazioni. È

Nome flusso di lavoro	Descrizione
	possibile accedere al file tramite un collegamento, una volta aggiunto il template.
deprovision.xml	Annullamento del provisioning di un gestore code IBM MQ for z/OS Questo flusso di lavoro di esempio: • Arresta l'iniziatore di canali (che arresta anche il listener TCP/IP) e il gestore code. • Attese per l'arresto dei sottosistemi • Annullare il provisioning di tutte le risorse di sistema dell'iniziatore di canali e del gestore code.
startQMgr.xml	Avviare un gestore code IBM MQ for z/OS Questo flusso di lavoro di esempio avvia il gestore code (che avvia anche l'iniziatore di canali e il listener TCP/IP).
stopQMgr.xml	Arresto di un gestore code IBM MQ for z/OS Questo flusso di lavoro di esempio arresta l'iniziatore di canali (che arresta anche il listener TCP/IP) e il gestore code.

Ogni flusso di lavoro esegue una o più operazioni. I commenti nei workflow descrivono la funzione eseguita da ciascun passo. Alcuni dei passi richiedono solo l'input dei dati, mentre altri inoltrano JCL, richiamano gli exec REXX, gli script Shell o emettono chiamate REST API per eseguire la funzione indicata.

Fare riferimento a ciascun passo per il nome esatto dei file exec JCL o REXX. I flussi di lavoro e i file exec JCL o REXX associati fanno riferimento a variabili dichiarate in uno o più file XML di variabili. Per ulteriori dettagli, consulta "File di dichiarazione delle variabili del workflow" a pagina 957.

deprovision, **startQMgr**e **stopQMgr** possono essere eseguiti come azioni su un gestore code IBM MQ for z/OS di cui è stato eseguito il provisioning.

Automatizzare il provisioning o l'annullamento del provisioning delle code locali IBM MQ ed eseguire azioni sulle code di cui è stato eseguito il provisioning

Vengono forniti i seguenti flussi di lavoro z/OSMF di esempio specifici della coda:

Nome flusso di lavoro	Descrizione
defineQueue.xml	Definire una coda locale Questo flusso di lavoro di esempio dimostra in che modo i flussi di lavoro z/OSMF possono essere utilizzati per definire code di piccole, medie o grandi dimensioni in base alle impostazioni delle proprietà. **Nota:** Viene fornito un file manifest (`provision.mf`) per assistere l'aggiunta di un template per questo workflow. Questo file contiene un riferimento al file **qaas_readme.pdf** che contiene ulteriori informazioni. È possibile accedere al file tramite un collegamento, una volta aggiunto il template.
displayQueue.xml	Visualizza attributi selezionati di una coda locale Questo flusso di lavoro di esempio visualizza gli attributi selezionati di una coda locale. Gli attributi vengono restituiti in una variabile z/OSMF (fare riferimento alla procedura nel workflow per il nome della variabile) e successivamente visualizzati. Se richiesto, è possibile accedere al contenuto della variabile utilizzando un REST API.

Nome flusso di lavoro	Descrizione
	Per ulteriori informazioni, fai riferimento a Cloud provisioning REST APIse vedi anche z/OSMF workflow services.
deleteQueue.xml	Elimina una coda locale Questo workflow di esempio elimina una coda locale su un gestore code specificato.
putQueue.xml	Inserire uno o più messaggi in una coda locale. Questo flusso di lavoro di esempio inserisce uno o più messaggi in una coda locale. Il testo del messaggio può essere specificato, ma se più di un messaggio viene inserito contemporaneamente in una coda locale, viene utilizzato lo stesso testo del messaggio.
getQueue.xml	Richiamare uno o più messaggi da una coda locale. Questo flusso di lavoro di esempio richiama uno o più messaggi da una coda locale. I messaggi vengono restituiti in una variabile z/OSMF (fare riferimento alla procedura nel workflow per il nome della variabile) e successivamente visualizzati. Se necessario, è possibile accedere al contenuto della variabile utilizzando un REST API. Per ulteriori informazioni, fai riferimento a Cloud provisioning REST APIse vedi anche z/OSMF workflow services.
loadQueue.xml	Caricare i messaggi da un dataset ad una coda locale. Questo flusso di lavoro di esempio carica i messaggi da un dataset su una coda locale. Il nome predefinito del data set viene specificato impostando una proprietà. Per ulteriori dettagli, consulta “Esecuzione dei flussi di lavoro” a pagina 958.
offloadQueue.xml	Scaricare i messaggi da una coda locale in un dataset. Questo flusso di lavoro di esempio scarica i messaggi da una coda locale a un dataset. Il nome predefinito del data set viene specificato impostando una proprietà. Per ulteriori dettagli, consulta “Esecuzione dei flussi di lavoro” a pagina 958.
clearQueue.xml	Cancellare i messaggi su una coda locale. Questo flusso di lavoro di esempio elimina (elimina) tutti i messaggi su una coda locale.

Note:

1. L'azione **Inserisci coda** consente di immettere alcuni dati del messaggio e di inserire uno o più messaggi in una coda. Se più di un messaggio deve essere inserito in una coda durante una determinata richiesta, vengono utilizzati gli stessi dati del messaggio.
2. I flussi di lavoro loadQueue.xml e offloadQueue.xml richiamano il modulo eseguibile, CSQUDMSG nella libreria SCSQLOAD, con un alias di QLOAD. È equivalente al programma di utilità **dmpmqmsg** disponibile con IBM MQ for Multiplatforms. Pertanto, i messaggi caricati da un dataset in una coda o da una coda in un dataset, devono essere nel formato **dmpmqmsg** .

   JCL di esempio viene fornito anche come membro CSQ4QLOD in SCSQPROC.

   Il modo più semplice per provare le operazioni loadQueue e offloadQueue è:

   a. Immettere **putQueue** alcune volte per inserire alcuni messaggi in coda.

   b. Utilizzare **offloadQueue** per scaricare i messaggi dalla coda su un dataset.

c. Se necessario, immettere **clearQueue** per rimuovere tutti i messaggi dalla coda.

d. Utilizzare **loadQueue** per caricare i messaggi da un dataset nella stessa coda o in una coda differente.

Se si è interessati al formato **dmpmqmsg** , è possibile sfogliare il contenuto del dataset, una volta emessa una richiesta Offload.

3. È possibile eseguire **displayQueue**, **deleteQueue**, **putQueue**, **getQueue**, **loadQueue**, **offloadQueue**e **clearQueue** come azioni su una coda locale IBM MQ for z/OS di cui è stato eseguito il provisioning. Per ulteriori dettagli sulle azioni e sui file di azione, fare riferimento al manuale *z/OSMF Programming Guide*.
4. Tutti i flussi di lavoro correlati all'azione vengono eliminati per impostazione predefinita. Il motivo è ridurre la necessità per gli utenti di ripulire i flussi di lavoro.

   Il problema con questo tuttavia è quello in cui un'azione risulta in qualche output. Ad esempio, le azioni **displayQueue** e **getQueue** producono entrambe un output.

   L'output non può essere visualizzato poiché il relativo flusso di lavoro viene eliminato non appena l'azione è stata eseguita. Quindi, se si guidano le azioni del workflow dalla WUI di z/OS , è necessario impostare l'indicatore **cleanAfterComplete** su *false* nella tag **< workflow>** per ogni azione di cui si desidera visualizzare l'output.

   Ad esempio, per visualizzare l'output di **displayQueue**, impostare l'indicatore nel modo seguente:

```
<action name="displayQueue">
  <workflow cleanAfterComplete="false">
  ...

  ...
  </workflow>
</action>
```

Tuttavia, ciò significa che è necessario ripulire manualmente i flussi di lavoro correlati all'azione.

Ogni flusso di lavoro z/OSMF di esempio esegue uno o più passi. I commenti nei workflow descrivono la funzione eseguita da ciascun passo. Alcuni dei passi richiedono solo l'immissione di dati mentre altri inoltrano JCL e altri richiamano le esecuzioni REXX per eseguire la funzione indicata.

Fare riferimento a ciascun passo per il nome esatto dei file exec JCL o REXX. I flussi di lavoro e i file exec JCL o REXX associati fanno riferimento a variabili dichiarate in uno o più “File di dichiarazione delle variabili del workflow” a pagina 957.

Concetti correlati

“Limitazioni” a pagina 953
Limitazioni quando si utilizza z/OSMF con IBM MQ.

z/OS V 9.1.0 Esecuzione dei workflow

Una descrizione dei file a cui fanno riferimento i flussi di lavoro z/OSMF di esempio e la modalità di esecuzione di un workflow.

File di dichiarazione delle variabili del workflow

I seguenti file dichiarano le variabili a cui fanno riferimento i flussi di lavoro z/OSMF di esempio e i file exec JCL o REXX associati:

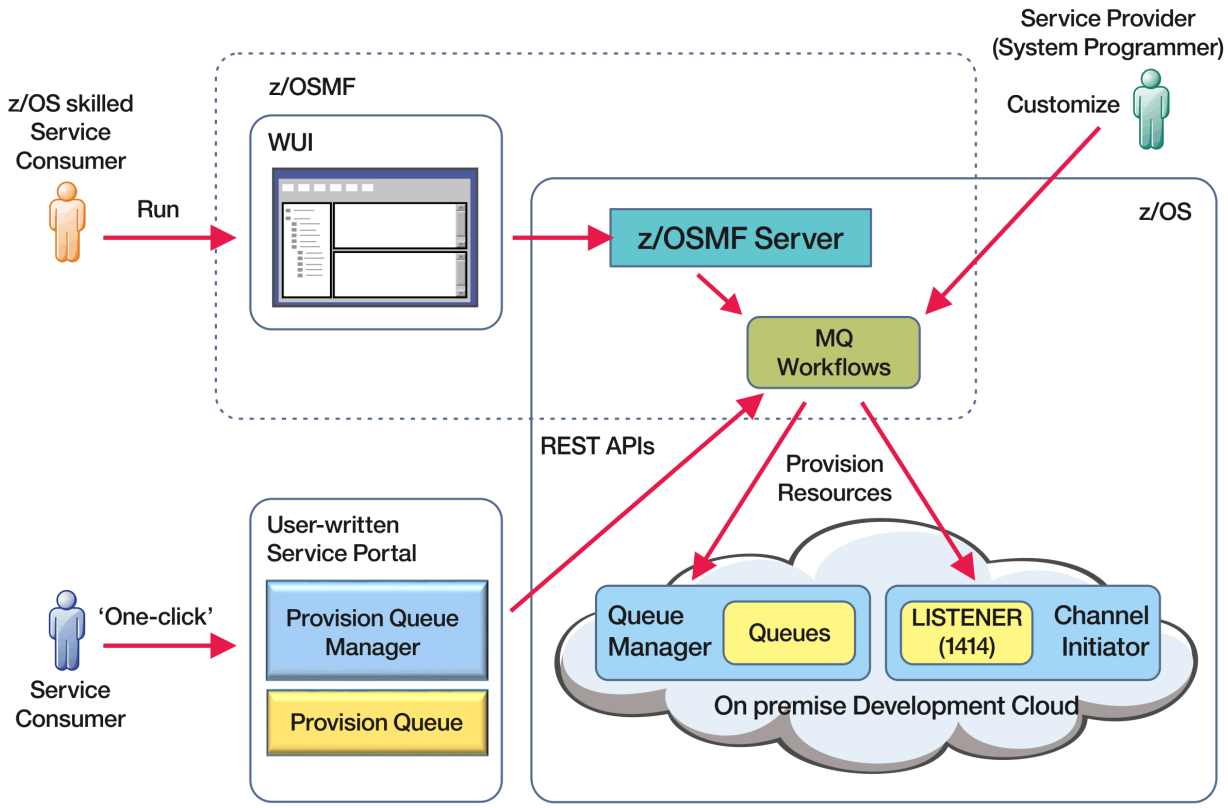
Nome file di dichiarazione della variabile del workflow	Descrizione
common_variables.xml	Variabili comuni sia al gestore code (più iniziatore del canale) che ai flussi di lavoro della coda.

Nome file di dichiarazione della variabile del workflow	Descrizione
qmgr_variables.xml	Variabili specifiche dei flussi di lavoro del gestore code (più iniziatore di canali).
queue_variables.xml	Variabili specifiche dei workflow della coda.
tcpip_variables.xml	Variabili specifiche dei flussi di lavoro del gestore code (più iniziatore del canale) e utilizzate per identificare le risorse TCP/IP.

Nota: La visibilità predefinita delle variabili è *private*. Per consentire alle variabili di essere sottoposte a query utilizzando z/OSMF REST API, le variabili selezionate sono state contrassegnate come *pubbliche*. Tuttavia, è possibile modificare la visibilità di una determinata variabile, se necessario.

Esecuzione dei flussi di lavoro

Figura 124. Provisioning 'one-click' delle risorse IBM MQ for z/OS



Prima di eseguire i flussi di lavoro, è necessario impostare alcune proprietà nel seguente file:

Nome file delle proprietà della variabile del workflow	Descrizione
workflow_variables.properties	Proprietà iniziali per le variabili del workflow. I commenti nel file indicano lo scopo di ciascuna proprietà. • Le proprietà tra meta - parentesi (<>) devono essere impostate su valori specifici dell'utente.

Nome file delle proprietà della variabile del workflow	Descrizione
	• Una proprietà di ambiente può essere impostata per eseguire il provisioning di gestori code per ambienti di sviluppo (DEV), di verifica (TEST), di garanzia della qualità (QA) o di produzione (PROD). Ulteriori impostazioni delle proprietà controllano le caratteristiche del gestore code di cui eseguire il provisioning per ciascun ambiente. Ad esempio, è possibile modificare il numero di log attivi o il numero di serie di pagine per ciascun tipo di ambiente. • Le altre proprietà sono impostate sui valori predefiniti di IBM MQ ma possono essere modificate per soddisfare le convenzioni locali, se necessario.

In generale, una volta impostate le proprietà, i flussi di lavoro possono essere eseguiti così come sono. Tuttavia, se necessario, è possibile personalizzare un flusso di lavoro per modificare o rimuovere i passi esistenti o per aggiungere nuovi passi.

I workflow possono essere eseguiti:

- Da z/OSMF WUI.

  Da Cloud Provisioning -> Servizi software in WUI, i flussi di lavoro possono essere eseguiti in modalità automatica o manuale. La modalità manuale è utile quando si esegue il test e in entrambe le modalità è possibile monitorare l'avanzamento di ogni fase del workflow.

  Per ulteriori dettagli, vedi Servizi di provisioning cloud e Crea un flusso di lavoro.
- Utilizzo di z/OSMF REST Workflow Services.

  REST Workflow Services può essere utilizzato per eseguire i flussi di lavoro tramite un REST API. Questa modalità è utile per creare operazioni con un solo clic da un portale scritto dall'utente.

  Per ulteriori informazioni, fai riferimento a Cloud provisioning REST APIse vedi anche z/OSMF workflow services.
- Utilizzo del portale marketplace di esempio fornito con z/OSMF.

Concetti correlati

“Automatizzare il provisioning di oggetti IBM MQ” a pagina 954
Gli esempi vengono forniti per automatizzare il provisioning dei gestori code e delle code locali.

z/OS MQ Adv. VUE V 9.1.0 Configurazione di IBM MQ Advanced for z/OS VUE

Utilizzare queste informazioni per configurare le funzioni disponibili con titolarità IBM MQ Advanced for z/OS VUE .

Informazioni su questa attività

È possibile abilitare le connessioni remote dell'agent Managed File Transfer con IBM MQ Advanced for z/OS Value Unit Edition.

Puoi utilizzare la connettività dai gestori code IBM MQ Advanced for z/OS Value Unit Edition al servizio IBM Blockchainin IBM Cloud (formerly Bluemix).

V 9.1.0 È possibile connettere un'applicazione IBM MQ classes for JMS, o IBM MQ classes for Java, a un gestore code su z/OS, che dispone dell'attributo **ADVCAP(ENABLED)** , utilizzando una connessione client. Per ulteriori informazioni, consultare Java e la connettività client JMS ai z/OS gestori code.

Procedura

1. Abilitare le connessioni remote dell'agente Managed File Transfer con IBM MQ Advanced for z/OS Value Unit Edition.
2. Configurare IBM MQ Advanced for z/OS VUE per l'utilizzo con il servizio IBM Blockchain in IBM Cloud.

z/OS MQ Adv. VUE V 9.1.0 Abilitazione della connettività dell'agente MFT ai gestori code z/OS remoti

Gli agent Managed File Transfer su z/OS, in esecuzione con l'identificativo del prodotto (PID) di IBM MQ Advanced for z/OS VUE, possono connettersi ad un gestore code remoto su z/OS utilizzando una connessione client.

Quando un agent viene avviato, scrive un messaggio BFGPR0137I nel relativo log eventi (output0.log) che mostra il PID con cui è in esecuzione. Un esempio di questo messaggio è:

```
BFGPR0137I: Registrazione dei dati di utilizzo del prodotto avviata per il prodotto 'MQ z/OS
MFT', id prodotto '5655-MF9'.
```

Per i dettagli sui prodotti IBM MQ , i valori PID associati e le classificazioni di esportazione, consultare IBM MQ Identificativi prodotto e informazioni di esportazione.

Un agent MFT su z/OS, in esecuzione in un qualsiasi altro PID, può connettersi a un gestore code locale utilizzando solo la connessione di bind.

Un agente MFT su z/OS può connettersi solo ad un gestore code, anch'esso in esecuzione su z/OS, indipendentemente dal PID MFT .

Se un agent IBM MQ Advanced for z/OS VUE tenta di collegarsi a un gestore code non in esecuzione su z/OS, viene emesso il messaggio BFGQM1044E: `La connessione client agent su z/OS deve essere a un gestore code su z/OS` e l'avvio dell'agent viene terminato.

Attività correlate

Avvio di un agent MFT su z/OS

z/OS Linux MQ Adv. VUE V 9.1.0 Configurazione di IBM MQ Advanced for z/OS VUE per l'utilizzo con blockchain

Imposta ed esegui IBM MQ Bridge to blockchain per connettere in modo sicuro un gestore code IBM MQ su z/OS e IBM Blockchain. Utilizza il bridge per connettersi in modo asincrono, cercare e aggiornare lo stato di una risorsa nella tua blockchain, utilizzando un'applicazione di messaggistica che si connette al tuo gestore code IBM MQ Advanced for z/OS VUE .

Prima di iniziare

- IBM MQ Bridge to blockchain è disponibile come parte di un Connector Pack su IBM MQ Advanced for z/OS Value Unit Edition 9.1.0. È possibile connettersi a gestori code IBM MQ Advanced for z/OS VUE in esecuzione sullo stesso livello di comando o su un livello superiore.
- IBM MQ Bridge to blockchain è supportato per l'utilizzo con la tua rete blockchain basata su Hyperledger Composer costruita su Hyperledger Fabric.
- IBM MQ Bridge to blockchain deve essere installato in un ambiente UNIX System Services e richiede Java runtime environment 8 da IBM.

Informazioni su questa attività

Blockchain è un libro mastro condiviso, distribuito, digitale che consiste in una catena di blocchi che rappresentano le transazioni concordate tra peer in una rete. Ogni blocco nella catena è collegato al blocco precedente, e così via, di nuovo alla prima transazione.

IBM Blockchain si basa su Hyperledger Fabric e Hyperledger Composer. Puoi sviluppare con esso localmente con Dockero in un cluster del contenitore in IBM Cloud. È inoltre possibile attivare e utilizzare

la rete IBM Blockchain in produzione, per creare e gestire una rete di business con livelli elevati di sicurezza, riservatezza e prestazioni. Per ulteriori informazioni, vedi IBM Blockchain Platform.

Hyperledger Fabric e Hyperledger Composer sono un framework blockchain aziendale open source sviluppato in modo collaborativo dai membri di Hyperledger Project, incluso IBM come contributore del codice iniziale. Hyperledger Project, o Hyperledger, è un' Linux Foundation iniziativa collaborativa, globale e open source per promuovere le tecnologie blockchain intersettoriali. Per ulteriori informazioni, consultare IBM Blockchain, Hyperledger Progetti, Hyperledger Fabrice Hyperledger Composer.

Se stai già usando IBM MQ Advanced for z/OS VUE e IBM Blockchain, puoi utilizzare IBM MQ Bridge to blockchain per guidare il tuo modello di business Hyperledger Composer attraverso l'interfaccia REST Hyperledger Composer , consentendoti di aggiornare o interrogare lo stato nella tua blockchain e ricevere risposte dalla tua rete blockchain. In questo modo, puoi integrare il tuo software IBM in loco con un servizio blockchain cloud o una soluzione in loco gestita localmente.

Una breve panoramica del processo operativo del bridge può essere visualizzata nella Figura 1. Un'applicazione utente inserisce un messaggio in formato JSON nella coda di input / richiesta sul gestore code z/OS . Utilizzando il server REST Hyperledger Composer , il bridge si connette al gestore code, richiama il messaggio dalla coda di input / richiesta, controlla che il JSON sia formattato correttamente, quindi invia la richiesta REST alla blockchain. I dati restituiti dalla blockchain vengono analizzati dal bridge e inseriti nella coda di risposta, come definito nel messaggio di richiesta IBM MQ originale. L'applicazione utente può connettersi al gestore code, ricevere il messaggio di risposta dalla coda di risposte e utilizzare le informazioni.

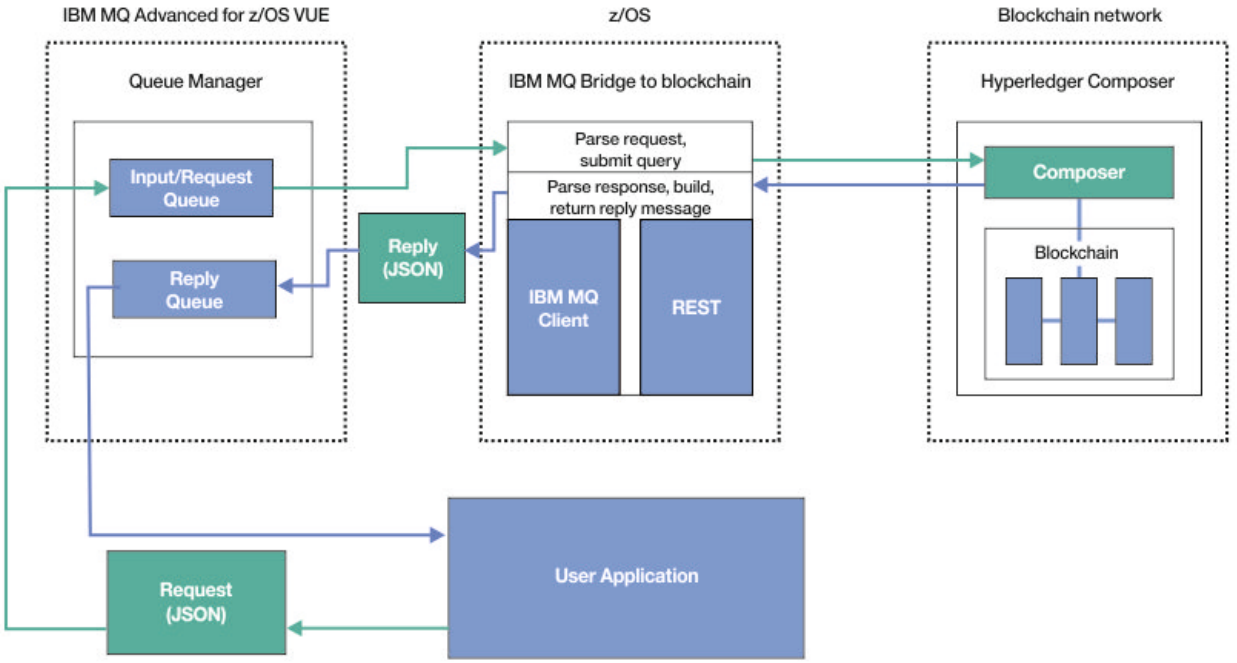


Figura 125. IBM MQ Bridge to blockchain

È necessario configurare IBM MQ Bridge to blockchain per connettersi direttamente a un server REST Hyperledger Composer piuttosto che al livello Hyperledger Fabric sottostante. Quando il bridge è in esecuzione, un'applicazione di messaggistica richiede al bridge di guidare l'API REST Hyperledger Composer , in base al modello di rete di business definito dall'utente, che a sua volta guida le routine del chaincode sottostanti che possono eseguire query o aggiornare lo stato della risorsa e restituire i risultati come risposta utilizzando il server REST Hyperledger Composer , all'applicazione di messaggistica.

Procedura

Creare le code per il bridge, personalizzando e inoltrando il JCL di esempio in `thlqual.SCSQPROC(CSQ4BCBQ)`.

Le definizioni di coda bridge di esempio vengono fornite per le code denominate predefinite utilizzate per:

- Input del messaggio al bridge: `SYSTEM.BLOCKCHAIN.INPUT.QUEUE`e `APPL1.BLOCKCHAIN.INPUT.QUEUE` .
- Risposte da blockchain: `APPL1.BLOCKCHAIN.REPLY.QUEUE`

Applicazioni differenti possono utilizzare la stessa coda di input, ma è possibile specificare più code di risposta, una per ogni applicazione. Non è necessario utilizzare code di risposta definite. Se si desidera utilizzare le code dinamiche per le risposte, è necessario considerarne la configurazione di sicurezza.

Risultati

Hai creato le code richieste dal bridge per elaborare i messaggi da IBM MQ e dalla tua rete blockchain.

Operazioni successive

Utilizza le informazioni per il tuo gestore code e le credenziali dalla tua rete blockchain per creare un file di configurazione per IBM MQ Bridge to blockchain.

z/OS MQ Adv. VUE V 9.1.0 Creazione del file di configurazione per IBM MQ Bridge to blockchain

Immetti il tuo gestore code e i tuoi parametri di rete blockchain per creare il file di configurazione per IBM MQ Bridge to blockchain per la connessione alle tue reti IBM MQ e IBM Blockchain .

Prima di iniziare

- Hai creato e configurato la tua rete blockchain Hyperledger Composer .
- Hai installato IBM MQ Bridge to blockchain nel tuo ambiente z/OS .
- È stato avviato il gestore code IBM MQ Advanced for z/OS VUE .

Informazioni su questa attività

Questa attività consente di eseguire la configurazione minima necessaria per creare il file di configurazione IBM MQ Bridge to blockchain e connettersi correttamente alle reti IBM Blockchain e IBM MQ .

Puoi utilizzare il bridge per connetterti alle reti blockchain basate su Hyperledger Composer. Per utilizzare il bridge, hai bisogno di informazioni di configurazione dalla tua rete blockchain. In ogni passo di questa attività puoi individuare i dettagli di configurazione di esempio basati su due reti blockchain configurate in modo diverso:

- Rete Hyperledger Composer in esecuzione in Docker. Per ulteriori informazioni, vedi Installazione di Hyperledger Composere Generazione di un'API REST.
- Rete Hyperledger Composer eseguita in un cluster Kubernetes in IBM Cloud. Per ulteriori informazioni, vedi Develop in a cloud sandbox on IBM Blockchain Platform.

Per ulteriori informazioni sul significato e sulle opzioni per tutti i parametri IBM MQ Bridge to blockchain , consultare il comando runmqbcb . È necessario considerare i propri requisiti di sicurezza e personalizzare i parametri appropriati per la propria distribuzione.

Procedura

1. Eseguire il bridge nell'ambiente USS (UNIX System shell) per creare un file di configurazione.

   Hai bisogno dei parametri dalle informazioni di sicurezza Hyperledger Composer e dal tuo gestore code IBM MQ Advanced for z/OS VUE .

Eseguire lo script del bridge dalla directory `mqbc/bin` dell'ubicazione in USS in cui è installato IBM MQ .

```
./runmqbcb -o config_file_name.cfg
```

Come illustrato nel seguente esempio, i valori esistenti vengono visualizzati all'interno delle parentesi. Premere `Enter` per accettare i valori esistenti, premere `Space` quindi `Enter` per cancellare i valori e digitare all'interno delle parentesi, quindi premere `Enter` per aggiungere nuovi valori. È possibile separare gli elenchi di valori (come i peer) mediante virgole o immettendo ciascun valore su una nuova riga. Una riga vuota termina l'elenco.

Nota: Non è possibile modificare i valori esistenti. È possibile conservarli, sostituirli o cancellarli.

2. Immettere i valori per la connessione al gestore code IBM MQ Advanced for z/OS VUE .

   I valori minimi necessari per la connessione sono il nome del gestore code e i nomi delle code di input del bridge definite. Per le connessioni ai gestori code IBM MQ Advanced for z/OS VUE remoti, sono necessari anche **`MQ Channel`** e **`MQ Conname`** (indirizzo host e porta su cui è in esecuzione il gestore code).

   Per utilizzare TLS per la connessione a IBM MQ nel passo “5” a pagina 963, è necessario utilizzare JNDI o CCDT e specificare **`MQ CCDT URL`** o **`JNDI implementation class`** e **`JNDI provider URL`** di conseguenza.

   Nota: I valori **`MQ CCDT`** o **`JNDI`** hanno la precedenza sul file di configurazione in cui i valori si sovrappongono.

```
Connection to Queue Manager
---------------------------
Queue Manager                     : [z/OS_ADV_VUE_qmgr_name]
Bridge Input Queue                : [APPL1.BLOCKCHAIN.INPUT.QUEUE]
MQ Channel                        : []
MQ Conname                        : []
MQ CCDT URL                       : []
JNDI implementation class         : []
JNDI provider URL                 : []
MQ Userid                         : []
MQ Password                       : []
```

3. Immetti le credenziali per il server REST Hyperledger Composer associato alla tua rete blockchain (se configurato).

   Nel seguente esempio, il server REST Hyperledger Composer è stato configurato con un archivio credenziali LDAP utilizzando il modulo **`passport-ldapauth NodeJS`** . Notare che è possibile utilizzare uno qualsiasi dei moduli **`passport-*`** che forniscono credenziali di base in stile utente e password in questo modo. Per ulteriori informazioni, consultare Abilitazione dell'autenticazione per il server REST.

```
User Identification
-------------------------------
Userid                          : []admin
Password                        : []******
API path for Login              : auth/ldap
```

4. Immettere l'indirizzo per il server REST Hyperledger Composer .

   Notare che in questo attributo non è necessario alcun protocollo, ovvero `http` o `https`, e che il numero di porta è obbligatorio. L'utilizzo del protocollo HTTP o HTTPS dipende dalla configurazione di sicurezza del server REST. Se vengono forniti un certificato e una chiave privata al server REST, viene utilizzato HTTPS. Viene utilizzato HTTPS. Altrimenti, viene utilizzato HTTP. Per informazioni su come specificare il certificato e la coppia di chiavi private, consultare il passo “5” a pagina 963.

```
REST Server
---------------------------
Address for Composer REST server     : [composer-rest-server-ip-address:3000]
```

5. Immettere i valori di memorizzazione certificato per connessioni TLS.

Il bridge funge da un client IBM MQ JMS che si connette a un gestore code, il che significa che può essere configurato per utilizzare la sicurezza TLS per connettersi in modo sicuro come qualsiasi altro client IBM MQ JMS . La configurazione dei dettagli di connessione TLS viene esposta solo dopo aver specificato le informazioni JNDI o CCDT nel passo “2” a pagina 963.

Gli archivi di certificati vengono utilizzati per Hyperledger Composere per il gestore code IBM MQ Advanced for z/OS VUE . Se vengono specificati gli archivi di certificati, il bridge tenta sempre di connettersi al server REST Hyperledger utilizzando HTTPS. Tuttavia, TLS può essere disabilitato per le connessioni IBM MQ , mentre ancora utilizza TLS per Hyperledger Composer utilizzando la seguente opzione.

```
Certificate stores for TLS connections
--------------------------------------
Personal keystore                    : []
Keystore password                    : []
Trusted store for signer certs       : []
Trusted store password               : []
Use TLS for MQ connection            : [N]
Timeout for Blockchain operations    : [12]
```

Per ulteriori informazioni, consultare Protezione del server REST utilizzando HTTPS e TLS.

6. Opzionale: Immettere l'ubicazione del file di log per IBM MQ Bridge to blockchain.

   È possibile specificare il nome e l'ubicazione del file di log, nel file di configurazione o sulla riga comandi.

```
Behavior of bridge program
--------------------------
Runtime logfile for copy of stdout/stderr : [/var/mqm/errors/runmqbcb.log]
Done.
```

Risultati

È stato creato il file di configurazione che IBM MQ Bridge to blockchain utilizza per connettersi alla rete IBM Blockchain e al gestore code IBM MQ Advanced for z/OS VUE .

Operazioni successive

Eseguire le operazioni per “Esecuzione di IBM MQ Bridge to blockchain” a pagina 965

Riferimenti correlati

runmqbcb (eseguire IBM MQ Bridge to blockchain)

z/OS V 9.1.0 Configurazione di sicurezza IBM MQ per IBM MQ Bridge to blockchain

Considerazioni per l'impostazione della sicurezza IBM MQcon IBM MQ Bridge to blockchain.

I seguenti esempi mostrano le definizioni RACF che possono essere utilizzate per fornire l'accesso IBM MQ Bridge to blockchain alle code di cui ha bisogno. Le definizioni presuppongono che il bridge sia in esecuzione con ID utente MQBCBUSR.

Inoltre, è necessario fornire a IBM MQ Bridge to blockchain l'accesso per la connessione al gestore code:

- Direttamente utilizzando la modalità bind; consultare Profili di sicurezza della connessione per le connessioni batchoppure
- Utilizzo di una modalità client tramite CHINIT; consultare Richieste MQI client

Autorizzazione per la coda di richiesta IBM MQ Bridge to blockchain

Immettere i seguenti comandi RACF per concedere all'ID utente MQBCBUSR l'accesso per ricevere i messaggi dal sistema SYSTEM.BLOCKCHAIN.INPUT.QUEUE QUEUE:

```
RDEFINE MQQUEUE SYSTEM.BLOCKCHAIN.INPUT.QUEUE UACC(NONE)
PERMIT SYSTEM.BLOCKCHAIN.INPUT.QUEUE CLASS(MQQUEUE) ID(MQBCBUSR) ACCESS(UPDATE)
```

Autorizzazione per la coda di risposta IBM MQ Bridge to blockchain

Immettere i seguenti comandi RACF per concedere all'ID utente MQBCBUSR l'accesso per inviare messaggi a APPL1.BLOCKCHAIN.REPLY.QUEUE. Questo nome di coda è specificato nel nome della coda di risposta nel messaggio di richiesta:

```
RDEFINE MQQUEUE APPL1.BLOCKCHAIN.REPLY.QUEUE UACC(NONE)
PERMIT APPL1.BLOCKCHAIN.REPLY.QUEUE CLASS(MQQUEUE) ID(MQBCBUSR) ACCESS(UPDATE)
PERMIT CONTEXT.APPL1.BLOCKCHAIN.REPLY.QUEUE CLASS(MQADMIN) ID(MQBCBUSR) ACCESS(UPDATE)
```

Concetti correlati

Profili per la sicurezza della coda

Attività correlate

“Esecuzione dell'esempio client IBM MQ Bridge to blockchain” a pagina 818

Puoi utilizzare l'esempio del client JMS fornito con IBM MQ Bridge to blockchain, per inserire un messaggio nella coda di input che il bridge blockchain sta controllando e visualizzare la risposta ricevuta. Questo esempio si basa sull'utilizzo dell'integrazione di IBM MQ Bridge to blockchain con l'esempio di rete Hyperledger Composer Trader.

Riferimenti correlati

Guida di riferimento rapido per l'accesso alla sicurezza delle risorse API

z/OS MQ Adv. VUE V 9.1.0 Esecuzione di IBM MQ Bridge to blockchain

Eseguire IBM MQ Bridge to blockchain per connettersi a IBM Blockchain e IBM MQ. Quando è connesso, il bridge è pronto per elaborare i messaggi di richiesta, inviarli alla tua rete blockchain Hyperledger Composer e ricevere ed elaborare le risposte.

Informazioni su questa attività

Utilizzare il file di configurazione creato nell'attività precedente per eseguire IBM MQ Bridge to blockchain.

Procedura

1. Avviare il gestore code IBM MQ Advanced for z/OS VUE che si desidera utilizzare con il bridge.
2. Avvia IBM MQ Bridge to blockchain per connetterti alla tua rete blockchain e al tuo gestore code IBM MQ Advanced for z/OS VUE .

   Le alternative sono:

   a) Eseguire il bridge direttamente in UNIX System Services (USS) dalla directory `mqbc/bin` nell'ubicazione USS in cui è installato IBM MQ .

   ```
   ./runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/logFile.log
   ```

   o

   b) b. Eseguire il bridge nel sistema z/OS , utilizzando il JCL di esempio fornito in `thlqual.SCSQPROC(CSQ4BCB)`.

   È necessario effettuare una serie di aggiornamenti al JCL, specifici per l'ambiente:

   - Sostituire ++THLQUAL++ con il qualificatore di livello superiore dei dataset della libreria di destinazione IBM MQ .
   - Sostituire ++LANGLETTER++ con la lettera della lingua in cui si desidera visualizzare i messaggi.

- Sostituire ++PATHPREFIX++ con il percorso di installazione dei componenti USS IBM MQ for z/OS .
- Sostituire ++CONFIGFILE++ con il percorso di un file di configurazione creato utilizzando il comando `runmqbc -o <file>` da USS.
- Sostituire ++JAVAHOME++ con l'ubicazione di una JVM (Java Virtual Machine) a 64 bit in esecuzione su Java 8 o versioni successive.

Quando il bridge è collegato, viene restituito un output simile al seguente:

```
2018-05-17 14:28:16.866 BST IBM MQ Bridge to Blockchain
5724-H72 (C) Copyright IBM Corp. 2017, 2024.

2018-05-17 14:28:19.331 BST Ready to process input messages.
```

3. Opzionale: Risolvi i problemi di connessioni al tuo gestore code IBM MQ Advanced for z/OS VUE e alla tua rete blockchain, se i messaggi restituiti dopo che hai eseguito il bridge indicano che una connessione non è riuscita.
   a) Immettere il comando in modo debug con l'opzione di debug 1.

   ```
   ./runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/
   logFile.log -d 1
   ```

   Il bridge passa attraverso la configurazione della connessione e mostra i messaggi di elaborazione in modalità concisa.

   b) Immettere il comando in modo debug con l'opzione di debug 2.

   ```
   ./runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/
   logFile.log -d 2
   ```

   Il bridge passa attraverso la connessione impostata e mostra i messaggi di elaborazione in modalità dettagliata. L'output completo viene scritto nel file di log.

   Tenere presente che, facoltativamente, è anche possibile specificare le opzioni della modalità di debug all'interno del JCL modificando '`-d 0`' in '`-d 1`' o '`-d 2`'.

Risultati

Hai avviato IBM MQ Bridge to blockchain e ti sei connesso al tuo gestore code e alla tua rete blockchain.

Operazioni successive

- Segui i passi in “Esecuzione dell'esempio client IBM MQ Bridge to blockchain” a pagina 818 per formattare e inviare un messaggio di query o di aggiornamento alla tua rete blockchain.
- Utilizzare la variabile *MQBCB_EXTRA_JAVA_OPTIONS* per passare le proprietà JVM, ad esempio per abilitare la funzione di traccia IBM MQ . Per ulteriori informazioni, consultare Traccia di IBM MQ Bridge to blockchain.

z/OS V 9.1.0 *Formati dei messaggi per IBM MQ Bridge to blockchain prima IBM MQ 9.1.4*

Informazioni sulla formattazione dei messaggi inviati e ricevuti da IBM MQ Bridge to blockchain.

LTS

Attenzione: Il formato esistente per i formati del messaggio è obsoleto. Da IBM MQ 9.1.4, se si dispone di una rete Hyperledger Fabric , utilizzare il formato dei messaggi descritti in “Formati dei messaggi per IBM MQ Bridge to blockchain da IBM MQ 9.1.4” a pagina 817.

Un'applicazione richiede che IBM MQ Bridge to blockchain esegua l'API REST definita da Hyperledger Composer per agire sulle informazioni contenute nella blockchain. L'applicazione esegue questa operazione inserendo un messaggio di richiesta nella coda di richiesta bridge. I risultati della richiesta REST vengono formattati dal ponte in un messaggio di risposta. Il bridge utilizza le informazioni contenute

nei campi **ReplyToQ** e **ReplyToQMgr** da MQMD del messaggio di richiesta come destinazione per il messaggio di risposta.

I messaggi di richiesta e risposta sono messaggi di testo (MQSTR) in formato JSON.

Formato messaggio di richiesta

I messaggi di richiesta contengono tre attributi:

metodo
Il verbo REST utilizzato per richiamare la API REST Hyperledger Composer , come POST, DELETE o GET

percorso
Il percorso dell'API REST Hyperledger Composer . Questo viene aggiunto all'URL del server di base. Il percorso deve iniziare con "`api/`".

corpo
Il contenuto specifico del metodo. Questa è spesso una struttura JSON.

Il seguente esempio utilizza il metodo POST , per il percorso `api/Trader`, per creare un nuovo oggetto Trader. Il corpo specifica la classe Traders, come definito dal modello Hyperledger Composer dell'utente, e specifica anche i valori aggiuntivi necessari per creare un nuovo oggetto Trader all'interno della rete blockchain.

```
{ "method": "POST",
  "path": "api/Trader",
  "body": {
    "$class" : "org.example.trading",
    "tradeId" : "Trader2",
    "firstName": "Jane",
    "lastName" : "Doe"
```

Formato messaggio di risposta

L'ID di correlazione dei messaggi di risposta è impostato sull'ID del messaggio in entrata. Tutte le proprietà definite dall'utente vengono copiate dal messaggio di richiesta al messaggio di risposta. L'ID utente nella risposta è impostato sull'ID utente del mittente.

statusCode è un codice di stato HTTP. Se l'errore proviene da IBM MQ o dal bridge, viene utilizzato un **statusCode** appropriato.

statusType è una stringa, *SUCCESS* o *FAILURE*.

Per le richieste con esito positivo, l'elemento "**data**" nel messaggio di risposta contiene la risposta dall'API REST Hyperledger Composer richiamata.

Un esempio di elaborazione riuscita:

```
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "data": [
      {
         "$class": "org.example.trading",
         "firstName": "John",
         "lastName": "Doe",
         "tradeId": "Trader1"
      },
      {
         "$class": "org.example.trading",
         "firstName": "Jane",
         "lastName": "Doe",
         "tradeId": "Trader2"
      }
   ]
}
```

Tutte le risposte di errore hanno gli stessi campi, indipendentemente dal fatto che siano generati dal bridge stesso, dalle chiamate al server REST Hyperledger Composer , alla blockchain o dal richiamo del chaincode. Ad esempio:

- Messaggio di input JSON errato

```
{
   "statusCode": 400,
   "statusType": "FAILURE",
   "message": "[AMQBC021E] Error: Cannot parse input message or there are
    missing fields in the message. Missing fields appear to be: "method".”
}
```

- Richiesta che non è stata elaborata dal server REST Hyperledger Composer

```
{
   "statusCode": 500,
   "statusType": "FAILURE",
   "message": "Error trying to invoke business network. Error: No valid responses
    from any peers.\nResponse from attempted peer comms was an error: Error: chaincode
    error (status: 500, message: Error: Failed to add object with ID 'Trader1'
    as the object already exists)"
}
```

Le applicazioni possono indicare se la richiesta ha avuto esito positivo o negativo esaminando la stringa **statusType** o l'esistenza del campo di dati. Quando si verifica un errore nell'elaborazione del messaggio di input e il bridge non lo invia alla blockchain, il valore restituito dal bridge è un valore MQRC, di norma **MQRC_FORMAT_ERROR**.

z/OS V 9.1.0 *Esecuzione dell'esempio client IBM MQ Bridge to blockchain*

Puoi utilizzare l'esempio del client JMS fornito con IBM MQ Bridge to blockchain, per inserire un messaggio nella coda di input che il bridge blockchain sta controllando e visualizzare la risposta ricevuta. Questo esempio si basa sull'utilizzo dell'integrazione di IBM MQ Bridge to blockchain con l'esempio di rete Hyperledger Composer Trader.

Prima di iniziare

Per ulteriori informazioni, vedi /trade_network

Il tuo IBM MQ Bridge to blockchain è in esecuzione ed è connesso al tuo gestore code IBM MQ Advancedo IBM MQ Advanced for z/OS VUEe alla tua rete blockchain.

Informazioni su questa attività

Trovare l'applicazione di esempio JMS (`ComposerBCBSamp.java`) nella directory `samp` di IBM MQ Bridge to blockchain.

Ad esempio: `<MQ_INSTALL_ROOT>/mqbc/samp/ComposerBCBSamp.java`, dove `<MQ_INSTALL_ROOT>` è:

- Linux Directory in cui è installato IBM MQ
- z/OS Directory USS in cui sono installati i componenti USS di IBM MQ

.

Procedura

1. Modificare il file di origine Java di esempio client.

   Segui le istruzioni nell'esempio per configurarlo in modo che corrisponda al tuo ambiente IBM MQ e alla tua rete blockchain.

Il seguente codice dell'esempio definisce tre messaggi di richiesta JSON da inviare al bridge:

a. In primo luogo, per rimuovere un '`commodity`' esistente

b. In secondo luogo, per creare un nuovo '`commodity`', '`owner`' e i valori associati,

c. Infine, visualizza le nuove informazioni su '`commodity`', seguendo i due messaggi di richiesta precedenti

```
private static JSONObject[] createMessageBodies() {
    JSONObject[] msgs = new JSONObject[3]; // This method creates 3 messages
    JSONObject m, m2;
    String commodityName = "BC";

    // Clean out the commodity in case it's already there. If
    // it's not there, there will be an error returned from Composer.
    m = new JSONObject();
    m.put("method", "DELETE");
    m.put("path", "api/Commodity/" + commodityName);
    msgs[0] = m;

    // To add the item to the table, the
    // operation looks like this:
    //
    // { "method": "POST",
    //   "path": "api/Commodity",
    //   "body" : {
    //     "$class": "org.example.trading.Commodity",
    //     "tradingSymbol" : "BC",
    //     "description" : "BC",
    //     "mainExchange" : "HERE",
    //     "owner" : "Me",
    //     "quantity" : 100
    //   }
    // }
    // You can see this structure in the API Explorer
    m = new JSONObject();
    m.put("method", "POST");
    m.put("path", "api/Commodity");
    m2 = new JSONObject();
    m2.put("$class", " org.example.trading.Commodity");
    m2.put("tradingSymbol", commodityName);
    m2.put("description", "Blockchain Sample Description");
    m2.put("mainExchange", "My Exchange");
    m2.put("owner", "Me");
    m2.put("quantity", 100);
    m.put("body", m2);
    msgs[1] = m;

    // And list all items that have been created
    m = new JSONObject();
    m.put("method", "GET");
    m.put("path", "api/Commodity");
    msgs[2] = m;

    return msgs;
  }
```

2. Compilare l'esempio.

   Puntare alle classi client IBM MQ e al file `JSON4J.jar` fornito nella directory bridge.

```
javac -cp <MQ_INSTALL_ROOT>/java/lib/*:<MQ_INSTALL_ROOT>/mqbc/prereqs/JSON4J.jar
ComposerBCBClient.java
```

3. Eseguire la classe compilata.

```
java -cp <MQ_INSTALL_ROOT>/java/lib/*:<MQ_INSTALL_ROOT>/mqbc/prereqs/JSON4J.jar:.
ComposerBCBClient
```

```
Starting Simple MQ Blockchain Bridge Client
Starting the connection.
Sent message:
  {"method":"DELETE"," path ":"api\/Commodity\/BC"}
```

```
Response text:
{
   "statusCode": 204,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": ""
}
SUCCESS
Sent message:
{"body":
{"$class":"org.example.trading.Commodity","owner":"Me","quantity":100,"description":"Blockcha
in Sample Description","mainExchange":"My
Exchange","tradingSymbol":"BC"},"operation":"POST","url":"Commodity"}
Response text:
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": {
      "$class": "org.example.trading.Commodity",
      "description": "Blockchain Sample Description",
      "mainExchange": "My Exchange",
      "owner": "Me",
      "quantity": 100,
      "tradingSymbol": "BC"
   }
}
SUCCESS
Sent message:
  {"method":"GET","path":"api\/Commodity"}
Response text:
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": [
      {
         "$class": "org.example.trading.Commodity",
         "description": "Blockchain Sample Description",
         "mainExchange": "My Exchange",
         "owner": "resource:org.example.trading.Trader#Me",
         "quantity": 100,
         "tradingSymbol": "BC"
      }
   ]
}
SUCCESS
```

Il campo **message** contiene "OK" per un messaggio elaborato correttamente oppure, in caso di richiesta non riuscita, informazioni relative al motivo dell'errore.

Se il client riceve un errore di timeout in attesa della risposta, verificare che il bridge sia in esecuzione.

Configurazione di IBM MQ Internet Pass-Thru

Questa sezione descrive le varie funzioni supportate da IBM MQ Internet Pass-Thru (MQIPT) e come configurarle.

Le proprietà che possono essere specificate nel file di configurazione MQIPT sono descritte in IBM MQ Internet Pass-Thru configuration reference.

Supporto per HTTP in MQIPT

MQIPT supporta il tunneling HTTP. MQIPT può essere configurato in modo che i pacchetti di dati inoltrati siano codificati come richieste HTTP.

I canali IBM MQ non accettano richieste HTTP. Pertanto, è necessario un secondo MQIPT per ricevere le richieste HTTP e convertirle nuovamente in normali pacchetti del protocollo IBM MQ . Il secondo MQIPT elimina l'intestazione HTTP per convertire nuovamente il pacchetto in entrata in un pacchetto di protocollo standard IBM MQ , prima di trasmetterlo al gestore code di destinazione.

Quando HTTP viene utilizzato tra due istanze di MQIPT, la connessione TCP/IP su cui il flusso di risposte e richieste HTTP è persistente e viene mantenuta aperta per la durata del canale di messaggi. MQIPT non chiude la connessione TCP/IP tra le coppie richiesta/risposta.

Se due istanze di MQIPT stanno comunicando tramite HTTP, è possibile che una richiesta HTTP rimanga in sospeso per un periodo prolungato. Un esempio è in un canale richiedente / server, quando il lato server è in attesa dell'arrivo di nuovi messaggi sulla propria coda di trasmissione. Il protocollo del canale IBM MQ fornisceun meccanismo "heartbeat", che richiede la fine dell'attesa periodicamente per inviare messaggi heartbeat al partner. Il periodo di heartbeat del canale predefinito è 5 minuti. MQIPT utilizza questo heartbeat come risposta HTTP. Non disabilitare questo heartbeat del canale o impostarlo su un valore eccessivamente elevato, per evitare di causare problemi con i timeout in alcuni firewall.

MQIPT accetta il traffico HTTP in formato suddiviso in blocchi, generato da un server o un proxy HTTP.

Per un esempio di utilizzo di HTTP in MQIPT, consultare Configurazione del tunneling HTTP.

Proxy HTTP

Un proxy HTTP può essere inserito tra le due istanze di MQIPT. Il proxy HTTP deve soddisfare i seguenti requisiti:

- Il proxy deve supportare il protocollo HTTP 1.1 .
- Le intestazioni HTTP **Connection** o **Proxy-Connection** impostate da MQIPT devono essere rispettate dal proxy. Ciò consente di mantenere aperte le connessioni tra due istanze di MQIPT per la durata del canale di messaggi.
- È necessario mantenere un'associazione uno - a - uno di connessioni persistenti nel proxy. Ciò garantisce che le connessioni TCP/IP dal proxy alla destinazione MQIPT non vengano utilizzate per trasmettere i dati per più di un canale di messaggi.

È possibile impostare le proprietà per configurare la modalità di gestione delle connessioni persistenti su alcuni proxy HTTP. Ad esempio, è possibile impostare il numero massimo di richieste che possono essere effettuate su una connessione persistente. È necessario impostare le seguenti proprietà:

- Le connessioni persistenti dovrebbero essere abilitate.
- Il riutilizzo delle connessioni TCP/IP dal proxy a MQIPT da parte di più di una sessione HTTP deve essere disabilitato, per mantenere un'associazione uno - a - uno di connessioni persistenti attraverso il proxy.
- Il timeout sulle richieste proxy deve essere impostata su un valore elevato. Ad esempio, 12 ore.
- Il numero massimo di richieste che possono essere effettuate su una connessione persistente deve essere impostato su un valore elevato. Ad esempio, 5000.

MQIPT utilizza richieste HTTP **POST** per inviare dati tra le due istanze di MQIPT. Se la configurazione MQIPT specifica il nome host del proxy utilizzando la proprietà **HTTPProxy** , MQIPT si connette al proxy e utilizza il metodo HTTP **CONNECT** per richiedere che il proxy stabilisca un tunnel per la destinazione MQIPT. Ciò consente alle connessioni HTTPS di passare attraverso il proxy senza terminare la sessione TLS nel proxy.

Se un programma di bilanciamento del carico viene inserito tra le istanze MQIPT , deve essere configurato per utilizzare il valore del cookie HTTP *MQIPTSessionId* per garantire che tutte le richieste per ogni sessione vengano inoltrate alla stessa destinazione.

HTTPS in MQIPT

HTTPS può essere utilizzato su una connessione HTTP abilitando le proprietà di instradamento **HTTPS** e **SSLClient** sul MQIPT che emette la connessione client.

MQIPT deve avere accesso al certificato CA attendibile che verrà utilizzato per autenticare il server / proxy HTTP di destinazione. La proprietà **SSLClientCAKeyring** può essere utilizzata per definire il file key ring contenente il certificato CA attendibile.

Una configurazione comune per HTTPS utilizzerà un proxy HTTP locale per eseguire il tunneling attraverso un firewall e connettersi a un server HTTP remoto (o un altro proxy), che a sua volta si connetterà al MQIPTremoto. Questo MQIPT sul lato server della connessione non richiede alcuna configurazione specifica, poiché la richiesta di connessione viene gestita come qualsiasi connessione HTTP normale.

MQIPT utilizza le proprietà **HTTPProxy** e **HTTPServer** per distinguere i proxy locali e remoti. L'instradamento MQIPT con la serie di proprietà **HTTPProxy** è visualizzato come proxy HTTP locale e l'instradamento MQIPT con la serie di proprietà **HTTPServer** è il server remoto (o proxy).

Le connessioni HTTPS vengono normalmente effettuate all'indirizzo di porta del listener 443 sul server / proxy HTTP, ma le proprietà **HTTPProxyPort** e **HTTPServerPort** possono essere utilizzate per sovrascrivere questo valore predefinito.

Supporto SOCKS in MQIPT

Un proxy SOCKS è un servizio di rete utilizzato come punto di uscita controllato attraverso un firewall. Un'applicazione abilitata SOCKS, in esecuzione all'interno del firewall, può utilizzare il proxy SOCKS per connettersi a un'applicazione remota.

MQIPT può fungere da proxy SOCKS abilitando la propriet ... **SocksServer** , consentendo quindi a un'applicazione IBM MQ abilitata a SOCKS di connettersi tramite MQIPT a un gestore code IBM MQ remoto. Quando si utilizza questa funzione, la destinazione e l'indirizzo della porta di destinazione vengono ottenuti durante il processo di handshake SOCKS e, pertanto, le proprietà di instradamento **Destination** e **DestinationPort** vengono sovrascritte. Questa è una funzione chiave per il supporto del cluster IBM MQ .

MQIPT può anche agire come un client SOCKS, per conto di un'applicazione IBM MQ locale che non è stata abilitata SOCKS. Ciò è utile quando si utilizza un firewall che consente connessioni in uscita solo tramite un proxy SOCKS. Ogni instradamento MQIPT può essere configurato per comunicare con un proxy SOCKS differente.

Consultare Configurazione di un proxy SOCKS per un esempio di come utilizzare SOCKS.

Cluster in MQIPT

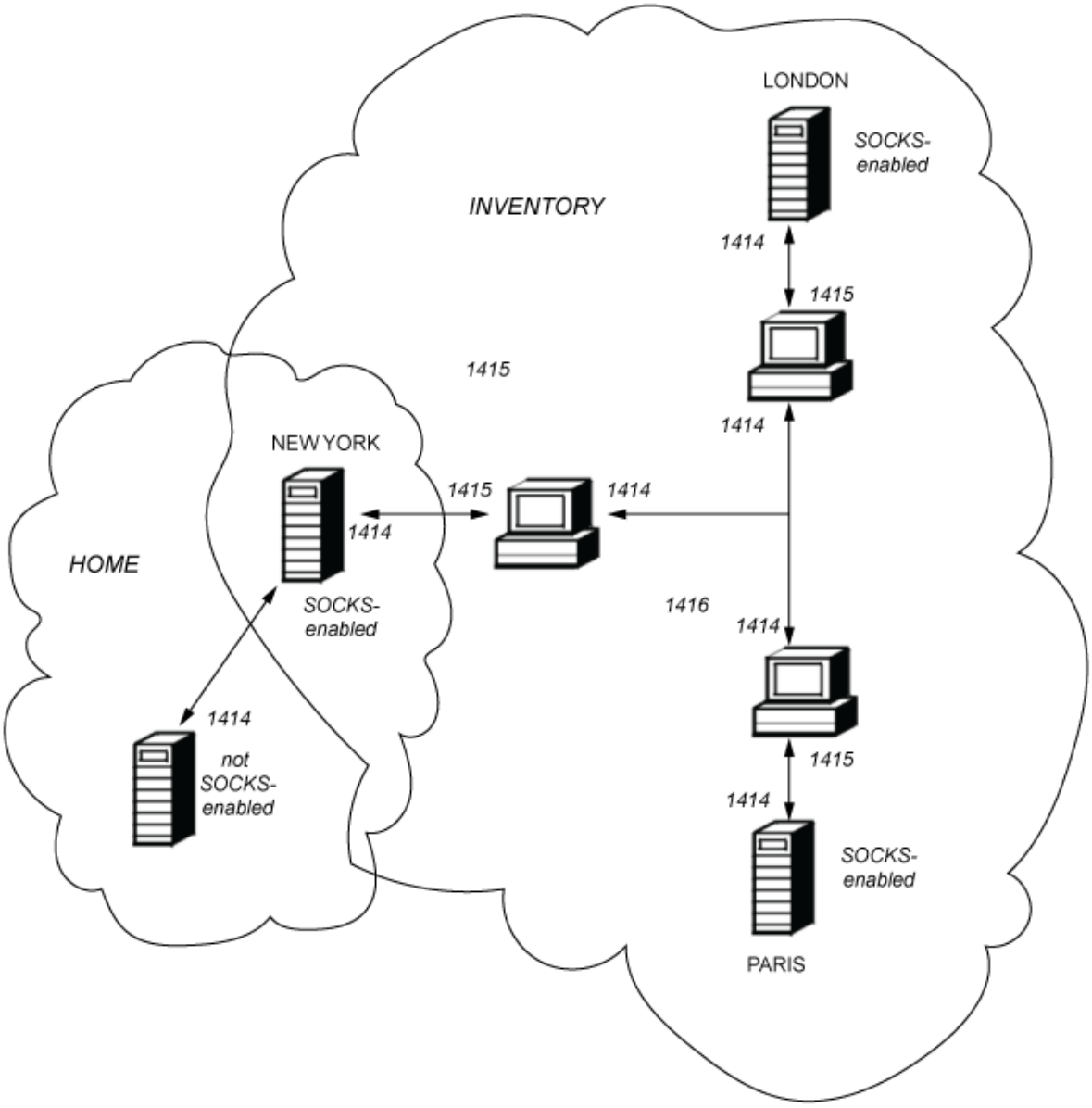
I cluster IBM MQ possono essere utilizzati con MQIPT da SOCKS - abilitando ogni gestore code nel cluster che si estende su Internet e abilitando MQIPT ad agire come proxy SOCKS.

Nel seguente diagramma, NEWYORK e CHICAGO si trovano in un cluster denominato HOME ed entrambi contengono repository completi. NEWYORK, LONDRA e PARIGI si trovano in un altro cluster chiamato INVENTORY. Nota che CHICAGO non ha bisogno di essere abilitato a SOCKS poiché si trova in un cluster che non ha bisogno di un MQIPT.

Ogni gestore code nel cluster INVENTORY è effettivamente "nascosto" dietro un MQIPT. Poiché il gestore code è stato abilitato a SOCKS, quando viene avviato un canale mittente del cluster, la richiesta viene inviata alla relativa destinazione, utilizzando MQIPT come proxy SOCKS. Di solito, il CONNAME su un canale ricevente del cluster viene usato per identificare il gestore code locale, ma quando viene usato con MQIPT, il CONNAME deve identificare il MQIPT locale e la sua porta listener in entrata. Nel seguente diagramma, tutti gli indirizzi della porta del listener in entrata sono 1414 e gli indirizzi della porta del listener in uscita sono 1415.

Esistono due metodi per eseguire un gestore code abilitato a SOCKS. Il primo è SOCKS - abilitare l'intero computer su cui è in esecuzione il gestore code. Il secondo è SOCKS - abilitare solo il gestore code. Utilizzando uno dei metodi, è necessario configurare il client SOCKS in modo che esegua solo connessioni remote utilizzando MQIPT come proxy SOCKS e disabilitare l'autenticazione utente. Ci sono una serie di prodotti sul mercato per ottenere il supporto SOCKS. È necessario sceglierne uno che supporti SOCKS V5 .

Consultare Configurazione del supporto cluster MQIPT per un esempio di configurazione di una rete cluster.



Supporto SSL/TLS in MQIPT

I socket sicuri possono essere utilizzati per garantire la privacy delle comunicazioni, l'integrità delle comunicazioni e l'autenticazione.

Riservatezza comunicazione
La connessione può essere resa privata. I dati da scambiare tra il client e il server possono essere codificati e solo il mittente e il destinatario possono dare un senso ai dati. Ciò significa che le informazioni private, come i numeri di carta di credito, possono essere trasferite in modo sicuro.

Integrità della comunicazione
La connessione è affidabile. Il trasporto del messaggio include un controllo di integrità del messaggio basato su una funzione hash sicura.

Autenticazione
Il client può autenticare il server e un server autenticato può autenticare il client. Ciò significa che le informazioni sono garantite per essere scambiate solo tra le parti previste. Il meccanismo di autenticazione si basa sullo scambio di certificati digitali (certificatiX.509v3).

Protocolli socket sicuri

In MQIPT, i socket sicuri vengono forniti utilizzando i protocolli TLS (Transport Layer Security) e SSL (Secure Sockets Layer). I due protocolli socket sicuri sono simili ma non interagiscono. In questa documentazione i termini SSL e TLS vengono utilizzati in modo intercambiabile a meno che non venga rilevata una differenza specifica.

MQIPT supporta SSL 3.0, TLS 1.0, TLS 1.1e TLS 1.2 forniti da Java runtime environment (JRE). La IBM MQ CipherSpec del canale remoto determina quale protocollo MQIPT utilizza.

SSL 3.0 non è sicuro e quindi è disabilitato per impostazione predefinita in MQIPT. Anche V 9.1.4 TLS 1.0 e TLS 1.1 sono disabilitati per impostazione predefinita in MQIPT da IBM MQ 9.1.4. Se è necessario utilizzare uno di questi protocolli disabilitati, è possibile riabilitarli seguendo la procedura in “Abilitazione di protocolli obsoleti e CipherSuites in MQIPT” a pagina 997.

I protocolli SSL/TLS possono utilizzare diversi algoritmi di firma digitale per l'autenticazione delle parti di comunicazione. Le operazioni di crittografia utilizzate in SSL/TLS, la crittografia per la riservatezza dei dati e l'hashing sicuro per l'integrità dei messaggi, si basano sulla condivisione delle chiavi segrete tra client e server. SSL/TLS fornisce vari meccanismi di scambio di chiavi che consentono la condivisione di chiavi segrete. SSL/TLS può utilizzare vari algoritmi per la crittografia e l'hashing.

Componente crittografico JRE

Il componente crittografico SSL/TLS del JRE contiene provider di sicurezza IBMJSSEFIPS e IBMJCEFIPS, certificati conformi a FIPS 140-2 al livello 1. Questi provider di sicurezza hanno la massima priorità nel JRE in modo che le implementazioni certificate FIPS vengano utilizzate ovunque siano disponibili. Sono supportati diversi algoritmi crittografici; specificarli utilizzando CipherSuitesSSL/TLS. Non tutte le CipherSuites sono certificate FIPS 140-2.

Modalità bridging SSL/TLS

Quando un instradamento ha sia SSLServer che SSLClient impostati, il MQIPT accetta una connessione protetta SSL/TLS in entrata e stabilisce una seconda connessione protetta SSL/TLS a un altro MQIPT o a un gestore code di destinazione. Le informazioni sul canale IBM MQ vengono decodificate e ricodificate tra queste due connessioni SSL/TLS. Il bridge SSL/TLS è anche indicato come *proxy di terminazione SSL/TLS*.

IBM MQ supporta il bridging SSL/TLS utilizzando MQIPT. Altri proxy di terminazione SSL/TLS con IBM MQ sono stati osservati per causare connessioni interrotte se il proxy combina o ricostruisce i record SSL/TLS con dimensioni diverse rispetto a quelle inviate da IBM MQ. Ciò è dovuto ad un'interazione tra il modo in cui i gestori code assegnano e gestiscono la memoria per i dati di rete IBM MQ in entrata e il modo in cui i dati di rete IBM MQ vengono compressi nei record SSL/TLS.

MQIPT conserva il packaging dei dati di rete IBM MQ nei record SSL/TLS senza suddividerli o combinarli. Se altri bridge SSL/TLS non conservano esattamente i record SSL/TLS, possono causare errori dei canali IBM MQ con messaggi di errore:

```
AMQ9638: SSL communications error for channel
AMQ9208: Error on receive from host
```

Modalità proxy SSL/TLS

Una rotta MQIPT può essere configurata in modalità proxy SSL/TLS come alternativa al bridging SSL/TLS. In questa modalità, l'instradamento inoltra solo i dati SSL/TLS tra due endpoint IBM MQ ; non partecipa all'handshake SSL/TLS e non richiede alcun certificato digitale.

È possibile utilizzare la modalità proxy SSL/TLS nei casi in cui i canali di IBM MQ che comunicano tramite MQIPT sono già configurati per la comunicazione SSL/TLS e si desidera utilizzare MQIPT per un altro scopo, come l'instradamento delle connessioni tramite i firewall o la limitazione della serie di connessioni consentite tramite un'uscita di sicurezza. Durante l'esecuzione in modalità proxy SSL/TLS, MQIPT verifica

che i pacchetti SSL/TLS iniziali ricevuti da una nuova connessione siano validi prima di inoltrare i pacchetti alla destinazione.

IBM MQ supporta la modalità proxy SSL/TLS con MQIPT o qualsiasi altro proxy SSL/TLS

IBM MQ supporto per più certificati con MQIPT

IBM MQ 8.0e versioni successive, supporta l'utilizzo di più certificati sullo stesso gestore code, utilizzando un'etichetta di certificato per canale, specificata utilizzando l'attributo **CERTLABL** nella definizione del canale. I canali in entrata per il gestore code (ad esempio, la connessione server o il destinatario) si basano sul rilevamento del nome del canale utilizzando SNI (Server Name Indication) TLS, al fine di presentare il certificato corretto dal gestore code.

Se un canale si connette al gestore code di destinazione tramite MQIPTe l'instradamento MQIPT ha sia **SSLServer** che **SSLClient** impostati, ci sono due sessioni TLS separate tra gli endpoint e i dati SNI non passano attraverso l'interruzione della sessione. Ciò impedisce l'utilizzo di un certificato per canale sul gestore code di destinazione per la connessione TLS tra MQIPT e il gestore code. Per utilizzare un certificato per canale sul gestore code di destinazione, per una connessione TLS che passa tramite MQIPT, la rotta MQIPT deve utilizzare la modalità proxy SSL/TLS, che inoltra tutti i flussi di controllo TLS intatti, incluso il nome SNI.

I certificati utilizzati per le connessioni TLS terminate o avviate da MQIPT possono essere configurati singolarmente per ogni instradamento, ad esempio utilizzando le proprietà di instradamento **SSLServerSiteLabel** e **SSLClientSiteLabel** .

CipherSuites supportati da MQIPT

La seguente tabella mostra quali CipherSuites sono supportati da MQIPT e quali sono abilitati per impostazione predefinita.

Per impostazione predefinita, è abilitata solo una sottoserie di CipherSuites . CipherSuites basato su diversi algoritmi considerati non sicuri sono disabilitati da JRE. Se si è consapevoli dei potenziali rischi, ma è ancora necessario utilizzare uno di questi CipherSuites, è possibile aggiungere il supporto per una CipherSuite disabilitata seguendo la procedura riportata in “Abilitazione di protocolli obsoleti e CipherSuites in MQIPT” a pagina 997.

CipherSuite	Abilitato per impostazione predefinita.
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	
SSL_DH_anon_WITH_AES_128_CBC_SHA	
SSL_DH_anon_WITH_AES_128_CBC_SHA256	
SSL_DH_anon_WITH_AES_128_GCM_SHA256	
SSL_DH_anon_WITH_AES_256_CBC_SHA	
SSL_DH_anon_WITH_AES_256_CBC_SHA256	
SSL_DH_anon_WITH_AES_256_GCM_SHA384	
SSL_DH_anonimo_WITH_DES_CBC_SHA	
SSL_DH_anon_WITH_RC4_128_MD5	
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	

CipherSuite	Abilitato per impostazione predefinita.
SSL_DHE_DSS_WITH_AES_128_CBC_SHA	V 9.1.4 Sì
SSL_DHE_DSS_WITH_AES_128_CBC_SHA256	V 9.1.4 Sì
SSL_DHE_DSS_WITH_AES_128_GCM_SHA256	V 9.1.4 Sì
SSL_DHE_DSS_WITH_AES_256_CBC_SHA	V 9.1.4 Sì
SSL_DHE_DSS_WITH_AES_256_CBC_SHA256	V 9.1.4 Sì
SSL_DHE_DSS_WITH_AES_256_GCM_SHA384	V 9.1.4 Sì
SSL_DHE_DSS_WITH_DES_CBC_SHA	
SSL_DHE_DSS_WITH_RC4_128_SHA	
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	
SSL_DHE_RSA_WITH_AES_128_CBC_SHA	V 9.1.4 Sì
SSL_DHE_RSA_WITH_AES_128_CBC_SHA256	V 9.1.4 Sì
SSL_DHE_RSA_WITH_AES_128_GCM_SHA256	V 9.1.4 Sì
SSL_DHE_RSA_WITH_AES_256_CBC_SHA	V 9.1.4 Sì
SSL_DHE_RSA_WITH_AES_256_CBC_SHA256	V 9.1.4 Sì
SSL_DHE_RSA_WITH_AES_256_GCM_SHA384	V 9.1.4 Sì
SSL_DHE_RSA_WITH_DES_CBC_SHA	
SSL_ECDH_anon_WITH_3DES_EDE_CBC_SHA	
SSL_ECDH_anon_WITH_AES_128_CBC_SHA	
SSL_ECDH_anon_WITH_AES_256_CBC_SHA	
SSL_ECDH_anon_WITH_NULL_SHA	
SSL_ECDH_anon_WITH_RC4_128_SHA	
SSL_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	
SSL_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Sì
SSL_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	Sì
SSL_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	Sì
SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Sì
SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	Sì
SSL_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	Sì
SSL_ECDH_ECDSA_WITH_NULL_SHA	
SSL_ECDH_ECDSA_WITH_RC4_128_SHA	

CipherSuite	Abilitato per impostazione predefinita.
SSL_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	
SSL_ECDH_RSA_WITH_AES_128_CBC_SHA	Sì
SSL_ECDH_RSA_WITH_AES_128_CBC_SHA256	Sì
SSL_ECDH_RSA_WITH_AES_128_GCM_SHA256	Sì
SSL_ECDH_RSA_WITH_AES_256_CBC_SHA	Sì
SSL_ECDH_RSA_WITH_AES_256_CBC_SHA384	Sì
SSL_ECDH_RSA_WITH_AES_256_GCM_SHA384	Sì
SSL_ECDH_RSA_WITH_NULL_SHA	
SSL_ECDH_RSA_WITH_RC4_128_SHA	
SSL_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	
SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Sì
SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Sì
SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Sì
SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Sì
SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Sì
SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Sì
SSL_ECDHE_ECDSA_WITH_NULL_SHA	
SSL_ECDHE_ECDSA_WITH_RC4_128_SHA	
SSL_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	
SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA	Sì
SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Sì
SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Sì
SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA	Sì
SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Sì
SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Sì
SSL_ECDHE_RSA_WITH_NULL_SHA	
SSL_ECDHE_RSA_WITH_RC4_128_SHA	
SSL_KRB5_EXPORT_WITH_DES_CBC_40_MD5	
SSL_KRB5_EXPORT_WITH_DES_CBC_40_SHA	
SSL_KRB5_EXPORT_WITH_RC4_40_MD5	
SSL_KRB5_EXPORT_WITH_RC4_40_SHA	
SSL_KRB5_WITH_3DES_EDE_CBC_MD5	
SSL_KRB5_WITH_3DES_EDE_CBC_SHA	
SSL_KRB5_WITH_DES_CBC_MD5	

CipherSuite	Abilitato per impostazione predefinita.
SSL_KRB5_WITH_DES_CBC_SHA	
SSL_KRB5_WITH_RC4_128_MD5	
SSL_KRB5_WITH_RC4_128_SHA	
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	
SSL_RSA_EXPORT_WITH_RC4_40_MD5	
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA (Nota 1)	
SSL_RSA_FIPS_WITH_DES_CBC_SHA (Nota 1)	
SSL_RSA_WITH_3DES_EDE_CBC_SHA	
SSL_RSA_WITH_AES_128_CBC_SHA	Sì
SSL_RSA_WITH_AES_128_CBC_SHA256	Sì
SSL_RSA_WITH_AES_128_GCM_SHA256	Sì
SSL_RSA_WITH_AES_256_CBC_SHA	Sì
SSL_RSA_WITH_AES_256_CBC_SHA256	Sì
SSL_RSA_WITH_AES_256_GCM_SHA384	Sì
SSL_RSA_WITH_DES_CBC_SHA	
SSL_RSA_WITH_NULL_MD5	
SSL_RSA_WITH_NULL_SHA	
SSL_RSA_WITH_NULL_SHA256	
SSL_RSA_WITH_RC4_128_MD5	Sì
SSL_RSA_WITH_RC4_128_SHA	

Nota:

1. Sebbene questa CipherSuite sia supportata per la compatibilità con le versioni precedenti, non è più conforme a FIPS e il suo uso deve essere evitato.

IBM MQ CipherSpecs e MQIPT CipherSuites

La seguente tabella mostra la relazione tra i CipherSpecs supportati da IBM MQ e i CipherSuites supportati da MQIPT.

La tabella mostra anche la versione del protocollo che IBM MQ prevede che ogni CipherSpec utilizzi.

Un IBM MQ CipherSpec determina in modo univoco sia l'algoritmo di crittografia che la versione del protocollo socket sicuro da utilizzare. Alcuni IBM MQ CipherSpecs differiscono solo per la versione del protocollo, quindi non è sufficiente configurare CipherSuite da soli. L'handshake SSL/TLS negozia la versione più elevata del protocollo SSL supportata da entrambi i lati, quindi seleziona una CipherSuite dalla serie di cifrature reciprocamente abilitate.

Ad esempio, un instradamento SSLClient con `SSLClientCipherSuites=SSL_RSA_WITH_3DES_EDE_CBC_SHA` potrebbe negoziare TLS_RSA_WITH_3DES_EDE_CBC_SHA (TLS 1.0) o TRIPLE_DES_SHA_US (SSL 3.0) con il gestore code remoto. In realtà è possibile negoziare questa CipherSuite su TLS 1.2, ma IBM MQ non supporta questa

CipherSuite su TLS 1.2. Per questo motivo, è particolarmente probabile che gli instradamenti SSLClient causino errori AMQ9616 o AMQ9631 nel gestore code.

Per evitare tali errori sugli instradamenti SSLClient, impostare la proprietà di instradamento **SSLClientProtocols** sul valore appropriato per la CipherSpecdesiderata. In alcuni casi potrebbe essere necessario limitare la serie di protocolli lato server utilizzando la proprietà di instradamento **SSLServerProtocols** . Utilizzare la versione del protocollo mostrata nella tabella per determinare l'impostazione corretta per queste proprietà di instradamento.

Questo problema riguarda in particolare le seguenti CipherSuites e CipherSpecs per le rotte SSLClient:

- SSL_RSA_WITH_3DES_EDE_CBC_SHA, che corrisponde a:
  - SSL 3.0: MQ CipherSpec TRIPLE_DES_SHA_US
  - TLS 1.0: MQ CipherSpec TLS_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA, che corrisponde a:
  - SSL 3.0: MQ CipherSpec DES_SHA_EXPORT
  - TLS 1.0: MQ CipherSpec TLS_RSA_WITH_DES_CBC_SHA
- SSL_RSA_WITH_RC4_128_SHA, che corrisponde a:
  - SSL 3.0: MQ CipherSpec RC4_SHA_US
  - TLS 1.2: MQ CipherSpec TLS_RSA_WITH_RC4_128_SHA256

Se si desidera utilizzare un singolo instradamento MQIPT SSLClient per eseguire il tunnel di più canali IBM MQ che utilizzano CipherSpecsdifferenti, assicurarsi che tutti i canali abbiano CipherSpecs che utilizzano la stessa versione di protocollo SSL e che si imposta **SSLClientProtocols** per utilizzare questa versione di protocollo singolo.

Per ulteriori informazioni su IBM MQ CipherSpecs, consultare Abilitazione di CipherSpecs.

IBM MQ CipherSpec	**MQIPT CipherSuite**	**Versione del protocollo**
DES_SHA_EXPORT	SSL_RSA_WITH_DES_CBC_SHA	SSLv3
DES_SHA_EXPORT1024	N/A	N/A
ECDHE_ECDSA_3DES_EDE_CBC_SHA256	SSL_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLSv1.2
ECDHE_ECDSA_AES_128_CBC_SHA256	SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
ECDHE_ECDSA_AES_128_GCM_SHA256	SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
ECDHE_ECDSA_AES_256_CBC_SHA384	SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
ECDHE_ECDSA_AES_256_GCM_SHA384	SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
ECDHE_ECDSA_NULL_SHA256	SSL_ECDHE_ECDSA_WITH_NULL_SHA	TLSv1.2
ECDHE_ECDSA_RC4_128_SHA256	SSL_ECDHE_ECDSA_WITH_RC4_128_SHA	TLSv1.2
ECDHE_RSA_3DES_EDE_CBC_SHA256	SSL_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.2
ECDHE_RSA_AES_128_CBC_SHA256	SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
ECDHE_RSA_AES_128_GCM_SHA256	SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
ECDHE_RSA_AES_256_CBC_SHA384	SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2

IBM MQ CipherSpec	MQIPT CipherSuite	Versione del protocollo
ECDHE_RSA_AES_256_GCM_SHA384	SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
ECDHE_RSA_NULL_SHA256	SSL_ECDHE_RSA_WITH_NULL_SHA	TLSv1.2
ECDHE_RSA_RC4_128_SHA256	SSL_ECDHE_RSA_WITH_RC4_128_SHA	TLSv1.2
FIPS_WITH_3DES_EDE_CBC_SHA (Nota 1)	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	SSLv3
FIPS_WITH_DES_CBC_SHA (Nota 1)	SSL_RSA_FIPS_WITH_DES_CBC_SHA	SSLv3
NULL_MD5	SSL_RSA_WITH_NULL_MD5	SSLv3
NULL_SHA	SSL_RSA_WITH_NULL_SHA	SSLv3
RC2_MD5_EXPORT	N/A	N/A
RC4_56_SHA_EXPORT1024	N/A	N/A
RC4_MD5_EXPORT	SSL_RSA_EXPORT_WITH_RC4_40_MD5	SSLv3
RC4_MD5_US	SSL_RSA_WITH_RC4_128_MD5	SSLv3
RC4_SHA_US	SSL_RSA_WITH_RC4_128_SHA	SSLv3
TLS_RSA_WITH_3DES_EDE_CBC_SHA	SSL_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1
TLS_RSA_WITH_AES_128_CBC_SHA	SSL_RSA_WITH_AES_128_CBC_SHA	TLSv1
TLS_RSA_WITH_AES_128_CBC_SHA256	SSL_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	SSL_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_CBC_SHA	SSL_RSA_WITH_AES_256_CBC_SHA	TLSv1
TLS_RSA_WITH_AES_256_CBC_SHA256	SSL_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	SSL_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_RSA_WITH_DES_CBC_SHA	SSL_RSA_WITH_DES_CBC_SHA	TLSv1
TLS_RSA_WITH_NULL_NULL	N/A	N/A
TLS_RSA_WITH_NULL_SHA256	SSL_RSA_WITH_NULL_SHA256	TLSv1.2
TLS_RSA_WITH_RC4_128_SHA256	SSL_RSA_WITH_RC4_128_SHA	TLSv1.2
TRIPLE_DES_SHA_US	SSL_RSA_WITH_3DES_EDE_CBC_SHA	SSLv3

Handshake SSL/TLS in MQIPT

Il processo di handshake SSL/TLS si verifica durante la richiesta di connessione iniziale tra il server e il client SSL/TLS, quando viene eseguita l'autenticazione e la negoziazione di CipherSuites .

Tutte le CipherSuites SSL/TLS supportate (vedere “Supporto SSL/TLS in MQIPT” a pagina 973), ad eccezione delle CipherSuitesanonime, richiedono l'autenticazione server e consentono l'autenticazione client; il server può essere configurato per richiedere l'autenticazione client. Dovresti evitare di usare CipherSuites anonime perché non forniscono alcuna garanzia sull'identità del peer remoto. È possibile per un attacco man - in - the - middle intercettare connessioni SSL/TLS anonime a tua insaputa. Utilizzare CipherSuites anonime solo su reti interne affidabili e solo se si è pronti ad accettare il rischio di intercettazione dei dati.

L'autenticazione peer di comunicazione in SSL/TLS si basa sulla codifica della chiave pubblica e sui certificati digitali X.509v3 . Un sito che deve essere autenticato nel protocollo SSL/TLS richiede una

chiave privata e un certificato digitale (che contiene la chiave pubblica corrispondente insieme alle informazioni sull'identità del sito), tempo di validità del certificato. I certificati sono firmati da un'autorità di certificazione, i certificati di tali autorità sono chiamati certificati del firmatario. Un certificato seguito da uno o più certificati del firmatario costituisce una catena di certificati. Una catena di certificati è caratterizzata dal fatto che, a partire dal primo certificato (certificato del sito), la firma di ogni certificato nella catena può essere verificata utilizzando la chiave pubblica contenuta nel certificato del firmatario successivo.

Quando viene stabilita una connessione sicura che richiede l'autenticazione del server, il server invia al client una catena di certificati per provare la sua identità. Il client SSL/TLS continuerà a stabilire la connessione al server solo se è in grado di autenticare il server, ad esempio, verificare la firma del certificato del sito del server. Per verificare la firma, il client SSL/TLS deve considerare attendibile il sito del server stesso o almeno uno dei firmatari nella catena di certificati fornita dal server. I certificati dei siti attendibili e dei firmatari devono essere conservati sul lato client per eseguire questa verifica.

Il client SSL/TLS ispeziona la catena di certificati del server, iniziando con il certificato del sito. Il client considera valida la firma del certificato del sito nelle seguenti circostanze:

- Il certificato del sito si trova nel repository del sito attendibile o dei certificati del firmatario
- Un certificato del firmatario nella catena può essere convalidato in base al relativo repository di certificati del firmatario attendibili

In quest' ultimo caso, il client SSL/TLS controlla che la catena di certificati sia effettivamente firmata correttamente, dal certificato del firmatario attendibile fino al certificato del sito del server. Ogni certificato coinvolto in questo processo viene anche esaminato per la correttezza del formato e delle date di validità. Se uno di questi controlli non riesce, la connessione al server viene rifiutata. Dopo aver verificato il certificato server, il client utilizza la chiave pubblica incorporata in tale certificato nei passi successivi del protocollo SSL/TLS. La connessione SSL/TLS può essere stabilita solo se il server ha realmente la chiave privata corrispondente.

L'autenticazione client segue la stessa procedura: se un server SSL/TLS richiede l'autenticazione client, il client invia al server una catena di certificati per provare la sua identità. Il server verifica la catena in base al relativo repository di certificati del firmatario e del sito attendibile. Dopo aver verificato il certificato del client, il server utilizza la chiave pubblica incorporata in tale certificato nei passi successivi del protocollo SSL/TLS. La connessione SSL/TLS può essere stabilita solo se il client ha realmente la chiave privata corrispondente.

Le versioni recenti dei protocolli TLS forniscono comunicazioni di alta sicurezza (SSL e i protocolli TLS precedenti sono considerati non sicuri). Tuttavia, il protocollo funziona in base alle informazioni fornite dall'applicazione. Solo se tale base di informazioni viene mantenuta in modo sicuro, è possibile raggiungere l'obiettivo generale di una comunicazione sicura. Ad esempio, se il repository dei certificati del sito attendibile e del firmatario è compromesso, è possibile stabilire una connessione sicura a un partner di comunicazione molto non sicuro.

Implementazione MQIPT di SSL/TLS

SSL 3.0 e TLS 1.0, 1.1e 1.2 sono implementati con token PKCS (Public Key Cryptography Standards) #12 memorizzati in file keyring (con tipi di file `.p12` o `.pfx`), contenenti X509.V3 V3. V 9.1.4 MQIPT può anche utilizzare keystore hardware crittografici che supportano lo standard PKCS#11 Cryptographic Token Interface. MQIPT utilizza il package JSSE (IBM Java Secure Socket Extension).

MQIPT può fungere da client SSL/TLS o da server SSL/TLS a seconda di quale estremità avvia la connessione. Il client avvia una connessione e il server accetta la richiesta di connessione. È possibile che un instradamento MQIPT agisca sia come client che come server. In questo caso, l'utilizzo della funzione Modalità proxy SSL/TLS in genere fornisce prestazioni migliori.

Quando MQIPT è configurato per la modalità proxy SSL/TLS, inoltra solo i dati SSL/TLS tra i due endpoint; non partecipa all'handshake SSL/TLS e non richiede alcun certificato digitale.

MQIPT non trasmette i dati SNI (Server Name Indication) TLS ricevuti su una connessione TLS in entrata tramite una connessione TLS in uscita. Questo significa che i certificati per canale, specificati utilizzando l'attributo del canale **CERTLABL** , non possono essere utilizzati per le connessioni TLS tra MQIPT e il

gestore code di destinazione. Per utilizzare un certificato per canale sul gestore code di destinazione, per una connessione TLS che passa tramite MQIPT, la rotta MQIPT deve utilizzare la modalità proxy SSL/TLS, che inoltra tutti i flussi di controllo TLS intatti, incluso il nome SNI. Per ulteriori informazioni sull'utilizzo di più certificati su un gestore code con MQIPT, consultare “IBM MQ supporto per più certificati con MQIPT” a pagina 975.

Ogni instradamento MQIPT può essere configurato in maniera indipendente con la propria serie di proprietà SSL/TLS. Per ulteriori dettagli, consultare MQIPT proprietà di instradamento .

Codifica di una password key ring in MQIPT

Codificare la parola d'ordine utilizzata per aprire un file keyringo per accedere all'hardware crittografico utilizzato da MQIPT, con il comando **mqiptPW** . La password codificata può essere utilizzata da una qualsiasi delle seguenti proprietà: **SSLClientKeyRingPW**, **SSLClientCAKeyRingPW**, **SSLServerKeyRingPW**e **SSLServerCAKeyRingPW**. Questo argomento descrive il modo corretto di memorizzare una password key ring per l'utilizzo da parte di MQIPT.

La funzione del file stash **mqiptkeyman** (iKeyman) non è supportata da MQIPT. Invece di utilizzare un file stash, è necessario utilizzare il comando **mqiptPW** per archiviare la password codificata.

Nelle versioni precedenti a IBM MQ 9.1.5, le password keyring per l'utilizzo da parte di MQIPT sono memorizzate nei file a cui fa riferimento una delle proprietà **SSL*KeyRingPW** .

V 9.1.5 Da IBM MQ 9.1.5, codificare le password key ring per l'utilizzo da parte di MQIPT utilizzando il comando **mqiptPW** e impostare il valore delle proprietà **SSL*KeyRingPW** sulla password codificata. MQIPT è in grado di distinguere tra password codificate e nomi file nei valori delle proprietà per compatibilità con le configurazioni create prima di IBM MQ 9.1.5.

Il metodo di crittografia delle password del keystore disponibile nelle versioni MQIPT precedenti a IBM MQ 9.1.5 è obsoleto, ma può essere ancora utilizzato. Per migliorare la protezione delle password key ring, codificare nuovamente le password key ring precedentemente codificate, utilizzando il metodo di protezione più recente.

Per codificare una password key ring per l'utilizzo da parte di MQIPT, attenersi alla procedura in Codifica delle password memorizzate.

È necessario utilizzare la password `mqiptSample` per aprire uno dei file keyring di esempio forniti nella directory secondaria `samples/ssl` della directory di installazione MQIPT .

Selezione di certificati da un file di chiavi in MQIPT

È possibile avere più di un certificato personale memorizzato nello stesso file key ring o token hardware crittografico. Le proprietà **SSLClientSite*** possono essere utilizzate sul lato client per selezionare il certificato da inviare al server per l'autenticazione e le proprietà **SSLServerSite*** possono essere utilizzate sul lato server per selezionare il certificato da inviare al client per l'autenticazione.

Utilizzando queste proprietà, è possibile selezionare un certificato in base al relativo DN (Distinguished Name). In alternativa, l'etichetta del certificato può essere utilizzata per selezionare un certificato utilizzando la proprietà **SSLServerSiteLabel** e **SSLClientSiteLabel** .

Impostazioni di attendibilità in MQIPT

Un key ring contiene un certificato personale che include il certificato del firmatario o una catena di certificati del firmatario.

Esistono due tipi di portachiavi utilizzati da MQIPT:

Key ring CA (Certificate Authority)
Questo key ring contiene i certificati CA attendibili utilizzati per convalidare i certificati appartenenti a un peer remoto. Questi certificati CA aiutano a determinare se il peer remoto è affidabile. MQIPT supporta i file keyring in formato PKCS #12 e i keystore hardware crittografici che supportano l'interfaccia PKCS #11 , per la memorizzazione dei certificati CA. I file di chiavi CA MQIPT sono identificati dalle proprietà di instradamento **SSLClientCAKeyRing** e **SSLServerCAKeyRing** .

L'utilizzo dell'hardware crittografico per accedere ai certificati CA è abilitato impostando la proprietà **SSLClientCAKeyRingUseCryptoHardware** e **SSLServerCAKeyRingUseCryptoHardware** .

Il keyring CA sul lato client SSL/TLS deve contenere un elenco di certificati CA attendibili che verranno utilizzati per autenticare il certificato inviato dal server. Se un instradamento del server SSL è configurato per l'autenticazione client, il keyring CA sul lato server SSL/TLS deve contenere un elenco di certificati CA attendibili che verranno utilizzati per autenticare il certificato inviato dal client.

Keyring certificato personale

Questo keyring contiene certificati personali che MQIPT utilizza per identificarsi con un peer remoto. Quando si genera un certificato autofirmato o si richiede un certificato firmato da una CA, è necessario farlo utilizzando il keyring del certificato personale. MQIPT supporta i file keyring in formato PKCS #12 e i keystore hardware crittografici che supportano l'interfaccia PKCS #11 per la memorizzazione di certificati personali. In MQIPT, i file keyring del certificato personale sono identificati dalle proprietà di instradamento **SSLClientKeyRing** e **SSLServerKeyRing** . L'utilizzo dell'hardware crittografico per accedere ai certificati personali è abilitato impostando le propriet ... **SSLClientKeyRingUseCryptoHardware** e **SSLServerKeyRingUseCryptoHardware** .

Il key ring sul lato server SSL/TLS deve contenere il certificato personale del server MQIPT . Se l'autenticazione client è necessaria su un instradamento client SSL, il file di chiavi sul lato client SSL/TLS deve contenere il certificato personale del client.

Se è necessaria l'autenticazione client, è necessario abilitare la proprietà **SSLServerAskClientAuth** sul lato server. Il keyring sul lato client deve contenere il certificato personale del client. Il file di chiavi MQIPT sul lato server, identificato dalla proprietà **SSLServerCAKeyRing** , deve contenere un elenco di certificati CA attendibili che verranno utilizzati per autenticare il client.

Se non si configura un keyring CA per un instradamento, MQIPT ricercherà i certificati CA nel keyring del certificato personale, se ne è configurato uno. Ad esempio, se non è impostato alcun valore per **SSLServerCAKeyRing**, MQIPT ricercherà i certificati CA nel file di chiavi identificato da **SSLServerKeyRing**.

Come alternativa all'uso di certificati firmati da una CA attendibile, è possibile utilizzare certificati autofirmati. È possibile trovare un esempio di certificato autofirmato nel file keyring di esempio `sslSample.pfx` fornito con MQIPT nella directory secondaria `samples/ssl` . Per aprire i file keyring PKCS#12 di esempio, è necessario utilizzare la password `mqiptSample`.

I certificati autofirmati possono essere utili negli scenari di test in cui è necessario garantire la connettività SSL/TLS senza pagare una CA per un certificato. Tuttavia, non utilizzare i certificati autofirmati negli ambienti di produzione. Per creare un certificato firmato dalla CA, consultare Creazione di un file key ring.

È possibile utilizzare un programma di utilità denominato **mqiptkeyman**, fornito con MQIPT, per gestire i certificati digitali e i keystore. Consultare “mqiptKeyman e mqiptKeycmd in MQIPT” a pagina 987 per istruzioni sull'installazione e per ulteriori informazioni.

È necessario proteggere i file keyring e i file di password utilizzando le funzioni di sicurezza del sistema operativo per impedire l'accesso non autorizzato ad essi.

Test di SSL/TLS in MQIPT

Puoi verificare una connessione SSL/TLS utilizzando gli esempi forniti in questa documentazione.

Per una descrizione dei vari scenari, vedi Introduzione a IBM MQ Internet Pass-Thru . In particolare, consultare le seguenti attività:

- Autenticazione di un server SSL/TLS
- Autenticazione di un client SSL/TLS
- Esecuzione MQIPT in modalità proxy SSL/TLS
- Esecuzione MQIPT in modalità proxy SSL/TLS con un gestore sicurezza

Per verificare che la configurazione SSL/TLS funzioni correttamente, è possibile utilizzare i certificati autofirmati. I certificati autofirmati sono utili negli scenari di test in modo da poter garantire la

connessione SSL/TLS senza pagare una CA (Certificate Authority) per un certificato. Consultare Creazione di certificati di test per i dettagli.

È possibile trovare un esempio di certificato autofirmato nel file keyring di esempio `sslSample.pfx` fornito con MQIPT nella directory secondaria `samples/ssl` . Per aprire i file keyring PKCS #12 di esempio, è necessario utilizzare la password `mqiptSample`. Il certificato di esempio viene fornito per comodità durante il test. Tuttavia, le chiavi private del certificato di esempio sono note a tutti gli utenti MQIPT . Ciò significa che non è sicuro e deve essere utilizzato solo in ambiente di test.

Non utilizzare certificati autofirmati negli ambienti di produzione, che si tratti o meno di certificati di esempio. Invece, ottenere un certificato firmato da una CA attendibile. Per creare un certificato firmato dalla CA, consultare Creazione di un file key ring.

Quando si crea o si richiede un certificato, è necessario considerare quale tipo di chiave, dimensione della chiave e algoritmo di firma digitale sono appropriati per le esigenze di sicurezza. Consultare “Considerazioni sul certificato digitale per MQIPT” a pagina 989 per ulteriori informazioni.

Certificati e tecnologie di gestione dei certificati sono disponibili da un numero di fornitori terzi.

Messaggi di errore SSL/TLS in MQIPT

Gli errori handshake vengono registrati nel log di connessione MQIPT sotto forma di eccezioni JSSE.

Per ulteriori informazioni, consultare “Log di connessione in MQIPT” a pagina 1011. La seguente tabella descrive le diverse eccezioni, la causa probabile e l'azione corrispondente per risolvere l'errore.

Le eccezioni di certificato di solito si riferiscono ai certificati all'estremità remota della connessione.

Se l'errore è correlato al certificato di un client IBM MQ o di un gestore code, il termine *file di chiavi* include il repository di chiavi IBM MQ del partner remoto.

In MQIPT, i certificati CA vengono memorizzati nel file key ring CA, identificato dalle proprietà di instradamento **SSLClientCAKeyRing** e **SSLServerCAKeyRing** . Se le proprietà di instradamento del key ring CA non sono impostate, i certificati CA vengono ricercati nel file keyring personale corrispondente (a cui fa riferimento la proprietà **SSLClientKeyRing** o **SSLServerKeyRing**).

Eccezione	Causa	Azione
CertificateException	Il certificato non è attendibile perché è firmato da una CA che non è nel keyring CA.	Controllare che tutti i certificati CA necessari siano presenti nel file keyring CA. Utilizzare lo strumento IBM Key Management fornito con MQIPT per aggiungere eventuali certificati CA mancanti, avendo cura di ottenere una copia di ciascun certificato CA da un'origine affidabile.
Eccezione CertificateExpired	1. Il certificato è scaduto: la sua data **notAfter** è passata. 2. L'orologio di sistema non è impostato correttamente.	1. Ottenere un nuovo certificato e inserirlo nel file keyring. Se il certificato appartiene a una CA (Certificate Authority), inserire il nuovo certificato nel file keyring CA. 2. Verificare che l'orologio di sistema UTC sia impostato sull'orario corretto.

Eccezione	Causa	Azione
Eccezione CertificateNotYetValid	1. Il certificato viene utilizzato prematuramente: la relativa data **notBefore** non è ancora arrivata. 2. L'orologio di sistema non è impostato correttamente.	1. Verificare che il certificato sia stato generato e firmato correttamente. Se la propria organizzazione gestisce la propria CA, l'orologio di sistema UTC per la CA potrebbe non essere corretto. 2. Verificare che l'orologio di sistema UTC sia impostato sull'orario corretto.
Eccezione CertificateParsing	1. Il certificato contiene dati DER non validi. 2. Il certificato utilizza funzioni DER non supportate.	Assicurarsi che il certificato sia stato generato correttamente e che possa essere visualizzato nello strumento IBM Key Management fornito con MQIPT. Si consiglia di ottenere un nuovo certificato con un numero inferiore di estensioni certificato.
Eccezione CertificateRevoked	Il controllo della revoca del certificato è abilitato e il certificato è stato revocato.	Il certificato in questione non deve essere attendibile. Ottenere un certificato di sostituzione e verificare che il nuovo certificato e la chiave privata siano presenti nel file keyring.
CertPathBuilderException	La catena di certificati non è stata firmata da un'autorità di certificazione riconosciuta.	1. Se si utilizzano certificati firmati dalla CA, verificare che tutti i certificati CA root e i certificati CA intermedi siano presenti nel file di chiavi della CA. 2. Se si utilizzano certificati autofirmati, assicurarsi di aver estratto una copia della parte pubblica del certificato remoto e di aver aggiunto tale copia al file di chiavi CA. Evitare di utilizzare certificati autofirmati in ambienti di produzione.

Eccezione	Causa	Azione
Eccezione CertStore Eccezione KeyStore	Si è verificato un errore durante la lettura di un certificato da un keyring per uno dei seguenti motivi: 1. Il file keyring è danneggiato. 2. Manca il file key ring. 3. La password memorizzata non corrisponde alla password del file key ring. 4. Se l'instradamento è configurato per utilizzare l'hardware crittografico, MQIPT non è stato in grado di connettersi all'hardware crittografico.	1. Verificare che sia possibile leggere il file di chiavi e che tutti i certificati possano essere visualizzati con IBM Key Management Tool. 2. Verificare che tutte le proprietà di instradamento key ring facciano riferimento al nome file corretto. 3. Verificare che la password del file key ring memorizzata sia corretta. Utilizzare lo strumento **mqiptPW** per memorizzare la password corretta. 4. Se l'instradamento è configurato per utilizzare l'hardware crittografico, controllare quanto segue: • Il file delle proprietà di sicurezza Java specifica che il provider di sicurezza IBMPKCS11Impl è installato. • Il file delle proprietà di sicurezza Java contiene il nome completo del file di configurazione utilizzato per inizializzare il provider di sicurezza IBMPKCS11Impl . • Il file di configurazione utilizzato per inizializzare il provider di sicurezza IBMPKCS11Impl è valido.
SSLException: Nessun certificato o chiave disponibile corrisponde alle suite di cifratura SSL abilitate.	È necessario disporre di un certificato personale con il tipo di chiave corretto per CipherSuites che si sta utilizzando. Ad esempio, CipherSuites i cui nomi iniziano con `SSL_ECDH_ECDSA_` richiedono un certificato con una chiave pubblica Elliptic Curve. Le CipherSuites più comunemente utilizzate richiedono un certificato con una chiave pubblica RSA.	Aprire il file di chiavi con IBM Key Management Tool. Nella vista Certificati personali, selezionare ogni certificato e visualizzarlo. Fare clic su **Visualizza dettagli** e passare alla sezione Chiave pubblica oggetto per visualizzare il tipo di chiave pubblica. Quindi, controllare le proprietà di instradamento MQIPT **SSLClientCipherSuites** e **SSLServerCipherSuites** per assicurarsi che le CipherSuites appropriate siano abilitate.

Eccezione	Causa	Azione
SSLException: nessuna suite di cifratura in comune SSLHandshakeException: nessuna suite di cifratura in comune	L'handshake non è riuscito a concordare una CipherSuite perché non vi è alcuna sovrapposizione tra le serie di CipherSuites abilitate ad entrambi i lati della connessione. In particolare, una connessione IBM MQ in uscita abilita solo una singola cifratura in modo che gli instradamenti SSLServer MQIPT abbiano particolarmente probabilità di riscontrare questo errore. Questo errore può verificarsi anche quando si verificano tutte e tre le seguenti condizioni: • non è stata specificata alcuna CipherSuite sull'instradamento • non è possibile trovare alcun certificato del sito adatto nel keyring configurato per l'instradamento • I CipherSuites anonimi sono disabilitati	Controllare l'elenco di CipherSuites abilitati nelle proprietà di instradamento MQIPT **SSLClientCipherSuites** e **SSLServerCipherSuites** . Considerare l'abilitazione di ulteriori CipherSuites. Consultare la tabella fornita per determinare la CipherSuites corretta da abilitare per ciascun valore CipherSpec del canale IBM MQ . Se non viene specificato alcun CipherSuite sull'instradamento, controllare che le proprietà dell'instradamento del key ring facciano riferimento al file key ring corretto e che il key ring contenga un certificato personale che MQIPT può utilizzare. Se l'instradamento è configurato per utilizzare l'hardware crittografico, verificare che l'attributo **tokenlabel** nel file di configurazione utilizzato per inizializzare il provider di sicurezza IBMPKCS11Impl specifichi l'etichetta del token dell'unità crittografica corretta.

mqiptKeyman e mqiptKeycmd in MQIPT

mqiptKeyman (iKeyman) è un'applicazione di gestione chiavi e certificati già nota agli utenti IBM MQ . I comandi **mqiptKeyman** e **mqiptKeycmd** possono essere utilizzati per gestire chiavi simmetriche e asimmetriche, certificati digitali e richieste di certificato nei file keyring utilizzati da IBM MQ Internet Pass-Thru. Questi file possono essere utilizzati anche per gestire i file key ring.

mqiptKeyman utilizza il termine *database delle chiavi* per fare riferimento ad un file di chiavi; questi termini sono sinonimi.

mqiptKeyman può essere eseguito in due modalità, GUI (graphical user interface) e CLI (command - line interface). Utilizzare il comando **mqiptKeyman** per avviare la GUI iKeyman e il comando **mqiptKeycmd** per eseguire la CLI iKeyman .

I comandi equivalenti per la gestione dei certificati in IBM MQ sono **strmqikm** per avviare la GUI iKeyman e **runmqckm** per eseguire la CLI iKeyman . I comandi IBM MQ sono descritti in Utilizzo di **runmqckm**, **runmqakm**e **strmqikm** per gestire i certificati digitali.

Formato file key ring richiesto per MQIPT

Quando si creano i file keyring da utilizzare in MQIPT, è necessario utilizzare il formato file PKCS #12 :

- Nella GUI, selezionare PKCS#12 nel campo **Tipo di database delle chiavi** durante la creazione del file di chiavi.
- Nella CLI, includi il parametro `-type pkcs12` nel comando `mqiptKeycmd -keydb -create` .

V 9.1.4 MQIPT può anche accedere ai certificati memorizzati in hardware di crittografia che supporta l'interfaccia PKCS #11 . L'interfaccia può essere utilizzata anche per gestire certificati

sull'hardware PKCS #11 . Per ulteriori informazioni, consultare “Utilizzo dell'hardware di crittografia PKCS #11 in MQIPT” a pagina 997.

Codifica della password key ring per MQIPT

Dopo aver creato il file keyring, è necessario codificare la relativa password in un formato che MQIPT può utilizzare per accedere al file. Per ulteriori informazioni, consultare “Codifica di una password key ring in MQIPT” a pagina 982 .

Tenere presente che la funzione di file stash non è supportata da MQIPT. È necessario utilizzare il comando **mqiptPW** per codificare la password key ring invece di utilizzare un file stash.

Esempi di riga comandi

La CLI utilizza la stessa sintassi del comando IBM MQ **runmqckm** . Accodare i parametri richiesti a **mqiptKeycmd**, come illustrato nei seguenti esempi:

- Per creare un file PKCS#12 :

```
mqiptKeycmd -keydb -create -db key.p12 -pw password -type pkcs12
```

- Per creare un certificato personale autofirmato per scopi di test:

```
mqiptKeycmd -cert -create -db key.p12 -pw password -type pkcs12
-label mqipt -dn "CN=Test Certificate,OU=Sales,O=Example,C=US"
-sig_alg SHA256WithRSA -size 2048
```

  Il comando crea un certificato digitale con una chiave pubblica RSA a 2048 bit e una firma digitale che utilizza RSA con algoritmo hash SHA-256 . Quando crei un certificato, fai attenzione a scegliere un algoritmo di crittografia della chiave pubblica, la dimensione della chiave e l'algoritmo di firma digitale che siano appropriati per le esigenze di sicurezza della tua organizzazione. Per ulteriori informazioni, consultare “Considerazioni sul certificato digitale per MQIPT” a pagina 989.

  Questo esempio utilizza un certificato autofirmato adatto per scopi di test. Tuttavia, in un ambiente di produzione è necessario utilizzare un certificato firmato dalla CA (Certificate Authority).

  Nota che MQIPT v2.0 e versioni precedenti non supportano le firme digitali SHA-2 , quindi questo certificato non è adatto per stabilire connessioni socket sicure alle release precedenti di MQIPT ; un algoritmo di firma precedente, come SHA1WithRSA, sarebbe richiesto.

- Per creare una richiesta di certificato per un certificato firmato CA per scopi di produzione:

```
mqiptKeycmd -certreq -create -db key.p12 -pw password -type pkcs12 -file cert.req
-label mqipt -dn "CN=Test Certificate,OU=Sales,O=Example,C=US"
-sig_alg SHA256WithRSA -size 2048
```

  Il comando crea una richiesta di certificato digitale con una chiave pubblica RSA a 2048-bit e una firma digitale che utilizza RSA con algoritmo hash SHA-256 . Quando crei un certificato, fai attenzione a scegliere un algoritmo di crittografia della chiave pubblica, la dimensione della chiave e l'algoritmo di firma digitale che siano appropriati per le esigenze di sicurezza della tua organizzazione. Per ulteriori informazioni, consultare “Considerazioni sul certificato digitale per MQIPT” a pagina 989.

- Per ricevere il file del certificato personale firmato CA `cert.crt` nel file keyring:

```
mqiptKeycmd -cert -receive -db key.p12 -pw password -type pkcs12 -file cert.crt
```

  È necessario assicurarsi che il certificato CA della CA che ha firmato il certificato personale sia presente nel file di chiavi CA, ad esempio:

```
mqiptKeycmd -cert -add -db key.p12 -pw password -type pkcs12 -file ca.crt -label rootCA
```

Considerazioni sul certificato digitale per MQIPT

I punti da considerare includono la dimensione della chiave del certificato, la selezione di un appropriato algoritmo di firma digitale del certificato e certificato digitale e il certificato CipherSuite compatibilityDigital e la compatibilità CipherSuite .

Considerazioni sulla dimensione della chiave del certificato per MQIPT

La dimensione della chiave pubblica dipende dalla politica di sicurezza dell'organizzazione e dall'algoritmo di cifratura utilizzato. In generale, le dimensioni delle chiavi più grandi sono più sicure. La seguente tabella elenca le dimensioni chiave minime da utilizzare:

Algoritmo	Dimensione chiave minima (bit)
Curva ellittica	256
RSA	2048

Specificare la dimensione della chiave del proprio certificato quando si crea un certificato o una richiesta di certificato.

- Quando si utilizza il comando CLI **mqiptKeycmd** , il parametro **-size** specifica la dimensione della chiave.
- Quando si usa la GUI di **mqiptKeyman** , il campo **Dimensione chiave** nella finestra Creazione certificato specifica la dimensione chiave.

Selezione di un algoritmo di firma digitale del certificato appropriato

Per prevenire la falsificazione di certificati digitali, è importante utilizzare un forte algoritmo di firma digitale. Quando si crea o si richiede un certificato, fare attenzione a selezionare un buon algoritmo.

Si consiglia di evitare l'utilizzo di vecchi algoritmi di firma digitale basati su MD5 o SHA-1 poiché tali algoritmi non sono più sufficientemente sicuri per l'utilizzo moderno. Se possibile, utilizzare uno dei più recenti algoritmi di firma digitale basati su SHA-2 come SHA-256 con RSA (SHA256WithRSA).

Tuttavia, le versioni di MQIPT precedenti alla Versione 2.1 non supportano le firme digitali SHA-2 , quindi, per l'interoperabilità con le release precedenti di MQIPT , utilizzare l'algoritmo di firma digitale SHA1WithRSA . Tuttavia, è necessario pianificare l'aggiornamento delle versioni precedenti di MQIPT e l'utilizzo delle firme digitali MD5 e SHA-1 .

- Quando si utilizza il comando CLI **mqiptKeycmd** , il parametro **-sig_alg** specifica l'algoritmo di firma digitale.
- Quando si utilizza la GUI **mqiptKeyman** , il campo **Algoritmo di firma** della finestra Creazione certificato specifica l'algoritmo di firma digitale.

Certificato digitale e compatibilità CipherSuite in MQIPT

Non tutte le CipherSuites possono essere utilizzate con tutti i certificati digitali. Esistono vari tipi di CipherSuite, raggruppati in base al prefisso del nome CipherSuite . Ogni tipo di CipherSuite impone restrizioni diverse sul tipo di certificato digitale che è possibile utilizzare. Queste limitazioni si applicano a tutte le connessioni MQIPT SSL/TLS, ma sono particolarmente rilevanti per gli utenti della crittografia Elliptic Curve. Quando si esegue l'handshake del socket sicuro, MQIPT seleziona automaticamente un certificato personale per identificare se stesso appropriato per la CipherSuitenegoziata. Nella maggior parte dei casi, MQIPT interagisce automaticamente con il peer remoto. Tuttavia, in alcuni scenari potrebbe essere necessario utilizzare una MQIPT CipherSuite specifica per interagire con un sistema IBM MQ remoto. L'applicazione **mqiptKeyman** fornita con MQIPT è in grado di creare certificati e richieste di certificati solo con chiavi pubbliche DSA e RSA. Inoltre, il programma di utilità IBM MQ **runmqakm** può creare certificati e richieste di certificati con chiavi pubbliche Elliptic Curve. Consultare l'autorità di certificazione per informazioni sulla creazione di altri tipi di certificati.

Il tipo di certificato digitale da utilizzare dipende dal tipo di CipherSuite utilizzato:

- CipherSuites con nomi che iniziano con SSL_ECDH_ECDSA_ e SSL_ECDHE_ECDSA_ richiedono un certificato digitale con una chiave pubblica della curva ellittica.
- CipherSuites con nomi che contengono *anon* sono anonimi; non richiedono un certificato digitale per identificare il peer remoto. Tali CipherSuites possono evitare i sovraccarichi di gestione del ciclo di vita dei certificati nelle reti in cui viene utilizzato un mezzo alternativo di autenticazione, ma in generale, evitarne l'utilizzo a causa della mancanza di autenticazione.
- Altre CipherSuites richiedono un certificato digitale con chiave pubblica RSA.

Nota: Gli strumenti **mqiptKeyman** e **mqiptKeycmd** non sono in grado di creare certificati o richieste di certificati con una chiave pubblica Elliptic Curve. È possibile utilizzare il comando **runmqakm** fornito con IBM MQ per questo scopo. Il comando **runmqakm** viene descritto in Utilizzo di **runmqckm**, **runmqakm** e **strmqikm** per gestire i certificati digitali.

Uscita certificato in MQIPT

Lo scopo di un'uscita certificato è convalidare un certificato peer SSL/TLS ricevuto da MQIPT.

Puoi configurare un instradamento MQIPT per agire come un client SSL/TLS quando effettua una nuova connessione e per agire come un server SSL/TLS quando riceve una richiesta di connessione. Durante il processo di handshake SSL/TLS, un client SSL/TLS riceve un certificato peer dal server e il certificato può essere utilizzato per autenticare il server. Un server SSL/TLS può anche ricevere un certificato peer dal client e il certificato può essere utilizzato per autenticare il client.

L'uscita del certificato viene richiamata quando MQIPT riceve un certificato peer, consentendo di eseguire un'ulteriore convalida. Tutte le eccezioni rilevate dall'uscita vengono rilevate da MQIPT e la richiesta di connessione viene terminata. Si consiglia, quindi, all'uscita di rilevare tutte le eccezioni e di restituire un codice di ritorno appropriato a MQIPT.

Viene fornito un esempio per mostrare che un'uscita certificato può essere implementata per ulteriori informazioni consultare Utilizzo di un'uscita certificato per autenticare un server SSL/TLS.

Nota: MQIPT viene eseguito in un singolo Java virtual machine in modo che un'uscita di certificato definita dall'utente possa compromettere il normale funzionamento di MQIPT in uno dei seguenti modi:

- Influisce sulle risorse di sistema
- Genera colli di bottiglia
- Prestazioni ridotte

È necessario verificare ampiamente gli effetti dell'uscita del certificato prima di implementarlo in un ambiente di produzione.

La classe com.ibm.mq.ipt.exit.CertificateExit in MQIPT

Una classe astratta che deve essere implementata dalla classe definita con la proprietà SSLExitName .

La classe contiene le implementazioni predefinite per l'esecuzione dell'uscita e alcuni metodi pubblici che è possibile sovrascrivere, in base ai propri requisiti. L'elenco completo dei metodi supportati è il seguente:

Metodi

init int pubblico (IPTTrace)

Il metodo init viene richiamato da MQIPT quando l'uscita viene caricata da MQIPT e può essere implementato per eseguire qualsiasi inizializzazione dell'uscita; ad esempio, il caricamento dei dati utilizzati durante il processo di convalida. L'implementazione predefinita non fa nulla.

aggiornamento int pubblico (IPTTrace)

Il metodo di aggiornamento è implementato per eseguire un aggiornamento di qualsiasi dato; ad esempio, il ricaricamento di qualsiasi dato per il disco utilizzato durante il processo di convalida. Questo metodo viene richiamato quando l'amministratore MQIPT ha immesso un comando di aggiornamento. L'implementazione predefinita non fa nulla.

public void close (IPTTrace)

Il metodo di chiusura viene implementato per eseguire le operazioni di manutenzione quando l'instradamento sta per essere arrestato o MQIPT sta per essere chiuso. L'implementazione predefinita non fa nulla.

Convalida risposta CertificateExitpubblica (IPTTrace)

Il metodo di convalida viene richiamato per eseguire la convalida del certificato peer. L'oggetto di ritorno può essere utilizzato per passare le informazioni a MQIPT; ad esempio, un codice di ritorno e del testo che può essere aggiunto al log di connessione. L'implementazione predefinita restituisce una risposta CertificateExitcon CertificateExitResponse.OK.

Metodi supportati per ottenere le proprietà:

public int getListenerPorta ()
richiama la porta del listener di instradamento - come definito dalla proprietà ListenerPort

public String getDestination()
richiama l'indirizzo di destinazione - come definito dalla proprietà Destinazione

public int getDestinationPort ()
richiama l'indirizzo della porta del listener di destinazione - come definito dalla proprietà DestinationPort

public String getClientIPAddress ()
richiama l'indirizzo IP del client che effettua la richiesta di collegamento

public int getClientPortAddress()
richiama l'indirizzo porta utilizzato dal client che effettua la richiesta di connessione

booleano pubblico isSSLClient()
utilizzato per determinare se l'uscita viene richiamata come un client SSL/TLS o un server SSL/TLS. Se questo valore restituisce true, l'uscita si trova sul lato client della connessione, convalidando il certificato ottenuto dal server. Se questo restituisce false, l'uscita si trova sul lato server della connessione, convalidando il certificato inviato dal client. È valido per un instradamento che funga sia da server SSL/TLS che da un client SSL/TLS, decodificando e ricodificando il traffico. In questa situazione, sebbene esista una singola classe di uscita, alcune istanze della classe verranno richiamate come client e alcune come server. È possibile utilizzare isSSLClient per determinare la situazione per una determinata istanza.

public int getConnThreadID()
utilizzato per richiamare l'ID del thread di lavoro che sta gestendo la richiesta di connessione, che può essere utile per il debug.

public String getChannelNome ()
richiama il nome del canale di IBM MQ utilizzato nella richiesta di connessione. Questa opzione è disponibile solo quando la richiesta in entrata non utilizza SSL/TLS e MQIPT funge da client SSL/TLS.

public String getQMName()
richiama il nome del gestore code IBM MQ utilizzato nella richiesta di connessione. Questa opzione è disponibile solo quando la richiesta client non utilizza SSL/TLS e MQIPT funge da client SSL/TLS.

Booleano pubblico getTimedout()
utilizzato dall'uscita per determinare se il timeout è scaduto.

public IPTCertificate getCertificate()
richiama il certificato SSL/TLS che deve essere convalidato.

public String getExitData ()
richiama i dati di uscita, come definito dalla proprietà SSLExitData .

public String getExitName ()
richiama il nome uscita, come definito dalla proprietà SSLExitName .

La classe com.ibm.mq.ipt.exit.CertificateExitResponse in MQIPT

Questa classe viene utilizzata per passare le informazioni a MQIPT dopo che un certificato è stato convalidato.

Costruttori

public CertificateExitResponse (*int rc*, messaggio stringa)

Questo costruttore può essere utilizzato per restituire un codice di ritorno e del testo del messaggio. I codici di errore possibili sono

- ExitRc.OK
- ExitRc.ERRORE_CONVALIDA
- ExitRc.CONVALIDA_RIFIUTATA

Risposta CertificateExitpubblica (*int rc*)

Questo costruttore può essere utilizzato per restituire un codice di ritorno, senza testo del messaggio. I codici di errore possibili sono

- ExitRc.OK
- ExitRc.ERRORE_CONVALIDA
- ExitRc.CONVALIDA_RIFIUTATA

Risposta () CertificateExitpubblica

Questo costruttore può essere utilizzato per passare il codice di ritorno ExitRc.OK, senza testo del messaggio.

Metodi

public String getVersion()

Questo metodo restituisce la versione di questa classe.

public String toString

Questo metodo restituirà una rappresentazione di stringa della risposta, ad esempio, " Codice di errore: 4, Messaggio: Controllo CRL non riuscito.

La classe com.ibm.mq.ipt.exit.IPTCertificate in MQIPT

Questa classe contiene il certificato SSL/TLS da convalidare.

Metodi

public int getVersion()

Questo metodo restituisce la versione di questa classe.

public byte [] getDerCodifica ()

Questo metodo restituisce la codifica ASN.1/DER del certificato X.509 o NULL se si verifica un errore.

byte pubblico [] getPemCodifica ()

Questo metodo restituisce la codifica PEM (BASE64) del certificato X.509 o NULL se si verifica un errore.

public String getLabel()

Questo metodo restituisce l'etichetta del certificato o NULL se si verifica un errore.

public String getName()

Questo metodo restituisce il DN (Distinguished Name) del certificato o NULL se non disponibile. Ad esempio:

```
CN=Test Queue Manager,OU=Sales,O=Example,L=London,C=GB
```

public String getIssuerNome ()

Questo metodo restituisce il DN (Distinguished Name) dell'emittente del certificato o NULL se non disponibile. Ad esempio:

```
CN=Certificate Authority,OU=Security,O=Example,L=New York,C=US
```

pubblico IPTCertificate getSigner()

Questo metodo restituisce il certificato del firmatario o NULL se non è disponibile. Per un certificato autofirmato, restituirà un riferimento a se stesso.

public String toString()

Questo metodo restituisce una rappresentazione stringa del certificato.

La classe com.ibm.mq.ipt.exit.IPTTrace in MQIPT

Le funzioni di traccia MQIPT forniscono chiamate di entrata e di uscita, che possono essere utilizzate all'entrata e all'uscita da un metodo. Ci sono anche varie chiamate di dati per tracciare informazioni utili.

Metodi

public void entry (String *fid*)

Dove *fid* viene utilizzato per identificare dove è stata effettuata la chiamata, ad esempio il nome della classe e del metodo.

Questo metodo scrive una voce nel file di output di traccia con il livello di rientro appropriato per registrare il punto in cui il flusso di controllo entra in un metodo. Questa chiamata è facoltativa, ma se viene utilizzata, è necessario utilizzare anche una chiamata corrispondente a "exit (String)" all'interno dello stesso metodo.

public void exit (String *fid*)

Dove *fid* viene utilizzato per identificare dove è stata effettuata la chiamata, ad esempio il nome della classe e del metodo.

Questo metodo scrive un'uscita nel file di output di traccia con il livello di rientro appropriato per registrare il punto in cui il flusso di controllo lascia un metodo. Questo metodo viene utilizzato solo quando una chiamata a "entry (String)" è stata precedentemente utilizzata all'interno dello stesso metodo.

public void exit (String *fid*, int *rc*)

Dove *fid* viene utilizzato per identificare il punto in cui è stata effettuata la chiamata, ad esempio il nome della classe e del metodo e *rc* è il codice di ritorno numerico dal metodo. Questo metodo di tracciamento deve essere utilizzato per registrare l'uscita dai metodi che restituiscono un numero intero.

Questo metodo scrive un'uscita nel file di output di traccia con il livello di rientro appropriato per registrare il punto in cui il flusso di controllo lascia un metodo e il codice di ritorno numerico da tale metodo. Questo metodo viene utilizzato solo quando una chiamata a "entry (String)" è stata precedentemente utilizzata all'interno dello stesso metodo.

public void exit (String *fid*, boolean *rc*)

Dove *fid* viene utilizzato per identificare dove è stata effettuata la chiamata, ad esempio il nome della classe e del metodo e *rc* è il codice di ritorno booleano dal metodo. Questo metodo di traccia deve essere utilizzato per registrare l'uscita dai metodi che restituiscono un valore booleano.

Questo metodo scrive un'uscita nel file di output di traccia con il livello di rientro appropriato per registrare il punto in cui il flusso di controllo lascia un metodo e il codice di ritorno booleano da tale metodo. Questo metodo viene utilizzato solo quando una chiamata a "entry (String)" è stata precedentemente utilizzata all'interno dello stesso metodo.

public void data (String *fid*, String data)

Dove *fid* viene utilizzato per identificare dove è stata effettuata la chiamata, ad esempio il nome della classe e del metodo.

Questo metodo scrive alcuni dati stringa nel file di output di traccia.

public void data (String *fid*, int data)

Dove *fid* viene utilizzato per identificare dove è stata effettuata la chiamata, ad esempio il nome della classe e del metodo.

Questo metodo scrive alcuni dati interi nel file di output di traccia.

public void data (String *fid*, byte [])

Dove *fid* viene utilizzato per identificare dove è stata effettuata la chiamata, ad esempio il nome della classe e del metodo.

Questo metodo scrive alcuni dati binari nel file di output di traccia.

Traccia di esempio

Per facilitare la diagnosi dei problemi in un'uscita, è possibile utilizzare la stessa funzione di traccia di MQIPT, oppure è possibile implementare le proprie funzioni di traccia. Se si decide di utilizzare le funzioni di traccia MQIPT , sono presenti chiamate di entrata e di uscita, che possono essere utilizzate all'entrata e all'uscita da un metodo. Esistono anche diverse chiamate di dati per tracciare informazioni utili come mostrato nel seguente esempio.

```
/**
* This method is called to initialize the exit (for example, for
* loading validation information) and place itself in a ready
* state to validate connection requests.
*/
 public int init(IPTTrace t) {
 final String fid = "MyExit.init";

 // Trace entry into this method
 t.entry(fid);

 // Trace useful information
 t.data(fid, "Starting exit - MQIPT version " + getVersion());

 // Perform initialization and load any data
 t.data(fid, "Ready for work");

 // Trace exit from this method
 t.exit(fid);

 return ExitRc.OK;
}
```

Questo metodo produce la traccia nel formato mostrato nel seguente esempio:

```
16:36:48.625    14   5000-1s    ------{ ConnectionThread.setCertificateExit()
16:36:48.625    14   5000-1s     Creating instance of certificate exit
16:36:48.625    14   5000-1s     Calling init() of certificate exit
16:36:48.625    14   5000-1s    -------{ MyExit.init()
16:36:48.625    14   5000-1s     Starting exit - MQIPT version 2.1.0.0
16:36:48.625    14   5000-1s    Ready for work
16:36:48.625    14   5000-1s    -------} MyExit.init() rc=0
16:36:48.625    14   5000-1s    ------} ConnectionThread.setCertificateExit() rc=0
```

Codici di ritorno di uscita certificato in MQIPT

I codici di ritorno che MQIPT riconosce quando si richiama un'uscita certificato in diverse situazioni.

I seguenti codici di ritorno vengono riconosciuti da MQIPT quando si richiama un'uscita certificato nelle situazioni seguenti:

Codice di ritorno	Descrizione	inizializzare	Convalida	Aggiorna
ExitRc.OK	Richiesta completata correttamente.	sì	sì	sì
ExitRc.ERRORE DI INIZIALIZZAZIONE	Richiesta di inizializzazione non riuscita, l'instradamento verrà disabilitato.	sì		
ExitRc.ERRORE_RISPEDIZIONE	Richiesta di aggiornamento non riuscita, l'instradamento verrà disabilitato.			sì
ExitRc.ERRORE_CONVALIDA	Processo di convalida non riuscito, richiesta di connessione rifiutata.		sì	
ExitRc.CONVALIDA_RIFIUTATA	Richiesta di convalida rifiutata, richiesta di connessione rifiutata.		sì	

LDAP e CRL in MQIPT

MQIPT supporta l'utilizzo di un server LDAP (Lightweight Directory Access Protocol) per eseguire l'autenticazione CRL (Certificate Revocation List) su un certificato digitale.

Il supporto LDAP è stato implementato in modo simile a quello in IBM MQ, poiché lo stesso server LDAP può essere utilizzato sia per IBM MQ che per MQIPT.

Durante l'handshake SSL/TLS, i partner comunicanti si autenticano reciprocamente con i certificati digitali. L'autenticazione può includere una conferma che il certificato ricevuto sia ancora ancora sicuro. Le autorità di certificazione (CA) revocano i certificati per vari motivi, tra cui:

- Il proprietario è stato spostato in un'organizzazione diversa.
- La chiave privata non è più segreta.

Le CA pubblicano i certificati personali revocati in un CRL (Certificate Revocation List). I certificati AC revocati vengono pubblicati in un elenco ARL (Authority Revocation List). Notare che i riferimenti successivi ai CRL si applicano anche agli ARL.

Per ulteriori informazioni sull'utilizzo dei server LDAP con IBM MQ e sulla gestione di CRL e ARL, consultare Gestione degli elenchi di revoca dei certificati e degli elenchi di revoca delle autorizzazioni.

MQIPT può supportare fino a due server LDAP su ciascun instradamento. Il primo server LDAP viene considerato come il server principale con il secondo server LDAP mantenuto come backup. Il secondo server viene utilizzato solo se non è possibile raggiungere il server principale. Il server di backup deve essere un'immagine di mirroring del server principale.

L'accesso alle informazioni memorizzate su un server LDAP può essere protetto con un ID utente e una password utilizzando le proprietà ID utente e password LDAP. Le password del server LDAP possono essere codificate nella configurazione MQIPT da IBM MQ 9.1.5. Per ulteriori informazioni sulla crittografia delle password che devono essere utilizzate da MQIPT, vedi Crittografia delle password memorizzate.

Quando MQIPT carica un token PKCS #12 da un file key ring, viene verificata la validità CRL di qualsiasi certificato CA. Se il certificato CA ha un CRL allegato, viene controllato per verificare se è scaduto e, in tal caso, viene richiamato un CRL più recente dal server LDAP. Qualsiasi CRL richiamato viene caricato nel token corrente e collegato al relativo certificato CA.

Se non ci sono voci che corrispondono alla CA fornita quando una query viene inviata al server LDAP principale, si presuppone che non ci siano CRL per quella CA e che il server di backup non venga utilizzato. Tuttavia, se il server LDAP principale non può essere raggiunto o non viene restituito entro un determinato intervallo di tempo, viene utilizzato il server di backup. Eventuali errori del server di backup causano la chiusura della connessione client. Questa azione può essere sovrascritta impostando la proprietà **LDAPIgnoreErrors** su `true`.

I CRL richiamati da MQIPT vengono conservati in una cache e condivisi da tutte le connessioni su tale instradamento. Se un CRL memorizzato nella cache è scaduto, il CRL viene rimosso dalla cache e ne viene

richiamato uno nuovo dal server LDAP. Se un nuovo CRL non è disponibile, la connessione viene ancora rifiutata.

Viene controllata anche la scadenza di un CRL richiamato dal server LDAP e viene visualizzato un messaggio di avviso (MQCPW001). Il CRL scaduto è ancora caricato nel sistema e tutte le richieste di connessione che fanno riferimento a quel CRL vengono rifiutate. Sostituire il CRL scaduto nel server LDAP con uno corrente.

La proprietà **LDAPCacheTimeout** può essere utilizzata per controllare la frequenza con cui la cache CRL viene cancellata. Il valore predefinito è 1 giorno. Se si imposta questo valore su `0` , le voci della cache non vengono cancellate fino a quando l'instradamento non viene riavviato.

Un CRL scaduto può essere memorizzato in un file key ring o su un server LDAP. Se non è stato emesso un nuovo CRL, vengono rifiutate ulteriori richieste di connessione. È possibile ignorare i CRL scaduti abilitando la proprietà **IgnoreExpiredCRLs** .

Nota: Se si abilita la proprietà **LDAPIgnoreErrors** o la proprietà **IgnoreExpiredCRLs** , è possibile utilizzare un certificato revocato per stabilire una connessione SSL/TLS.

Proprietà OU del certificato con più valori in MQIPT

È possibile mettere in corrispondenza più valori OU (organizational unit) nel certificato DN (Distinguished Name).

Le seguenti proprietà di instradamento ora supportano la corrispondenza di più valori OU:

- **SSLClientDN_OU**
- **SSLClientSiteDN_OU**
- **SSLServerDN_OU**
- **SSLServerSiteDN_OU**

Per far corrispondere più valori OU, utilizzare una virgola come separatore nel valore della proprietà di instradamento. Ad esempio:

```
SSLClientDN_OU=Sales, Europe
```

Questo corrisponde ai certificati con `OU=Sales` e `OU=Europe`. I valori OU corrispondono nella stessa sequenza di più valori OU nei filtri IBM MQ SSLPEER.

Non specificare la stessa proprietà di instradamento più di una volta nella sezione `[route]` . Il modo corretto per far corrispondere più valori OU è specificare la proprietà una volta, come mostrato nell'esempio precedente. Se si immette lo stesso attributo più di una volta nella stessa sezione `mqipt.conf` , l'ultimo valore diventa effettivo. Ad esempio, le seguenti voci risulterebbero solo nella corrispondenza di `Europa` perché la seconda riga sovrascrive la prima:

```
SSLClientDN_OU=Sales
SSLClientDN_OU=Europe
```

Se è necessario mettere in corrispondenza una virgola letterale all'interno di un valore OU, inserire una barra retroversa (\) come carattere escape immediatamente prima della virgola. Ad esempio:

```
SSLClientDN_OU=Sales\, Europe
```

Corrisponde a un singolo valore: `OU=Sales, Europe`. Una barra rovesciata che non è immediatamente seguita da una virgola corrisponde a una barra rovesciata letterale.

Se si sta eseguendo l'aggiornamento da una release precedente di MQIPT e si basa sulla capacità di mettere in corrispondenza virgole nei valori OU, è necessario inserire caratteri di escape barra retroversa nelle proprietà di instradamento OU per preservare il comportamento precedente.

Abilitazione di protocolli obsoleti e CipherSuites in MQIPT

Per impostazione predefinita, i protocolli dei socket sicuri e le CipherSuites considerate non sicure sono disabilitati nel Java runtime environment (JRE) fornito con MQIPT. Questi protocolli obsoleti e CipherSuites devono essere abilitati prima di poter essere utilizzati.

Informazioni su questa attività

Se si è consapevoli dei potenziali rischi, ma è ancora necessario utilizzare uno dei protocolli o CipherSuites considerati non sicuri in MQIPT, seguire questa procedura per abilitare il protocollo o CipherSuite che è necessario utilizzare.

Procedura

1. Modificare il file `java.security` , che si trova nella directory *mqipt_path*`/java/jre/lib/security` , dove *mqipt_path* è l'ubicazione in cui è installato MQIPT.
2. Aggiungere il supporto al JRE per un protocollo o un algoritmo rimuovendo la voce corrispondente dall'elenco di algoritmi disabilitati nella proprietà `jdk.tls.disabledAlgorithms` .
   - V 9.1.4 Per aggiungere il supporto per un protocollo, rimuovere il protocollo dall'elenco degli algoritmi disabilitati. Ad esempio, per aggiungere supporto per TLS 1.0, rimuovere TLSv1 dall'elenco.
   - Per aggiungere il supporto per CipherSuite, rimuovere l'algoritmo corrispondente dall'elenco degli algoritmi disabilitati. Ad esempio, per aggiungere il supporto per SSL_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA Cipher Suite, rimuovere 3DES_EDE_CBC dall'elenco.
3. V 9.1.4
   Per abilitare SSL 3.0 in JRE, è necessario impostare anche le proprietà del sistema `com.ibm.jsse2.disableSSLv3=false`.
   È possibile impostare la proprietà utilizzando la variabile di ambiente **MQIPT_JVM_OPTIONS**. Ad esempio:
   ```
   set MQIPT_JVM_OPTIONS=-Dcom.ibm.jsse2.disableSSLv3=false
   ```
4. Per abilitare SSL 3.0, TLS 1.0o TLS 1.1 su una rotta MQIPT , aggiungere il protocollo corrispondente alla proprietà di instradamento **SSLServerProtocols** o **SSLClientProtocols** .
5. Riavviare MQIPT per rendere effettive le modifiche alle proprietà JRE.

V 9.1.4 Utilizzo dell'hardware di crittografia PKCS #11 in MQIPT

MQIPT può accedere ai certificati digitali memorizzati nell'hardware crittografico che supporta l'interfaccia PKCS #11 .

Prima di iniziare

Prima di iniziare a configurare MQIPT per l'utilizzo dell'hardware crittografico, assicurarsi che la scheda crittografica, il driver della scheda e qualsiasi software di supporto associato siano installati e funzionino correttamente.

Il supporto per l'hardware di crittografia PKCS #11 in MQIPT è fornito dal provider di crittografia IBM Java PKCS11 (providerIBMPKCS11Impl). Per ulteriori informazioni relative al provider IBMPKCS11Impl e all'elenco delle schede di crittografia supportate da Java 8, consultare IBM PKCS11 Cryptographic Provider.

Informazioni su questa attività

È possibile memorizzare i certificati personali e i certificati CA a cui accede MQIPT in un keystore hardware crittografico. Tuttavia, poiché una periferica PKCS #11 normalmente non dispone di spazio

sufficiente per memorizzare una grande quantità di certificati del firmatario, è possibile utilizzare un keystore basato su file separato per i certificati CA.

Seguire questa procedura per configurare MQIPT per utilizzare i certificati in un keystore hardware crittografico.

Nota: L'utilizzo dell'hardware crittografico con MQIPT è una funzionalità IBM MQ Advanced . Per utilizzare questa funzionalità, è necessario che il gestore code locale connesso utilizzando la rotta MQIPT disponga anche della titolarità IBM MQ Advanced, IBM MQ Appliance o IBM MQ Advanced for z/OS VUE .

Procedura

1. Creare il file di configurazione utilizzato durante l'inizializzazione del provider IBMPKCS11Impl .

   Scaricare i file di configurazione di esempio per ciascuna delle schede crittografiche hardware supportate dal provider IBMPKCS11Impl e configurare un esempio per il sistema. Gli esempi possono essere scaricati dal seguente argomento Java in IBM Documentation: File di configurazione.

   Il file di configurazione è un file di testo e deve contenere almeno i seguenti attributi:

   nome
   Il suffisso del nome dell'istanza provider.

   libreria
   Il nome completo della libreria PKCS #11 fornita con l'hardware crittografico.

   Etichetta token
   L'etichetta del token dell'unità crittografica PKCS #11 .

   Ad esempio, il file di configurazione potrebbe contenere le seguenti voci:

   ```
   name = IPTPKCS11Provider
   library = /usr/lib64/pkcs11/PKCS11_API.so
   tokenlabel = icatoken
   ```

2. Modificare il file delle proprietà di sicurezza Java , `java.security`, che si trova nella sottodirectory `java/jre/lib/security` della directory di installazione MQIPT .
   a) Se non è già presente nel file, aggiungere il provider di sicurezza IBMPKCS11Impl .

      Ad esempio, aggiungendo la seguente riga:

      ```
      security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
      ```

   b) Aggiungere il nome completo del file di configurazione dopo il nome provider.

      Ad esempio, se il file di configurazione creato nel passo “1” a pagina 998 viene denominato `/opt/mqipt/pkcs11.cfg`, è necessario aggiungere questo percorso alla stessa riga del provider di sicurezza:

      ```
      security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /opt/mqipt/
      pkcs11.cfg
      ```

3. Se si sta utilizzando un file di chiavi per i certificati CA, invece di memorizzare i certificati CA nell'hardware crittografico, creare un file di chiavi CA in formato PKCS #12 .

   È possibile creare un file key ring CA utilizzando la GUI (graphical user interface) **mqiptKeyman** o la CLI (command line interface) **mqiptKeycmd** .

   - Per utilizzare la CLI, immettere il comando seguente:

     ```
     mqiptKeycmd -keydb -create -db filename -pw password -type pkcs12
     ```

     dove *nomefile* è il nome del file key ring da creare e *password* è la password key ring.
   - Per utilizzare la GUI, attenersi alla seguente procedura:
     a. Avviare la GUI immettendo il comando **mqiptKeyman**.
     b. Fare clic su **File database di chiavi** > **Apri**.

c. Fare clic su **Tipo database di chiavi** e selezionare **PKCS11Config**.

d. Fare clic su **OK**. Viene visualizzata la finestra Apri token crittografico.

e. Selezionare l'etichetta del token dell'unità crittografica che si desidera utilizzare per memorizzare i certificati.

f. Nel campo **Password token crittografico** , immettere la password necessaria per accedere all'hardware crittografico.

g. Per creare un nuovo file keyring CA, selezionare **Crea nuovo file database di chiavi secondario**.

h. Fare clic su **Tipo database delle chiavi** e selezionare **PKCS12**.

i. Nel campo **Nome file** , immettere il nome file del keyring CA.

j. Nel campo **Ubicazione** , immettere il percorso completo del file key ring CA.

k. Fare clic su **OK**. Viene visualizzata la finestra Richiesta password.

l. Immettere una password per il keyring CA nel campo **Password** e immetterla nuovamente nel campo **Conferma password** .

m. Fare clic su **OK**.

4. Utilizzando **mqiptKeycmd** o **mqiptKeyman**, richiedere un certificato personale per l'hardware crittografico.

- Per utilizzare la CLI, immettere il comando seguente:

```
mqiptKeycmd -certreq -create -crypto module_name -tokenlabel hardware_token
            -pw password -label label -size key_size
            -sig_alg algorithm -dn distinguished_name -file filename
```

dove:

-crypto *nome_modulo*
Specifica il nome completo della libreria PKCS #11 fornita con l'hardware crittografico.

-tokenlabel *etichetta_token*
Specifica l'etichetta del token dell'unità crittografica PKCS #11 .

-pw *password*
Specifica la parola d'ordine per l'accesso all'hardware crittografico.

-label *label*
Specifica l'etichetta del certificato.

-size *dimensione_chiave*
Specifica la dimensione della chiave. Il valore può essere 512, 1024, 2048o 4096.

-sig_alg *algoritmo*
Specifica l'algoritmo di firma asimmetrico utilizzato per creare la coppia di chiavi della voce. Il valore può essere MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSAo SHAWithDSA. Il valore predefinito è SHA256WithRSA.

-dn *nome_distinto*
Specifica il nome distinto X.500 racchiuso tra virgolette.

-file *nomefile*
Specifica il nome file per la richiesta di certificato.

- Per utilizzare la GUI, attenersi alla seguente procedura:

a. Dal menu **Crea** , fare clic su **Nuova richiesta certificato**.

b. Nel campo **Etichetta chiave** , immettere l'etichetta del certificato.

c. Selezionare la **Dimensione chiave** e l' **Algoritmo di firma** richiesti.

d. Immettere i valori per **Nome comune** e **Organizzazione**e selezionare un **Paese**. Per i restanti campi facoltativi, accettare i valori predefiniti oppure immettere o selezionare nuovi valori.

e. Nel campo **Immettere il nome di un file in cui memorizzare la richiesta di certificato** , accettare il valore predefinito `certreq.arm`oppure immettere un nuovo valore con un percorso completo.

f. Fare clic su **OK**.

g. L'elenco **Richieste di certificati personali** mostra l'etichetta della nuova richiesta di certificato personale creata. La richiesta di certificato viene memorizzata nel file scelto.

5. Dopo che la CA ha inviato il certificato personale, aggiungere il certificato CA al keystore crittografico o al file key ring della CA, se non è già presente.

   - Per utilizzare la CLI per aggiungere il certificato CA al file key ring CA, immettere il seguente comando:

     ```
     mqiptKeycmd -cert -add -db filename -pw password -type pkcs12
                 -label label -file cert_filename
     ```

     dove *filename* è il nome del file di chiavi CA, *password* è la password del file di chiavi CA, *label* è l'etichetta allegata al certificato e *cert_filename* è il nome del file contenente il certificato CA.

   - Per utilizzare la CLI per aggiungere il certificato CA all'hardware crittografico, immettere il seguente comando:

     ```
     mqiptKeycmd -cert -add -crypto module_name -tokenlabel hardware_token
                 -pw password -label label -file cert_filename
     ```

     dove *module_name* è il nome completo della libreria PKCS #11 fornita con l'hardware crittografico, *hardware_token* è l'etichetta del token del dispositivo crittografico PKCS #11 , *password* è la password per l'accesso all'hardware crittografico, *label* è l'etichetta allegata al certificato e *cert_filename* è il nome del file contenente il certificato CA.

   - Per utilizzare la GUI, attenersi alla seguente procedura:

     a. Nel campo **Contenuto database delle chiavi**, selezionare **Certificati del firmatario**.

     b. Fare clic su **Aggiungi**. Viene aperta la finestra per aggiungere la certificazione della CA (autorità di certificazione) da un file.

     c. Digitare il nome del file e la posizione di memorizzazione del certificato oppure fare clic su **Sfoglia** per selezionare il nome e la posizione.

     d. Fare clic su **OK**. Viene visualizzata la finestra Immettere un'etichetta.

     e. Nella finestra Immettere un'etichetta, digitare il nome del certificato.

     f. Fare clic su **OK**. Il certificato viene aggiunto al database di chiavi.

6. Ricevere il certificato personale, fornito dalla CA, nel keystore dell'hardware crittografico.

   - Per utilizzare la CLI, immettere il comando seguente:

     ```
     mqiptKeycmd -cert -receive -file filename -crypto module_name
                 -tokenlabel hardware_token -pw password
     ```

     dove *filename* è il nome del file contenente il certificato da ricevere, *module_name* è il nome completo della libreria PKCS #11 fornita con l'hardware crittografico, *hardware_token* è l'etichetta del token del dispositivo crittografico PKCS #11 e *password* è la password per l'accesso all'hardware crittografico.

     Se il certificato CA è memorizzato in un file di chiavi CA, piuttosto che nell'hardware crittografico, si riceverà un'avvertenza che la catena di certificati non può essere convalidata poiché il comando **mqiptKeycmd** non può accedere al file di chiavi CA quando si riceve il certificato personale nel file di chiavi crittografico.

   - Per utilizzare la GUI, attenersi alla seguente procedura:

     a. Fare clic su **Ricevi**. Viene visualizzata la finestra Ricevi certificato da file.

b. Immettere il nome file del certificato e l'ubicazione per il nuovo certificato personale oppure fare clic su **Sfoglia** per selezionare il nome e l'ubicazione.

c. Fare clic su **OK**. Il campo **Certificati personali** visualizza l'etichetta del nuovo certificato personale aggiunto.

7. Codificare la parola d'ordine per accedere all'hardware crittografico utilizzando il comando **mqiptPW** .

   V 9.1.5 Immettere il seguente comando:

   ```
   mqiptPW -sf encryption_key_file
   ```

   dove *encryption_key_file* è il nome di un file che contiene la chiave di codifica della password per l'installazione di MQIPT . Non è necessario specificare il parametro **-sf** se l'installazione di MQIPT utilizza la chiave di codifica della password predefinita. Immettere la password per accedere all'hardware crittografico da codificare quando richiesto.

   Per ulteriori informazioni sulla codifica delle password dell'archivio chiavi, consultare “Codifica di una password key ring in MQIPT” a pagina 982.

8. Se è stato creato un file di chiavi CA nel passo “3” a pagina 998, codificare la password per il file di chiavi CA seguendo le istruzioni nel passo “7” a pagina 1001.

9. Modificare il file di configurazione `mqipt.conf` .

   a) Confermare di disporre della titolarità appropriata per utilizzare questa funzione IBM MQ Advanced impostando la proprietà globale **EnableAdvancedCapabilities** su `true`.

   b) Abilitare l'utilizzo del keystore hardware di crittografia sull'instradamento impostando una o più delle proprietà **SSLServerKeyRingUseCryptoHardware**, **SSLServerCAKeyRingUseCryptoHardware**, **SSLServerKeyRingUseCryptoHardware**o **SSLServerKeyRingUseCryptoHardware** su `true`.

   Per ulteriori informazioni sulle proprietà per abilitare l'utilizzo dell'hardware crittografico su un instradamento, consultare MQIPT route properties.

   c) Se si sta utilizzando un file di chiavi per i certificati CA, specificare l'ubicazione del file di chiavi CA impostando una o più proprietà **SSLServerCAKeyRing** o **SSLServerCAKeyRing** .

   Se è stato configurato un instradamento per utilizzare l'hardware di crittografia per il certificato del sito e non si specifica un file keyring CA, il keystore dell'hardware di crittografia viene utilizzato come keystore CA.

   d) Specificare la password crittografata per accedere all'hardware crittografico e al keyring CA utilizzando la proprietà **SSLServerKeyRingPW**, **SSLServerCAKeyRingPW**, **SSLClientKeyRingPW**o **SSLClientCAKeyRingPW** .

   V 9.1.5 Impostare il valore delle proprietà **SSL*KeyRingPW** sull'output della password codificata mediante il comando **mqiptPW** .

   e) Se l'hardware crittografico contiene più di un certificato personale, specificare quale certificato deve essere selezionato da MQIPT da inviare al server SSL/TLS o al client per l'autenticazione.

   È possibile specificare quale certificato deve essere selezionato impostando una o più proprietà **SSLClientSite*** per un instradamento client SSL/TLS o una o più proprietà **SSLServerSite*** per un instradamento server SSL/TLS.

   Per ulteriori informazioni sulla selezione dei certificati da un keyring, consultare “Selezione di certificati da un file di chiavi in MQIPT” a pagina 982. Le proprietà per selezionare un certificato da un file di chiavi sono descritte in MQIPT proprietà di instradamento.

V 9.1.5 Ad esempio, per utilizzare un keystore hardware crittografico per il certificato sito su un instradamento server TLS e un file key ring per memorizzare i certificati CA per lo stesso instradamento, aggiungere le seguenti proprietà alla definizione di instradamento:

```
SSLServerKeyRingUseCryptoHardware=true
SSLServerKeyRingPW=<mqiptPW>1!gORdM4wft5d1rCgNMDEGag==!dZxhgQD2A8Ea0yeqawQvPg==
SSLServerCAKeyRing=/opt/mqipt/ssl/ca.pfx
```

```
SSLServerCAKeyRingPW=<mqiptPW>1!3Vdrpiu6kMwn0sWRCVgT5g==!LHltGLEg3OFvN8+02Re0YA==
SSLServerSiteLabel=mqiptsite
```

10. Riavviare MQIPT.

Java security manager in MQIPT

Java security manager può essere utilizzato con qualsiasi funzione MQIPT per fornire un ulteriore livello di sicurezza.

MQIPT utilizza il valore predefinito Java security manager come definito nella classe `java.lang.SecurityManager` . La funzione Java security manager in MQIPT può essere abilitata o disabilitata utilizzando la proprietà globale **`SecurityManager`**. Per ulteriori informazioni, consultare MQIPT proprietà globali .

Java security manager utilizza due file di politica predefiniti:

- Un file della politica del sistema globale denominato *$MQIPT_PATH*`/java/jre/lib/security/java.policy` (dove *$MQIPT_PATH* è la directory in cui è installato MQIPT) viene utilizzato da tutte le istanze di una macchina virtuale su un host.
- Un file della politica specifico per l'utente denominato `.java.policy`, che può esistere nella directory home dell'utente.

È anche possibile utilizzare un ulteriore file della politica MQIPT . Si consiglia di utilizzare il file delle politiche MQIPT invece dei file delle politiche predefiniti descritti in precedenza. Per ulteriori informazioni, consultare **`SecurityManagerPolicy`** in MQIPT proprietà globali .

La sintassi del file delle politiche è piuttosto complessa e, sebbene sia possibile modificarla utilizzando un editor di testo, di solito è più semplice utilizzare il programma di utilità Policy Tool fornito con Java per apportare eventuali modifiche. Il programma di utilità Policy Tool è disponibile nella directory *$MQIPT_PATH*`/java/jre/bin` ed è completamente documentato nella documentazione Java.

Un file della politica di esempio (`mqiptSample.policy`) è stato fornito con MQIPT per mostrare quali autorizzazioni devono essere impostate per l'esecuzione di MQIPT.

È necessario modificare il file della politica di esempio in modo che corrisponda alla configurazione. In particolare, tenere presente che la directory home di MQIPT (l'ubicazione di mqipt.conf) potrebbe non essere la stessa della directory di installazione di MQIPT , quindi prestare attenzione a specificare le directory corrette durante la configurazione delle voci FilePermission nella politica di sicurezza.

È necessario modificare le seguenti voci:

- La voce **`java.io.FilePermission`** che concede l'accesso in lettura e scrittura alla directory degli errori. Il percorso file in questa voce deve fare riferimento alla directory home di MQIPT , poiché è qui che si trova la directory degli errori. MQIPT crea i file FFST Failure Data Capture (`AMQ*.FDC`) e i file di traccia (`AMQ*.TRC*`) nella directory degli errori. È necessario assicurarsi che MQIPT disponga dell'autorizzazione per creare file di traccia e FFST nella directory degli errori, in modo che sia possibile la risoluzione dei problemi.
- La voce **`java.io.FilePermission`** che concede l'accesso in lettura e scrittura alla directory dei log. Il percorso file in questa voce deve fare riferimento alla directory home di MQIPT , poiché è qui che si trova la directory dei log. MQIPT crea i file di log di connessione (`mqipt*.log`) nella directory logs se la proprietà globale ConnectionLog è abilitata.
- Le voci **`java.io.FilePermission`** che concedono l'accesso in lettura ed esecuzione a qualsiasi directory nella directory di installazione di MQIPT , come le directory `bin`, `exits`, `libe` `ssl` . I percorsi dei file in queste voci devono essere modificati per fare riferimento alla directory di installazione di MQIPT . Alcune di queste voci possono essere omesse se non sono richieste.
- Le voci **`java.net.SocketPermission`** devono essere modificate per controllare le connessioni in ciascun instradamento MQIPT in ascolto. Le autorizzazioni di ascolto e accettazione sono richieste per la porta listener e l'indirizzo listener per ogni instradamento MQIPT .
- Le voci **`java.net.SocketPermission`** devono essere modificate per controllare le connessioni al di fuori di ogni instradamento MQIPT . L'autorizzazione di connessione è richiesta per tutte le

destinazioni di instradamento, i server proxy o i server LDAP a cui si connette l'instradamento MQIPT . L'autorizzazione di risoluzione è richiesta quando si specificano gli indirizzi utilizzando un nome host.

A seconda della configurazione, potrebbe essere necessario aggiungere anche le seguenti voci:

- Una voce **java.io.FilePermission** per concedere l'accesso in lettura a mqipt.confo alla directory home di MQIPT contenente mqipt.conf. Se è necessario configurare MQIPT in remoto utilizzando il Client di gestione, MQIPT avrà anche bisogno dell'accesso in scrittura a mqipt.conf in modo che possa salvare le modifiche di configurazione.
- Una voce **java.io.FilePermission** per concedere l'accesso in lettura al file della politica di sicurezza. Ciò è utile se un aggiornamento MQIPT fa sì che il file della politica di sicurezza venga riletto.
- Alcune voci **java.io.FilePermission** per concedere l'accesso in lettura ai file keyring SSL/TLS e ai file stash delle password. Ciò è richiesto solo quando si utilizza un instradamento con le proprietà SSLClient o SSLServer abilitate.
- Alcune voci **java.io.FilePermission** per concedere l'accesso di lettura o esecuzione a qualsiasi classe di uscita MQIPT . Ciò è richiesto solo quando è abilitata un'uscita MQIPT . Potrebbe essere necessario concedere ulteriori autorizzazioni, se richiesto dall'uscita.

Nota: Le voci Windows **java.io.FilePermission** devono utilizzare due caratteri barra rovesciata (\\) per ogni barra rovesciata nel percorso. Ciò è dovuto al fatto che una singola barra rovesciata viene utilizzata come carattere escape.

Il file di esempio presuppone che MQIPT sia stato installato su un sistema Windows in `C:\Program Files\IBM\MQ Internet Pass-Thru`. Si presuppone inoltre che la directory home di MQIPT (l'ubicazione del file `mqipt.conf`) sia uguale alla directory di installazione di MQIPT .

Se MQIPT è stato installato in un'altra posizione, è necessario modificare la directory nella definizione codeBase per fare riferimento alla propria directory di installazione di MQIPT . Fare attenzione a includere il prefisso corretto (`file:/`) e il suffisso file corretto (`/lib/com.ibm.mq.ipt.jar`). Sui sistemi UNIX and Linux , un tipico URL codeBase potrebbe essere `file:/opt/mqipt/lib/com.ibm.mq.ipt.jar`, supponendo che MQIPT sia installato in `/opt/mqipt`.

Le autorizzazioni sono generalmente definite con tre attributi. Per controllare le connessioni socket, i loro valori sono:

autorizzazione classe
`java.net.SocketPermission`

nome da controllare
Questo è costituito dal formato `hostname:port`, in cui ogni componente del nome può essere specificato da un carattere jolly. Il nome host può essere un nome dominio o un indirizzo IP. La posizione più a sinistra del nome host può essere specificata da un asterisco (*). Ad esempio, `harry.company1.com` corrisponderebbe a ciascuna di queste stringhe:

- `harry`
- `harry.company1.com`
- `*.company1.com`
- `*`
- `198.51.100.123` (supponendo che questo sia l'indirizzo IP di `harry.company1.com`)

Il componente porta del nome può essere specificato come un indirizzo porta singolo o un intervallo di indirizzi porta, ad esempio:

1414
solo porta 1414

1414-
tutti gli indirizzi di porta maggiori o uguali a 1414

-1414
tutti gli indirizzi di porta minori o uguali a 1414

1-1414
tutti gli indirizzi di porta compresi tra 1 e 1414, inclusi

Azione consentita
Le azioni utilizzate da `java.net.SocketPermission` sono:

- accettare, ciò consente all'autorizzazione di accettare le connessioni dalla destinazione specificata
- connessione, consente l'autorizzazione a connettersi alla destinazione specificata
- in ascolto, ciò consente l'autorizzazione ad ascoltare sulla porta o sulle porte specificate per le richieste di connessione
- risolvi, consente di utilizzare il servizio nomi DNS per risolvere i nomi dominio in indirizzi IP

Il controllo di Java security manager può essere effettuato anche tramite le proprietà di sistema `java.security.manager` e `java.security.policy` Java , ma si consiglia di utilizzare le proprietà SecurityManager e SecurityManagerPolicy per il controllo MQIPT.

Per includere informazioni diagnostiche nella traccia e nei record FFST , MQIPT deve accedere a determinate proprietà di sistema e variabili di ambiente MQIPT . È necessario includere sempre le seguenti proprietà nella politica di sicurezza Java :

```
permission java.util.PropertyPermission "java.home", "read";
permission java.util.PropertyPermission "java.version", "read";
permission java.util.PropertyPermission "java.runtime.version", "read";
permission java.util.PropertyPermission "java.vm.info", "read";
permission java.util.PropertyPermission "java.vm.vendor", "read";
permission java.util.PropertyPermission "os.arch", "read";
permission java.util.PropertyPermission "os.name", "read";
permission java.util.PropertyPermission "os.version", "read";
permission java.lang.RuntimePermission "getenv.MQIPT_PATH";
permission java.lang.RuntimePermission "getStackTrace";
```

Se non si includono tutte queste proprietà, MQIPT non funzionerà correttamente e la diagnostica del problema sarà compromessa.

Uscite di sicurezza in MQIPT

Utilizzare un'uscita di sicurezza per controllare l'accesso a una destinazione, come definita dalla proprietà di instradamento **Destination** . L'uscita di sicurezza viene richiamata nel punto in cui MQIPT riceve una richiesta di connessione da un client, ma prima di effettuare la connessione alla destinazione di destinazione.

In base alle proprietà di connessione iniziali, l'uscita di sicurezza decide se è possibile completare la connessione.

Quando viene avviato un instradamento, l'uscita di sicurezza viene richiamata per inizializzarsi e per prepararsi a elaborare una richiesta di collegamento. Il processo di inizializzazione deve essere utilizzato per caricare tutti i dati utente e preparare questi dati per un accesso rapido e semplice, riducendo così il tempo necessario per elaborare una richiesta di connessione.

Ogni instradamento può avere la propria uscita di sicurezza.

- La proprietà **SecurityExit** viene utilizzata per abilitare / disabilitare l'uscita di sicurezza definita dall'utente.
- La propriet ... **SecurityExitName** viene utilizzata per definire il nome classe dell'exit di sicurezza definita dall'utente.
- La proprietà **SecurityExitPath** viene utilizzata per definire il nome della directory contenente il file di classe. Se questa proprietà non è impostata, si presuppone che il file di classe si trovi nella sottodirectory delle uscite. **SecurityExitPath** può anche definire il nome di un file JAR contenente l'uscita di sicurezza definita dall'utente.
- La proprietà **SecurityExitTimeout** viene utilizzata da MQIPT per determinare per quanto tempo deve attendere una risposta dall'uscita di sicurezza durante la convalida di una richiesta di connessione.

Consultare MQIPT proprietà di instradamento per dettagli sulle proprietà dell'uscita di sicurezza.

MQIPT utilizza la classe `SecurityExit` per richiamare un'uscita di sicurezza definita dall'utente. Questa classe deve essere estesa dall'uscita di sicurezza definita dall'utente e la maggior parte dei suoi metodi deve essere sovrascritta per fornire la funzionalità richiesta. Un oggetto `SecurityExitResponse` viene utilizzato per restituire i dati a MQIPT e questi dati vengono usati da MQIPT per decidere se la richiesta di connessione deve essere accettata o rifiutata. L'oggetto `SecurityExitResponse` può contenere anche una nuova destinazione e un indirizzo di porta di destinazione, utilizzati per sovrascrivere l'instradamento definito dalle proprietà dell'uscita di sicurezza.

Vengono fornite tre uscite di sicurezza di esempio per mostrare come è possibile implementare un'uscita di sicurezza.

- `SampleSecurityExit` mostra come controllare l'accesso a un gestore code IBM MQ , in base al nome del canale IBM MQ . Consente solo una connessione con un nome canale che inizia con la stringa "MQIPT." Per ulteriori informazioni, consultare Utilizzo di un'uscita di sicurezza .
- `SampleRoutingExit` consente l'instradamento dinamico delle richieste di connessioni client a un pool di server IBM MQ definiti, ciascun server che ospita un gestore code con lo stesso nome e gli stessi attributi. L'esempio include un file di configurazione che contiene un elenco di nomi server. Per ulteriori informazioni, consultare Instradamento delle richieste di connessione client ai server del gestore code IBM MQ utilizzando le uscite di sicurezza .
- `SampleOneRouteExit` consente l'instradamento dinamico a un gestore code IBM MQ derivato dal nome del canale IBM MQ utilizzato nella richiesta di connessione. L'esempio include un file di configurazione che contiene una mappa di nomi gestore code e nomi server. Per ulteriori informazioni, consultare Instradamento dinamico delle richieste di connessione client .

Nota: MQIPT viene eseguito in una singola JVM, in modo che un'uscita di sicurezza definita dall'utente possa compromettere il normale funzionamento di MQIPT in uno dei seguenti modi:

- Influisce sulle risorse di sistema
- Genera colli di bottiglia
- Prestazioni ridotte

È necessario verificare ampiamente gli effetti dell'uscita di sicurezza prima di implementarla in un ambiente di produzione.

La classe com.ibm.mq.ipt.exit.SecurityExit in MQIPT

Questa classe e i relativi metodi pubblici devono essere estesi dall'uscita di sicurezza definita dall'utente per accedere ad alcuni dati comuni e consentire l'inizializzazione di MQIPT .

Prima che ogni metodo venga richiamato da MQIPT, alcune proprietà saranno rese disponibili per l'utilizzo da parte del metodo. I loro valori possono essere richiamati utilizzando i metodi get appropriati definiti in questa classe.

Metodi

init int pubblico (IPTTrace)

Sono disponibili le seguenti proprietà:

- porta del listener
- destinazione
- porta di destinazione
- versione

Il metodo init verrà richiamato da MQIPT quando viene avviato un instradamento. Al ritorno da questo metodo, l'exit di protezione deve essere pronta per convalidare una richiesta di collegamento. I codici di ritorno possibili validi sono ExitRc.OK o ExitRc.ERRORE INIT.

aggiornamento int pubblico (IPTTrace)

Sono disponibili le seguenti proprietà:

- porta del listener

- destinazione
- porta di destinazione

Il metodo di aggiornamento verrà richiamato da MQIPT quando viene richiesto di aggiornare se stesso da IPT Administration Client. Questa azione di solito viene richiamata quando una proprietà è stata modificata nel file di configurazione. MQIPT caricherà tutte le proprietà dal file di configurazione e determinerà quali sono state modificate e se un instradamento deve essere riavviato immediatamente o se può attendere fino al successivo riavvio di MQIPT .

Questo metodo deve eseguire un ricaricamento dei dati esterni che utilizza (ovvero, i dati caricati durante il metodo init). I codici di ritorno possibili validi sono ExitRc.OK o ExitRc.ERRORE_GRATUITA.

public void close (IPTTrace)
Sono disponibili le seguenti proprietà:

- porta del listener
- destinazione
- porta di destinazione

Il metodo close () verrà richiamato da MQIPT quando viene richiesto di arrestarlo da MQIPT IPT Administration Client. Dovrebbe liberare tutte le risorse di sistema che ha acquisito durante il suo funzionamento. MQIPT attenderà il completamento di questo metodo prima di chiudere.

Questo metodo verrà richiamato anche se è stata abilitata un'uscita di sicurezza, ma ora è stata disabilitata nel file di configurazione.

convalida della risposta SecurityExitpubblica (IPTTrace)
Sono disponibili le seguenti proprietà:

- porta del listener
- destinazione
- porta di destinazione
- tempo massimo
- Indirizzo IP client
- indirizzo porta client
- nome canale
- Nome gestore code

Il metodo validate verrà richiamato da MQIPT quando riceve una richiesta di convalida di connessione. Il nome del canale e il nome del gestore code non saranno disponibili se la proprietà SSLProxyMode è stata abilitata, poiché questa funzione viene utilizzata solo per eseguire il tunneling dei dati SSL/TLS e quindi i dati di solito ottenuti dal flusso di dati iniziale non saranno leggibili.

L'uscita di sicurezza deve restituire un oggetto risposta SecurityExit, contenente le seguenti informazioni:

- codice motivo (deve essere impostato)
- nuovo indirizzo di destinazione (facoltativo)
- nuovo indirizzo porta listener di destinazione (facoltativo)
- Messaggio (opzionale)

Il codice di errore determinerà se la connessione verrà accettata o rifiutata da MQIPT. I campi newDestination e newDestinationPort possono essere facoltativamente impostati per definire un nuovo gestore code di destinazione. Se non si impostano queste proprietà, verranno utilizzate le proprietà di destinazione di instradamento e DestinationPort definite nel file di configurazione. Qualsiasi messaggio verrà aggiunto alla voce del file di log di connessione.

Metodi supportati per ottenere le proprietà:

public int getListenerPorta ()
richiama la porta del listener di instradamento - come definito dalla proprietà ListenerPort

public String getDestination()
richiama l'indirizzo di destinazione - come definito dalla proprietà Destinazione

public int getDestinationPort ()
richiama l'indirizzo della porta del listener di destinazione - come definito dalla proprietà DestinationPort

public String getClientIPAddress ()
richiama l'indirizzo IP del client che effettua la richiesta di collegamento

public int getClientPortAddress()
richiama l'indirizzo porta utilizzato dal client che effettua la richiesta di connessione

public int getTimeout()
richiama il valore di timeout. MQIPT attenderà che l'uscita di sicurezza convalidi una richiesta - come definito dalla proprietà Timeout SecurityExit

public int getConnThreadID()
richiama l'ID thread di collegamento che gestisce la richiesta di collegamento, utile per il debug

public String getChannelNome ()
richiama il nome canale IBM MQ utilizzato nella richiesta di collegamento

public String getQMName()
richiama il nome del gestore code IBM MQ utilizzato nella richiesta di connessione

Booleano pubblico getTimedout()
può essere utilizzato dall'uscita di sicurezza per stabilire se il timeout è scaduto

La classe com.ibm.mq.ipt.exit.SecurityExitResponse

Questa classe viene utilizzata per passare una risposta a MQIPT da un'exit di sicurezza definita dall'utente e viene utilizzata per stabilire se la richiesta di connessione deve essere accettata o rifiutata. Gli oggetti di questo tipo vengono creati solo nel metodo di convalida (consultare "La classe com.ibm.mq.ipt.exit.SecurityExit in MQIPT" a pagina 1005). Esistono costruttori di convenienza per la creazione di questi oggetti ed esistono metodi per ogni proprietà. Consultare le uscite di sicurezza di esempio per ulteriori informazioni.

La creazione di un oggetto risposta SecurityExitpredefinito rifiuta la richiesta di connessione.

Costruttori

- **public SecurityExitResponse (String dest, int destPort, int rc, String msg)**

  dove:

  - `dest` è la nuova destinazione
  - `destPort` è il nuovo indirizzo porta di destinazione
  - `rc` è il codice di errore
  - `msg` è un messaggio che verrà aggiunto alla voce del log di connessione
- **public SecurityExitResponse (String dest, int destPort, int rc)**
- **public SecurityExitRisposta (int rc, String msg)**
- **SecurityExitRisposta (int rc)**

Metodi

public void setDestination(String dest)
imposta un indirizzo di destinazione nuovo per la richiesta di collegamento

public void setDestinationLa porta (int port) genera IPTException
imposta un nuovo indirizzo di porta del listener di destinazione per la richiesta di connessione - genera un'eccezione IPTException per un indirizzo di porta non valido

public void setMessage(String msg)
aggiunge un messaggio al record di log di connessione

public void setReasonCodice (int rc)
imposta il codice motivo per la richiesta di collegamento.

Codici di ritorno dell'uscita di sicurezza in MQIPT

I codici di ritorno che MQIPT riconosce quando richiama un'uscita di sicurezza in diverse situazioni.

I seguenti codici di ritorno vengono riconosciuti da MQIPT quando si richiama un'uscita di sicurezza nelle seguenti situazioni:

Codice di ritorno	Descrizione	inizializzare	Convalida	Aggiorna
ExitRc.OK	Richiesta completata correttamente.	sì	sì	sì
ExitRc.ERRORE DI INIZIALIZZAZIONE	Richiesta di inizializzazione non riuscita, l'instradamento verrà disabilitato.	sì		
ExitRc.ERRORE_RISPEDIZIONE	Richiesta di aggiornamento non riuscita.			sì
ExitRc.NON_AUTORIZZATO	Processo di convalida non riuscito, richiesta di connessione rifiutata.		sì	
ExitRc.DISABILITAZIONE_SSL	Richiesta di convalida riuscita, la connessione alla destinazione non utilizzerà SSL o TLS.		sì	

Controllo numero porta in MQIPT

Quando si utilizza MQIPT, è possibile limitare l'intervallo del numero di porta locale utilizzato quando si effettua una connessione in uscita.

Impostare la proprietà **OutgoingPort** sull'instradamento per specificare il numero di porta locale iniziale e impostare **MaxConnectionThreads** per specificare il numero di porte da utilizzare. Ad esempio, se si imposta **OutgoingPort** su 1600 e **MaxConnectionThreads** su 20, l'intervallo dei numeri di porta locali per tale instradamento è 1600 - 1619.

È responsabilità dell'amministratore di MQIPT assicurarsi che non vi siano conflitti di numeri di porta tra gli instradamenti.

Se **OutgoingPort** non è definito, un valore predefinito di 0 indica che per ogni connessione viene utilizzato un numero di porta assegnato dal sistema.

Quando si utilizza HTTP, il numero di porte in uscita è doppio rispetto a quando non si utilizza HTTP. Nell'esempio precedente, se l'instradamento utilizzava HTTP, l'intervallo di numeri sarebbe 1600 - 1639.

Per ulteriori informazioni, consultare Assegnazione di numeri di porte .

Sistemi multihomed

Quando si usa un sistema multihomed, è possibile specificare a quale indirizzo IP si collegherà una connessione in uscita utilizzando la proprietà **LocalAddress** . I nomi host non sono supportati su questa proprietà.

V 9.1.5 Crittografia delle password memorizzate in MQIPT

La configurazione di MQIPT potrebbe includere le password per accedere a varie risorse, nonché la password per accedere a MQIPT utilizzando la porta comandi. Da IBM MQ 9.1.5, tutte queste password devono essere protette mediante crittografia.

Informazioni su questa attività

Nelle versioni precedenti a IBM MQ 9.1.5, è possibile codificare solo le password utilizzate da MQIPT per accedere ai file di chiavi o agli archivi di chiavi hardware crittografico. Le password codificate vengono memorizzate in file a cui fa riferimento una delle proprietà **SSL*KeyRingPW** . Le altre password per i server LDAP e la password di accesso MQIPT sono memorizzate in testo semplice nel file di configurazione `mqipt.conf` .

Da IBM MQ 9.1.5, tutte le password archiviate per l'utilizzo da parte di MQIPT devono essere protette codificando la password con il comando **mqiptPW** . Le password codificate vengono memorizzate come valori di proprietà nel file di configurazione `mqipt.conf` . MQIPT è in grado di distinguere tra password codificate, password in testo semplice e nomi file nei valori delle proprietà. È necessario crittografare tutte le password memorizzate per l'utilizzo da parte di MQIPT in questo modo in quanto è il metodo di protezione più sicuro.

Il metodo di crittografia delle password dell'archivio chiavi utilizzato in MQIPT prima di IBM MQ 9.1.5 è obsoleto, ma può essere ancora utilizzato. Per migliorare la protezione delle password key ring, codificare nuovamente le password key ring precedentemente codificate, utilizzando il metodo di protezione più recente.

Se nella configurazione di MQIPT è presente un testo semplice o una password debolmente protetta, viene emesso un messaggio di avviso quando viene avviato MQIPT o quando viene avviato un instradamento.

Utilizzare questa procedura per codificare una password da memorizzare per l'utilizzo da parte di MQIPT utilizzando il metodo di protezione più recente. Per codificare una password key ring in MQIPT in IBM MQ 9.1.4 o versioni precedenti, attenersi alla procedura descritta in “Crittografia di una password key ring in MQIPT in IBM MQ 9.1.4 o versioni precedenti” a pagina 1010.

Procedura

1. Opzionale: Creare un file contenente la chiave di codifica della password, se non si dispone già di una chiave.

   MQIPT utilizza una chiave di codifica per codificare le password. È possibile specificare la propria chiave di codifica in un file. Il file deve contenere almeno un carattere e solo una riga di testo.

   La stessa chiave di codifica della parola d'ordine viene utilizzata per codificare e decodificare tutte le parole d'ordine memorizzate per un'istanza di MQIPT. Pertanto, è necessario solo un singolo file di chiavi di codifica della parola d'ordine per ogni installazione di MQIPT .

   Se si intende eseguire MQIPT come un servizio avviato automaticamente, è necessario creare il file della chiave di codifica della password con il nome predefinito `mqipt_cred.keye` posizionarlo nella directory home MQIPT .

   Non è necessario specificare una chiave di codifica della password, tuttavia è più sicuro farlo. Se non si specifica la propria chiave di codifica, viene utilizzata la chiave di codifica predefinita.

   Nota: È necessario assicurarsi che le autorizzazioni file appropriate siano impostate sul file della chiave di codifica della parola d'ordine per impedire agli utenti non autorizzati di leggere la chiave di codifica. Solo l'utente che esegue il comando **mqiptPW** e l'utente con cui viene eseguito MQIPT necessitano dell'autorità per leggere la chiave di codifica della parola d'ordine.
2. Codificare la password utilizzando il comando **mqiptPW** .

   La sintassi del comando **mqiptPW** è descritta in mqiptPW (encrypt stored password).

   Se è stato creato un file di chiavi di codifica della password nel passo “1” a pagina 1009, specificare il nome file utilizzando il parametro **-sf** su **mqiptPW**. Ad esempio, il seguente comando può essere immesso per codificare una parola d'ordine utilizzando la chiave di codifica nel file specificato dal parametro **-sf** :

   ```
   mqiptPW -sf /opt/mqipt/mqipt_password.key
   ```
3. Immettere la password da codificare quando richiesto.

La password codificata verrà emessa da **mqiptPW**.

4. Copiare la password codificata nella proprietà appropriata nel file di configurazione `mqipt.conf` .

   Ad esempio, la seguente riga specifica una parola d'ordine codificata per la parola d'ordine di accesso MQIPT :

   ```
   AccessPW=<mqiptPW>1!QL+2Jvj/tigKKlD7Nz8Oqw==!AMDBefOUrmPf5i1OuqV5MA==
   ```

5. Avviare MQIPT. Se è stato creato un file di chiavi di codifica della password nel passo “1” a pagina 1009 con un nome diverso da quello predefinito, specificare il nome del file di chiavi di codifica all'inizio di MQIPT.

   È possibile specificare il nome del file della chiave di codifica password utilizzando il parametro **-sf** quando si avvia MQIPT. Ad esempio, immettere il seguente comando per avviare MQIPT utilizzando la chiave di crittografia nel file specificato dal parametro **-sf** :

   ```
   mqipt /opt/mqipt -sf /opt/mqipt/mqipt_password.key
   ```

   Per informazioni su altri metodi per specificare il nome file della chiave di codifica della password all'avvio di MQIPT, consultare Specifica della chiave di codifica della password.

Crittografia di una password key ring in MQIPT in IBM MQ 9.1.4 o versioni precedenti

In IBM MQ 9.1.4 e versioni precedenti, le parole d'ordine codificate utilizzate per accedere ai file di chiavi utilizzati da MQIPT sono memorizzate in file. Seguire la procedura in questa attività per codificare una password key ring per l'utilizzo da parte di MQIPT in IBM MQ 9.1.4 o versioni precedenti.

Informazioni su questa attività

Da MQIPT in IBM MQ 9.1.5, utilizzare invece il metodo di protezione più sicuro descritto in “Crittografia delle password memorizzate in MQIPT” a pagina 1008 .

Procedura

1. Codificare la password key ring utilizzando il comando **mqiptPW** .

   Immettere il seguente comando per codificare la parola d'ordine:

   ```
   mqiptPW password filename
   ```

   dove

   password
   è la password in testo chiaro necessaria per accedere al keyring

   nome file
   è il nome del file di password da creare

   La sintassi del comando **mqiptPW** è descritta in mqiptPW (encrypt stored password).

2. Impostare la proprietà di instradamento appropriata sul nome del file che contiene la password codificata creata nel passaggio “1” a pagina 1010.

   Ad esempio, per specificare il file di password per il key ring che contiene il certificato server TLS MQIPT , aggiungere la riga seguente al file di configurazione `mqipt.conf` :

   ```
   SSLServerKeyRingPW=filename
   ```

Altre considerazioni sulla sicurezza per MQIPT

MQIPT dispone di diverse funzioni aggiuntive che consentono a un designer di creare una soluzione sicura.

- Se ci sono molti client in una rete interna che tentano di effettuare connessioni in uscita, possono tutti passare attraverso un MQIPT che si trova all'interno del firewall. L'amministratore del firewall deve quindi concedere l'accesso esterno solo al computer MQIPT .
- MQIPT può connettersi solo ai gestori code per cui è stato esplicitamente configurato nel relativo file di configurazione, a meno che MQIPT non agisca come un proxy SOCKS o utilizzi un'uscita di sicurezza.
- MQIPT verifica che i messaggi ricevuti e trasmessi siano validi e conformi al protocollo IBM MQ . Ciò consente di evitare che MQIPT venga utilizzato per attacchi di sicurezza all'esterno del protocollo IBM MQ . Se MQIPT agisce come un proxy SSL/TLS, quando tutti i dati e i protocolli IBM MQ sono stati codificati, MQIPT può garantire solo l'handshake SSL/TLS iniziale. In questa situazione, utilizzare Java security manager.
- MQIPT consente alle uscite canale di eseguire i propri protocolli di sicurezza end - to - end.
- È possibile limitare il numero totale di connessioni in entrata impostando la proprietà `MaxConnectionThreads` . Ciò consente di proteggere un gestore code interno vulnerabile dagli attacchi DoS (denial of service).

File di configurazione

È necessario proteggere il file di configurazione MQIPT , `mqipt.conf`, dalla lettura da parte di utenti non autorizzati perché potrebbe contenere informazioni sensibili, come la password **AccessPW** che controlla l'accesso amministrativo remoto a MQIPT. Proteggi tutte le password specificate nel file di configurazione seguendo la procedura in "Crittografia delle password memorizzate in MQIPT" a pagina 1008. Inoltre, verificare che `mqipt.conf` sia protetto da modifiche non autorizzate. Impostare le autorizzazioni del file del sistema operativo per `mqipt.conf` in modo che solo l'account utente che esegue MQIPT possa leggere o aggiornare il file.

Porta comandi

La porta comandi MQIPT accetta comandi di controllo emessi dallo script **mqiptAdmin** o da IPT Administration Client. Se la porta comandi MQIPT è abilitata, è necessario impedire l'accesso non autorizzato ad essa. In particolare, se la proprietà **RemoteShutdown** è abilitata, un utente remoto potrebbe chiudere MQIPT.

È necessario utilizzare un firewall per limitare la serie di computer che possono connettersi alla porta comandi MQIPT . È inoltre necessario impostare una password per controllare l'accesso alla porta comandi utilizzando la proprietà **AccessPW** .

Nota: Le connessioni alla porta comandi MQIPT non sono codificate. I dati inviati sulla rete, inclusa la parola d'ordine, potrebbero essere visibili ad altri utenti sulla rete.

È necessario valutare i rischi di consentire la gestione remota di MQIPT prima di abilitare la porta comandi. Disabilitare l'arresto remoto con la proprietà **RemoteShutdown** se la porta comandi è abilitata.

Log di connessione in MQIPT

MQIPT fornisce una funzione di log di connessione che contiene elenchi di tutti i tentativi di connessione riusciti e non riusciti.

È controllato utilizzando le proprietà **ConnectionLog** e **MaxLogFileSize** . Per ulteriori informazioni, consultare MQIPT proprietà globali .

Ogni volta che MQIPT viene avviato, viene creato un nuovo log di connessione. Per l'identificazione, il nomefile include la data / ora corrente, ad esempio:

```
mqiptYYYYMMDDHHmmSS.log
```

dove

YYYY è l'anno
MM è il mese

DD è il giorno
HH sono le ore
mm è il minuto
SS sono i secondi

Quando un log di connessione raggiunge la dimensione massima determinata dalla proprietà **MaxLogFileSize** , viene creato un file di backup, `mqipt001.log`. Vengono conservati un numero massimo di due file di backup (`mqipt001.log` e `mqipt002.log`).

Una voce nel log di connessione rappresenta ogni parte di una richiesta di collegamento. Una richiesta di connessione ricevuta da MQIPT e la nuova connessione risultante che MQIPT effettua all'indirizzo di destinazione viene visualizzata come due voci di log e, successivamente, due ulteriori voci al termine di ogni connessione.

Di seguito è riportato il log di connessione per una richiesta di connessione riuscita:

```
Wed May 15 13:13:51 BST 2013 conn accept 127.0.0.1(3842) 127.0.0.1(5000) OK 5000-0
Wed May 15 13:13:51 BST 2013 conn conn   127.0.0.1(3843) localhost(3500) OK 5000-0
Wed May 15 13:13:52 BST 2013 conn close  127.0.0.1(3842) 127.0.0.1(5000) OK 5000-0
Wed May 15 13:13:52 BST 2013 conn close  127.0.0.1(3843) localhost(3500) OK 5000-0
```

Di seguito è riportato un log di connessione per una richiesta di collegamento non riuscita:

```
Wed May 15 14:56:40 BST 2013 conn accept 127.0.0.1(4138) 127.0.0.1(7000) OK    7000-0
Wed May 15 14:56:40 BST 2013 conn close  127.0.0.1(4138) 127.0.0.1(7000) ERROR 7000-0
 Unrecognized SSL handshake request '54'
```

Configurazione di IBM MQ Internet Pass-Thru utilizzando i container

Puoi eseguire IBM MQ Internet Pass-Thru (MQIPT) in un contenitore. L'immagine di base utilizzata dall'immagine contenitore deve utilizzare un sistema operativo Linux supportato.

Procedura

- Nel repository GitHub del contenitore mq è disponibile un'immagine MQIPT Docker di esempio. Per creare ed eseguire il contenitore, segui le istruzioni in IBM MQ Internet Pass-Thru su Docker.

Operazioni successive

È possibile visualizzare i contenitori in esecuzione utilizzando il comando **docker ps** . Per visualizzare l'output della console di MQIPT in esecuzione su un contenitore Docker , utilizza il comando **docker logs ${CONTAINER_ID}** .

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 tale documento non concede alcuna licenza a tali brevetti. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

Director of Commercial Relations
IBM Corporation
Schoenaicher Str. 220
D-7030 Boeblingen
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.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate su base periodica; tali modifiche vengono incorporate nelle nuove edizioni della pubblicazione. IBM si riserva il diritto di apportare miglioramenti o modifiche al prodotto/i e/o al programma/i descritti nella pubblicazione in qualsiasi momento e senza preavviso.

Qualsiasi riferimento a siti Web non IBM contenuto nelle presenti informazioni è fornito per consultazione e non vuole in alcun modo promuovere i suddetti siti Web. I materiali presenti in tali siti Web non sono parte dei materiali per questo prodotto IBM e l'utilizzo di tali siti Web è a proprio rischio.

Tutti i commenti e i suggerimenti inviati potranno essere utilizzati liberamente da IBM e diventeranno esclusiva della stessa.

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a:

IBM Corporation
Coordinatore interoperabilità software, Dipartimento 49XA
Autostrada 3605 52 N

Rochester, MN 55901
U.S.A.

Queste informazioni possono essere rese disponibili secondo condizioni contrattuali appropriate, compreso, in alcuni casi, il pagamento di un addebito.

Il programma su licenza descritto in queste informazioni e tutto il materiale su licenza disponibile per esso sono forniti da IBM in base ai termini dell' IBM Customer Agreement, IBM International Program License Agreement o qualsiasi altro accordo equivalente tra le parti.

Tutti i dati relativi alle prestazioni contenuti in questo documento sono stati determinati in un ambiente controllato. Pertanto, i risultati ottenuti in altri ambienti operativi possono variare in modo significativo. Alcune misurazioni potrebbero essere state fatte su sistemi a livello di sviluppo e non vi è alcuna garanzia che queste misurazioni saranno le stesse sui sistemi generalmente disponibili. Inoltre, alcune misurazioni potrebbero essere state stimate mediante estrapolazione. I risultati quindi possono variare. Gli utenti di questo documento dovrebbero verificare i dati applicabili per il loro ambiente specifico.

Le informazioni relative a prodotti non IBM provengono dai fornitori di tali prodotti, dagli annunci pubblicati o da altre fonti pubblicamente disponibili. IBM non ha verificato tali prodotti e, pertanto, non può garantirne l'accuratezza delle prestazioni. Eventuali commenti relativi alle prestazioni dei prodotti non IBM devono essere indirizzati ai fornitori di tali prodotti.

Tutte le dichiarazioni riguardanti la direzione o l'intento futuro di IBM sono soggette a modifica o ritiro senza preavviso e rappresentano solo scopi e obiettivi.

Questa pubblicazione contiene esempi di dati e prospetti utilizzati quotidianamente nelle operazioni aziendali, Per 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 testati approfonditamente tenendo conto di tutte le condizioni possibili. IBM, quindi, non può garantire o sottintendere l'affidabilità, l'utilità o il funzionamento di questi programmi.

Se si sta visualizzando queste informazioni in formato elettronico, le fotografie e le illustrazioni a colori potrebbero non apparire.

Informazioni sull'interfaccia di programmazione

Le informazioni sull'interfaccia di programmazione, se fornite, consentono di creare software applicativo da utilizzare con questo programma.

Questo manuale contiene informazioni sulle interfacce di programmazione che consentono al cliente di scrivere programmi per ottenere i servizi di WebSphere MQ.

Queste informazioni, tuttavia, possono contenere diagnosi, modifica e regolazione delle informazioni. La diagnosi, la modifica e la regolazione delle informazioni vengono fornite per consentire il debug del software applicativo.

Importante: Non utilizzare queste informazioni di diagnosi, modifica e ottimizzazione come interfaccia di programmazione poiché sono soggette a modifica.

Marchi

IBM, il logo IBM , ibm.com, sono marchi di IBM Corporation, registrati in molte giurisdizioni nel mondo. Un elenco aggiornato dei marchi IBM è disponibile sul web in "Copyright and trademark

information"www.ibm.com/legal/copytrade.shtml. Altri nomi di prodotti e servizi potrebbero essere marchi di IBM o altre società.

Microsoft e Windows sono marchi di Microsoft Corporation negli Stati Uniti 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 Java sono marchi registrati di Oracle e/o di società affiliate.

Numero parte:

(1P) P/N: