9.4

IBM MQ Scenari

Nota

Prima di utilizzare queste informazioni e il prodotto che supportano, leggere le informazioni in “Informazioni particolari” a pagina 221.

Questa edizione si applica alla versione 9 release 4 di IBM® MQ e a tutte le successive release e modifiche se non diversamente indicato nelle nuove edizioni.

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

© Copyright International Business Machines Corporation 2007, 2025.

Indice

Scenari.....5
Introduzione aIBM MQ.....5
Pianificazione della soluzione.....5
Implementazione della soluzione.....7
Cosa fare successivamente.....18
Scenario point - to - point.....18
Pianificazione della soluzione.....18
Implementazione della soluzione.....20
Protezione della topologia point - to - point.....26
Code di streaming.....29
Configurazione delle code di flusso.....30
Flusso a code remote e alias.....31
Limitazioni della coda di flusso.....32
Transazioni e code di flusso.....33
Flusso verso e da code cluster.....33
Utilizzo delle code di streaming per memorizzare una cronologia di messaggi.....34
Scenari di pubblicazione / sottoscrizione.....35
Scenario: creazione di un cluster di pubblicazione / sottoscrizione.....35
Scenari di gerarchia di pubblicazione / sottoscrizione.....41
Scenari di supporto transazionale.....50
Introduzione delle unità di lavoro.....50
Scenario 1: il gestore code esegue il coordinamento.....51
Scenario 2: Altri software forniscono il coordinamento.....76
Unità di lavoro globali in scadenza.....84
Unit of recovery disposition.....85
Scenari di sicurezza.....86
Security scenario: two queue managers on z/OS.....86
Security scenario: queue sharing group on z/OS.....93
Server-to-server message channel interception example configurations.....98
Connessione di due gestori code utilizzando SSL/TLS.....99
Connessione sicura di un client a un gestore code.....106
Migrazione su Windows.....112
Pianificazione della soluzione.....112
Implementazione della soluzione utilizzando la GUI (graphical user interface).....117
Installazione di una versione più recente di IBM MQ per coesistere con una versione precedente su Windows.....143
Panoramica di più installazioni.....143
Installazione di una versione successiva di IBM MQ affiancata a una versione precedente.....144
Utilizzo del comando **setmqenv** per l'esecuzione con entrambe le versioni di IBM MQ.....145
Creazione di un gestore code.....147
Migrazione di un gestore code a una versione successiva di IBM MQ.....149
Installazione di un fix pack su IBM MQ 9.4.....151
Managed File Transfer scenario.....153
Topologie comuni MFT.....153
Configurazione del server di base.....156
Introduzione aIBM MQ Internet Pass-Thru.....164
Verifica del corretto funzionamento di MQIPT.....166
Creazione di certificati di verifica.....167
Richiedi un certificato firmato CA per MQIPT.....168
Autenticazione di un server TLS.....171
Autenticazione di un client TLS.....173
Autenticazione di client e server TLS.....175

Configurazione del tunneling HTTP....179
Configurazione del controllo accessi....181
Configurazione di un proxy SOCKS....183
Configurazione di un client SOCKS....185
Configurazione del supporto cluster MQIPT....187
Assegnazione dei numeri di porta....190
Richiamo di CRL utilizzando un server LDAP....191
Esecuzione di MQIPT in modalità proxy TLS....194
Esecuzione di MQIPT in modalità proxy TLS con un gestore sicurezza....195
Utilizzo di un'uscita di sicurezza....198
Instradamento delle richieste di connessione client ai server del gestore code IBM MQ utilizzando le uscite di sicurezza....200
Instradamento dinamico delle richieste di connessione client....203
Utilizzo di un'uscita certificato per autenticare un server TLS....206
Scenari di Kafka Connect....208
Topologie comuni di Kafka Connect....209
Supporto esattamente una volta....217
Esecuzione di Kafka Connect su IBM z/OS....218

Informazioni particolari....221
Informazioni sull'interfaccia di programmazione....222
Marchi....222

IBM MQ Scenari

Ogni scenario guida l'utente attraverso una serie significativa di attività e consente di configurare una funzione del prodotto principale. Gli scenari includono collegamenti utili ad altri contenuti per consentire una migliore comprensione dell'area a cui si è interessati.

Gli scenari IBM MQ disponibili sono descritti nei topic secondari riportati di seguito.

Windows Introduzione aIBM MQ

Questo scenario spiega come iniziare a utilizzare IBM MQ su una piattaforma Windows . Utilizzare questo scenario se non si è mai utilizzato IBM MQ e si desidera iniziare rapidamente.

Questo scenario descrive la procedura di base per l'installazione, la configurazione e la verifica di IBM MQ su Windows , se non è già installato sul sistema. È possibile completare i passi dello scenario utilizzando la GUI (graphical user interface) o la CLI (command - line interface).

Pianificazione della soluzione

Scegliere un metodo per installare IBM MQ su Windows. Utilizzare l'interfaccia utente grafica e le procedure guidate che guidano l'utente attraverso il processo di installazione e configurazione oppure utilizzare la riga comandi per eseguire un'installazione non presidiata.

Panoramica: la topologia logica fornita

La topologia logica fornita dopo il completamento dello scenario.

L'istanza del server IBM MQ installata consente la creazione di oggetti IBM MQ : code e gestori code. È possibile utilizzare IBM MQ Explorer per immettere e richiamare i messaggi dalla coda locale tramite il gestore code. Una volta completato questo scenario, la topologia fornita sarà simile alla Figura 1.

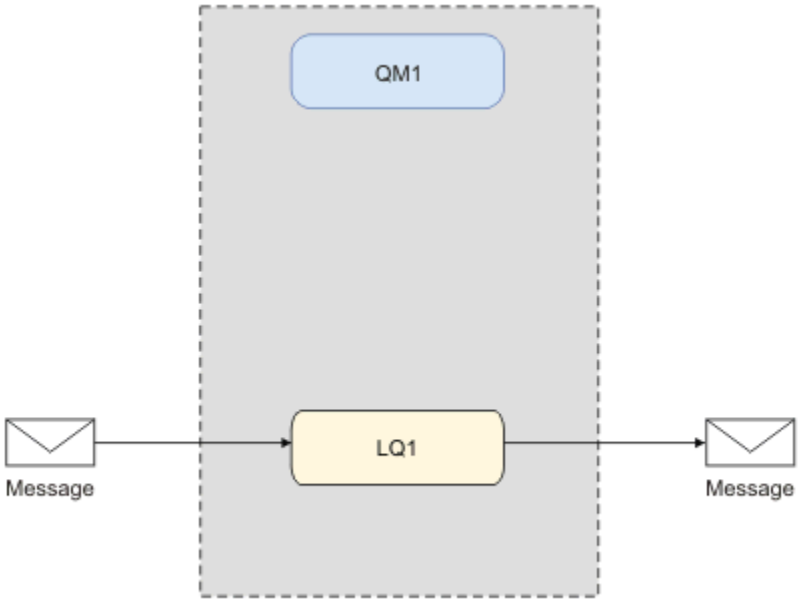


Figura 1. Inserire il messaggio in LQ1, richiamare il messaggio da LQ1.

Concetti di base e termini chiave

Descrizione dei concetti di base e dei termini chiave che è necessario conoscere prima di utilizzare lo scenario Introduzione a IBM MQ.

© Copyright IBM Corp. 2007, 2025

Concetti di base

IBM MQ consente alle applicazioni di leggere e scrivere messaggi in una coda. L'applicazione di lettura e quella di scrittura dei messaggi sono indipendenti. Non è richiesta l'esecuzione simultanea delle due applicazioni. Se non è disponibile alcuna applicazione per la lettura del messaggio, esso viene inserito nella coda IBM MQ finché l'applicazione non lo legge.

In questo scenario è possibile scegliere di installare e configurare IBM MQ in uno dei seguenti modi:

“Installazione e configurazione mediante la GUI (graphical user interface)” a pagina 7

Durante l'installazione utilizzando un'interfaccia utente grafica, è possibile essere guidati tramite diverse schermate o procedure guidate per ricevere aiuto nell'applicazione delle opzioni e delle configurazioni più importanti:

Launchpad
Controllare i requisiti software, specificare le informazioni di rete e avviare la procedura guidata di installazione di IBM MQ.

Procedura guidata di installazione di IBM MQ
Installare il software e avviare la Prepare IBM MQ Wizard.

Prepare IBM MQ Wizard
Avviare il servizio IBM MQ e IBM MQ Explorer.

IBM MQ Explorer
Gestire le code e i gestori coda.

“Installazione e configurazione mediante la CLI (command line interface)” a pagina 11

L'installazione dell'interfaccia riga di comandi può essere non presidiata o interattiva. L'installazione non presidiata è completamente accessibile e viene trattata in questo scenario. Durante l'installazione utilizzando la riga comandi, si viene guidati tramite diversi passi per ricevere aiuto nell'applicazione delle opzioni e delle configurazioni più importanti:

- InstallaIBM MQ
- Creare e configurare gli oggetti IBM MQ; i gestori code e le code.
- Verificare l'installazione utilizzando `amqsput` per inserire e `amqsget` per ottenere un messaggio da una coda.

Così come utilizzando IBM MQ Explorer e la riga comandi per creare gli oggetti IBM MQ, è possibile fare lo stesso utilizzando l'interfaccia programmabile. Questa non è inclusa nello scenario corrente.

Termini chiave

Il seguente è un elenco dei termini chiave sulla coda dei messaggi.
Termini chiave sulla coda dei messaggi.

Termine	Descrizione
Gestori code	Il gestore code è responsabile della gestione delle code di sua proprietà e della memorizzazione di tutti i messaggi ricevuti nelle code appropriate.
Messaggi	Un messaggio è una stringa di byte significativa per l'applicazione che la utilizza. I messaggi vengono utilizzati per trasferire informazioni da un programma applicativo a un altro. Le applicazioni possono essere in esecuzione in un solo computer o su computer diversi.
Code locali	Una coda locale è una struttura di dati utilizzata per memorizzare i messaggi. La coda può essere di tipo normale o di trasmissione. Una coda normale contiene messaggi che devono essere letti da un'applicazione che sta leggendo il messaggio direttamente dal gestore code. Una coda di trasmissione memorizza i messaggi che sono in transito verso un altro gestore code.

Implementazione della soluzione

Implementa la soluzione allo scenario. Installare IBM MQ su Windows utilizzando il Launchpad di installazione, quindi verificare l'installazione utilizzando IBM MQ Explorer.

Installazione e configurazione mediante la GUI (graphical user interface)

Installare IBM MQ su Windows utilizzando il launchpad di installazione e verificare l'installazione utilizzando IBM MQ Explorer. Dopo aver verificato l'installazione, creare un gestore code e una coda, quindi provare a inserire un messaggio nella coda e a richiamare un messaggio dalla coda.

Installazione mediante il launchpad

Installare IBM MQ su Windows utilizzando il launchpad di installazione.

Prima di iniziare

Prima di avviare questa attività, completare i seguenti controlli:

- Quando si esegue l'installazione, è necessario disporre dell'autorità di amministratore locale. Definire questa autorizzazione mediante le funzioni Windows .
- Assicurarsi che il nome della macchina non contenga spazi.
- Assicurarsi di disporre di spazio su disco sufficiente per installare completamente IBM MQ for Windows. Per ulteriori informazioni, vedi Requisiti di spazio su disco su Multiplatforms.
- Determinare se è necessario definire gli ID utente del dominio Windows per gli utenti IBM MQ .

Prima di installare IBM MQ, verificare che il sistema soddisfi i requisiti hardware e software. Per ulteriori informazioni sui requisiti hardware e software su tutte le piattaforme supportate, consultare Requisiti di sistema per 'IBM MQ.

Informazioni su questa attività

Il launchpad e le successive procedure guidate guidano l'utente attraverso il processo di installazione e consentono di esaminare i requisiti software e le impostazioni IBM MQ .

Questa attività presuppone che si stia installando IBM MQ per la prima volta sulla macchina e che si utilizzeranno le posizioni predefinite. Per default, l'ubicazione dei file di programma IBM MQ è `C:\Program Files\IBM\MQ`e l'ubicazione dei file di dati e di log è `C:\Programmi\ IBM \ MQ`.

Nota: Se si sta installando IBM MQ 9.0e si dispone di eventuali installazioni precedenti di IBM MQ sulla macchina, l'ubicazione del programma e dei file di dati sarà diversa da quella predefinita. Per ulteriori informazioni, consultare Program and data directory locations. Se questo scenario è stato già completato in precedenza e si desidera ripeterlo con una singola nuova installazione utilizzando le ubicazioni predefinite, rimuovere l'installazione precedente prima di avviare nuovamente lo scenario. Per disinstallare un'istanza esistente di IBM MQ dalla macchina, consultare “disinstallazioneIBM MQ” a pagina 17.

I programmi di installazione contengono collegamenti a ulteriori informazioni, se richieste durante il processo di installazione.

Procedura

1. Avviare il Launchpad, rivedere e, se necessario, modificare i requisiti software e la configurazione di rete.
   a) Passare alla directory del software IBM MQ e fare doppio clic su `Setup.exe` per avviare il Launchpad.
   b) Selezionare la scheda **Requisiti software** per visualizzare le impostazioni **Requisiti software** .
   c) Verificare che i requisiti software siano stati soddisfatti e che la voce per il requisito visualizzi un segno di spunta verde con le parole 0K. Apportare le correzioni indicate.

Nota:

Per i dettagli di un requisito, fare clic sulla casella di spunta per espandere una scheda di informazioni.

d) Selezionare la scheda **Configurazione di rete** per visualizzare le impostazioni **Configurazione di rete** .

e) Selezionare **No**.

Nota: Questo scenario presuppone che non sia necessario configurare un ID utente di dominio per IBM MQ. Per ulteriori informazioni relative alla configurazione degli utenti del dominio IBM MQ for Windows , fare clic su **Ulteriori informazioni**.

f) Nella scheda **IBM MQ Installazione** del Launchpad, selezionare la lingua di installazione e fare clic su **Avvia IBM MQ Installer** per avviare la procedura guidata di installazione di IBM MQ .

È stata completata l'impostazione di IBM MQ soddisfacendo o specificando i propri requisiti di installazione e si è avviata la procedura guidata di installazione di IBM MQ .

2. Utilizzare la procedura guidata di installazione IBM MQ per installare il software e avviare Prepare IBM MQ Wizard.

a) Nella procedura guidata di installazione di IBM MQ , leggere l'accordo di licenza e fare clic sulla casella di spunta **Accetto i termini nell'accordo di licenza** , quindi fare clic su **Avanti**.

b) Fare clic su **Tipico**, quindi fare clic su **Avanti**.

c) Nella pagina **Pronto per l'installazione IBM MQ** , esaminare le informazioni di installazione e fare clic su **Installa**.

Nota: Si notano i seguenti dettagli:

- Nome installazione
- Cartella di livello superiore per Program Files
- Cartella di livello superiore per File di dati

Sono installate le seguenti funzionalità:

- IBM MQ Server
- IBM MQ: un'interfaccia grafica per la gestione e il monitoraggio delle risorse di IBM MQ
- Java e .NET Messaging e servizi Web
- IBM MQ Toolkit di sviluppo

Il processo di installazione inizia. In base al sistema, il processo di installazione può richiedere diversi minuti.

Alla fine del processo di installazione, la finestra IBM MQ Setup visualizza il messaggio `Installation Wizard Completed Successfully` .

d) Fare clic su **Fine**.

IBM MQ è stato installato correttamente Prepare IBM MQ Wizard viene avviato automaticamente, visualizzando la pagina **Prepare IBM MQ Wizard** .

3. Utilizza Prepare IBM MQ Wizard per avviare il servizio IBM MQ .

a) Nella pagina Benvenuti in Prepare IBM MQ Wizard , selezionare **Avanti**.

Prepare IBM MQ Wizard visualizza il messaggio `Status: Checking IBM MQ Configuration` e una barra di avanzamento. Una volta completato il processo, viene visualizzata la pagina Configurazione di rete IBM MQ .

b) Nella pagina Configurazione di rete IBM MQ di Prepare IBM MQ Wizard, selezionare **No**.

c) Fare clic su **Avanti**.

Prepare IBM MQ Wizard visualizza un messaggio `Status: starting the IBM MQ Service` e una barra di avanzamento. Una volta completato il processo, la procedura guidata visualizza la pagina Completamento di Prepare IBM MQ Wizard .

d) Selezionare **Avvia IBM MQ Explorer** e scegliere se visualizzare le note sulla release, quindi fare clic sul pulsante **Fine** .

IBM MQ Explorer viene avviato.

È stato installato IBM MQ. È stato avviato anche IBM MQ Explorer.

Risultati

IBM MQ è installato e verificato e si è pronti a configurare oggetti come gestori code e code.

Operazioni successive

Seguire le istruzioni riportate in "Creazione di un gestore code denominato QM1" a pagina 9.

Concetti correlati

Requisiti di spazio su disco

Requisiti hardware e software sui sistemi di Windows

Introduzione a IBM MQ

Attività correlate

Installazione di un server IBM MQ in Windows

Configurazione di un server IBM MQ

Creazione di un gestore code denominato QM1

Creare un gestore code, denominato QM1 utilizzando IBM MQ Explorer. I gestori code sono i principali componenti di una rete di messaggistica IBM MQ .

Prima di iniziare

È necessario che IBM MQ sia installato. In caso contrario, consultare "Installazione mediante il launchpad" a pagina 7 per informazioni su come eseguire tale operazione.

Informazioni su questa attività

In questo esempio, tutti i nomi vengono immessi in maiuscolo e, poiché i nomi IBM MQ sono sensibili al maiuscolo / minuscolo, è necessario immettere anche tutti i nomi in maiuscolo.

Per creare e avviare un gestore code utilizzando IBM MQ Explorer, completare la seguente procedura.

Procedura

1. Avviare IBM MQ Explorer come amministratore.
2. Nella vista **Navigator** , fare clic con il tasto destro del mouse sulla cartella **Gestori code** , quindi selezionare **Nuovo> Gestore code**. Viene avviata la procedura guidata **Crea gestore code** .
3. Nel campo **Nome gestore code** , immettere QM1.
4. Selezionare la casella di controllo `Make this the default queue manager.`
5. Nel campo **Dead - letter queue** immettere SYSTEM.DEAD.LETTER.QUEUE.

   Questo è il nome della coda di messaggi non instradabili che viene creata automaticamente quando si crea il gestore code.
6. Lasciare vuoti gli altri campi e fare clic su **Fine**oppure, se il pulsante è disabilitato, fare clic su **Avanti**.

   Il pulsante **Fine** è disabilitato se il numero di porta è in conflitto con un gestore code esistente, ad esempio il gestore code creato come parte della configurazione predefinita. È necessario continuare con la procedura guidata per modificare il numero di porta predefinito.
7. Se si è fatto clic su **Avanti**, continuare ad accettare i valori predefiniti e fare clic su **Avanti** su ogni pagina fino a quando non si arriva alla pagina finale della procedura guidata, quando il pulsante **Fine** diventa disponibile. Modificare il numero di porta specificato, ad esempio in 1415e fare clic su **Fine**.

   IBM MQ visualizza una finestra di dialogo **Creazione gestore code** mentre il gestore code viene creato e avviato.

Operazioni successive

Per creare una coda, consultare “Creazione di una coda denominata LQ1” a pagina 10.

Attività correlate

Creazione e gestione di gestori code su più piattaforme

Creazione di una coda denominata LQ1

Creare una coda utilizzando IBM MQ Explorer. Le code sono strutture di dati utilizzate per memorizzare i messaggi e sono oggetti del gestore code IBM MQ .

Informazioni su questa attività

In questa attività è possibile creare oggetti IBM MQ utilizzando IBM MQ Explorer.

Per creare e avviare una coda utilizzando IBM MQ Explorer, completare la seguente procedura.

Procedura

1. Nella vista **Navigator**, espandere la cartella **Gestori code**.
2. Espandere gestore code **QM1**.
3. Fare clic con il pulsante destro del mouse sulla cartella **Code** , quindi selezionare **Nuovo> Coda locale ...** Viene avviata la procedura guidata **Nuova coda locale** .
4. Nel campo **Nome** , immettere LQ1.
5. Fare clic su **Fine**.

   La nuova coda LQ1, viene visualizzata nella vista **Contenuto** . Se la coda non viene visualizzata nella vista **Contenuto** , fare clic sul pulsante **Aggiorna** , nella parte superiore della vista **Contenuto** .

Operazioni successive

Si è pronti a inserire un messaggio nella coda. Per inserire un messaggio in una coda, consultare “Inserimento di un messaggio nella coda LQ1” a pagina 10.

Inserimento di un messaggio nella coda LQ1

Inserire un messaggio nella coda LQ1 utilizzando IBM MQ Explorer.

Informazioni su questa attività

Questa attività presuppone che sia stato creato un gestore code denominato QM1 come descritto in “Creazione di un gestore code denominato QM1” a pagina 14 e una coda denominata LQ1 come descritto in “Creazione di una coda denominata LQ1” a pagina 10.

Per inserire un messaggio nella coda utilizzando IBM MQ Explorer, completare la seguente procedura.

Procedura

1. Nella vista **Navigator**, espandere la cartella **Gestori code**.
2. Espandere il gestore code QM1, creato.
3. Fare clic sulla cartella **Code**. Le code del gestore code verranno visualizzate nella vista Contenuto.
4. Nella vista Contenuto, fare clic con il tasto destro del mouse sulla coda locale LQ1, quindi selezionare **Inserisci messaggio di prova**.

   Viene aperta la finestra **Inserisci messaggio di prova**.
5. Nel campo **Dati messaggio** , immettere del testo, ad esempio `Hello World`, quindi fare clic su **Inserisci messaggio**.

   Il campo **Dati del messaggio** verrà cancellato e il messaggio verrà inserito sulla coda.
6. Fare clic su **Chiudi**.

Nella vista Contenuto, notare che il valore LQ1 **Profondità coda corrente** è ora 1. Se la colonna **Profondità coda corrente** non è visibile, potrebbe essere necessario scorrere verso destra la vista **Contenuto**.

Operazioni successive

Per ottenere un messaggio dalla coda, vedere “Richiamo di un messaggio dalla coda LQ1” a pagina 11.

Richiamo di un messaggio dalla coda LQ1

Ottenere un messaggio dalla coda LQ1 utilizzando IBM MQ Explorer.

Informazioni su questa attività

Questa attività presuppone che sia stato già inserito un messaggio QM1 come descritto in “Inserimento di un messaggio nella coda LQ1” a pagina 10.

Per ottenere un messaggio da una coda utilizzando IBM MQ Explorer, completare la seguente procedura.

Procedura

1. Nella vista **Navigator** , espandere la cartella **Gestori code** , quindi espandere QM1.
2. Fare clic sulla cartella **Code**.
3. Nella visualizzazione **Contenuto** , fare clic con il tasto destro del mouse sulla coda locale LQ1, quindi selezionare **Sfoglia messaggi ...**. Viene aperto il **Browser messaggi** per mostrare l'elenco dei messaggi attualmente presenti su QM1.
4. Fare doppio clic sull'ultimo messaggio per aprire la finestra delle proprietà.

   Nella pagina **Dati** della finestra delle proprietà, nel campo **Dati del messaggio** è riportato il contenuto del messaggio in formato leggibile.

Operazioni successive

Seguire le istruzioni negli scenari successivi per esplorare ulteriormente le funzionalità di IBM MQ .

Per informazioni sulla scrittura di applicazioni di accodamento, sulla connessione e sulla disconnessione da un gestore code, sulla pubblicazione / sottoscrizione e sull'apertura e la chiusura di oggetti, consultare Scrittura di un'applicazione procedurale per l'accodamento.

Installazione e configurazione mediante la CLI (command line interface)

Installa IBM MQ su Windows utilizzando la riga di comando per eseguire un'installazione non presidiata e configurare la variabile di ambiente. Dopo aver verificato l'installazione, creare un gestore code e una coda, quindi provare a inserire un messaggio nella coda e a richiamare un messaggio dalla coda.

Installazione mediante un'installazione non presidiata

Installare IBM MQ su Windows utilizzando la riga comandi per eseguire un'installazione non presidiata e confermare che l'ambiente per l'installazione è impostato correttamente.

Prima di iniziare

Prima di avviare questa attività, completare i seguenti controlli:

- Quando si esegue l'installazione, è necessario disporre dell'autorità di amministratore locale. Definire questa autorizzazione mediante le funzioni Windows .
- Assicurarsi che il nome della macchina non contenga spazi.
- Assicurarsi di disporre di spazio su disco sufficiente. Per ulteriori informazioni, vedi Requisiti di spazio su disco su Multiplatforms.
- Determinare se è necessario definire gli ID utente del dominio Windows per gli utenti IBM MQ .

Prima di installare IBM MQ, verificare che il sistema soddisfi i requisiti hardware e software. Per i dettagli più recenti sui requisiti hardware e software su tutte le piattaforme supportate, consultare Requisiti di sistema per 'IBM MQ.

Informazioni su questa attività

Questo scenario presuppone che si stia installando IBM MQ per la prima volta sulla macchina e che si stiano utilizzando le ubicazioni predefinite. Per default, l'ubicazione dei file di programma IBM MQ 9.0 è `C:\Program Files\IBM\MQ`e l'ubicazione dei file di dati e di log è `C:\Programmi\ IBM \ MQ`.

Nota: Se si dispone di precedenti installazioni di IBM MQ sulla macchina, le ubicazioni predefinite del programma e dei file di dati potrebbero cambiare. Per ulteriori informazioni, consultare Program and data directory locations. Se questo scenario è stato già completato in precedenza e si desidera ripeterlo con una singola nuova installazione utilizzando le ubicazioni predefinite, rimuovere l'installazione precedente prima di avviare nuovamente lo scenario. Per disinstallare un'istanza esistente di IBM MQ dalla macchina, consultare “disinstallazioneIBM MQ” a pagina 17.

IBM MQ su Windows utilizza la tecnologia MSI per installare il software. Per ulteriori informazioni sull'installazione mediante la tecnologia MSI, consultare Installazione avanzata mediante msiexec.

Per installare IBM MQ utilizzando la riga comandi, è necessario specificare i seguenti parametri:

- `/i "`*`MQ_INSTALLATION_MEDIA`*`\MSI\IBM MQ.msi"` dove *MQ_INSTALLATION_MEDIA* è l'ubicazione del file `IBM MQ.msi` . Questo argomento specifica l'ubicazione del file .msi.
- `/l*v `*`USER_LOGFILE_LOCATION`*`\install.log` dove *USER_LOGFILE_LOCATION* è il punto in cui si desidera scrivere i log di installazione.

  Nota: La cartella in cui si desidera creare `install.log` deve esistere prima di eseguire il comando.
- `/q[n|b|r|f]` /q deve essere associato a uno tra n, b, `r`o `f`. L'esecuzione del comando **msiexec** da un prompt dei comandi apre il file della guida, che mostra l'uso corretto.
- USEINI="*RESPONSE_FILE*" dove *RESPONSE_FILE* è il nome e l'ubicazione del file di risposte che deve essere utilizzato dall'installazione non presidiata. Questo scenario utilizza il file `Response.ini` di esempio, incluso nei supporti di installazione IBM MQ .
- TRANSFORMS="*TRANSFORM_FILE*" dove *TRANSFORM_FILE* è il nome del file di trasformazione da applicare all'installazione. Questo scenario utilizza la trasformazione Inglese americano, `1033.mst`.
- `AGREETOLICENSE="YES"` questo parametro deve essere incluso oppure l'installazione non può essere completata.
- `ADDLOCAL="Server"` questo parametro elenca i componenti da installare.

Procedura

1. Utilizzare la riga comandi per eseguire un'installazione non presidiata.
   a) Per richiamare l'installazione non presidiata da un prompt dei comandi elevato, fare clic sul **pulsante Start** sulla **barra delle applicazioni di Windows** e immettere cmd nel campo **programmi di ricerca e file** . Fare clic con il pulsante destro del mouse sul programma **cmd.exe** e selezionare **Esegui come amministratore**.
   b) Nel prompt dei comandi di Windows , immettere il seguente comando:

      Nota: Il comando viene qui presentato su più righe, ma deve essere immesso su una riga.

      ```
      msiexec /i "MQ_INSTALLATION_MEDIA\MSI\IBM MQ.msi"
      /l*v c:\wmqinslogs\install.log
      /q USEINI="MQ_INSTALLATION_MEDIA\Response.ini"
      TRANSFORMS="1033.mst"
      AGREETOLICENSE="yes"
      ADDLOCAL="Server"
      ```

      Dove *MQ_INSTALLATION_MEDIA* è il percorso del supporto di installazione di IBM MQ .

Nota: La cartella in cui si desidera creare `install.log` deve esistere prima di eseguire il comando.

Dopo aver immesso il comando, la riga comandi restituirà il prompt.

c) Per visualizzare l'avanzamento delle installazioni, aprire il file di log specificato. Se l'installazione è stata completata correttamente, viene visualizzato il messaggio `Product: IBM MQ (Installation1) -- Installation operation completed successfully.` due paragrafi in alto dalla fine del file di log.

d) Una volta completata l'installazione, il servizio viene avviato e l'icona IBM MQ viene visualizzata nella barra delle applicazioni.

Hai installato IBM MQe hai avviato il servizio IBM MQ .

2. Impostare le variabili di ambiente per l'installazione utilizzando il comando **setmqenv** .

a) Immettere il comando seguente nella riga comandi:

```
"MQ_INSTALLATION_PATH/bin/setmqenv" -s
```

dove *MQ_INSTALLATION_PATH* fa riferimento all'ubicazione in cui è installato IBM MQ . Assicurarsi di racchiudere il percorso a **setmqenv** nella cartella `bin` , tra virgolette, per impedire che la richiesta restituisca un errore.

Nota: Se è stata utilizzata l'ubicazione predefinita, il percorso dell'installazione sarà `C:\Program Files\IBM\MQ`.

b) Verificare che l'ambiente sia impostato correttamente immettendo il seguente comando:

```
dspmqver
```

Se il comando viene completato correttamente e vengono restituiti il numero di versione e il nome di installazione previsti, l'ambiente viene impostato correttamente. Il messaggio deve includere la riga:

```
Version: n.n.n.n
```

dove *n.n.n.n* è il numero di versione e, se non è stato specificato un nome di installazione non predefinito, la riga:

```
InstName: Installation1
```

IBM MQ è stato installato correttamente utilizzando un'installazione non presidiata.

Risultati

L'utente ha eseguito un'installazione non presidiata di IBM MQ e ha confermato che l'ambiente è impostato correttamente.

Operazioni successive

- È possibile eseguire Prepare IBM MQ Wizard.
- Seguire le istruzioni in “Creazione di un gestore code denominato QM1” a pagina 14.

Se si verificano dei problemi durante l'installazione, controllare il log di installazione, nel percorso specificato nel comando **msiexec** , in questo scenario il percorso del file di log è: `c:\wmqinslogs\install.log`. Eseguire qualsiasi azione specificata nel log ed eseguire di nuovo l'installazione. Puoi anche controllare i parametri che hai passato con il comando, mascherando che stai includendo tutti i parametri richiesti.

Attività correlate

Installazione del server utilizzando msiexec

Utilizzo delle trasformazioni con msiexec

Installazione di IBM MQ - panoramica

Creazione di un gestore code denominato QM1

Creare un gestore code denominato QM1 utilizzando la CLI (command - line interface). I gestori code sono i principali componenti di una rete di messaggistica IBM MQ .

Prima di iniziare

È necessario che IBM MQ sia installato. In caso contrario, consultare “Installazione mediante un'installazione non presidiata” a pagina 11 per informazioni su come eseguire tale operazione.

Informazioni su questa attività

In questo esempio, tutti i nomi vengono immessi in maiuscolo e, poiché i nomi IBM MQ sono sensibili al maiuscolo / minuscolo, è necessario immettere anche tutti i nomi in maiuscolo.

Procedura

1. Aprire un prompt dei comandi come amministratore.
2. Creare un gestore code denominato QM1 immettendo il seguente comando:

   ```
   crtmqm QM1
   ```

   Quando il sistema crea il gestore code, viene visualizzato il seguente output:

   ```
   C:\>crtmqm QM1
   IBM MQ queue manager created.
   Creating or replacing default objects for QM1.
   Default objects statistics : 61 created. 0 replaced. 0 failed.
   Completing setup.
   Setup completed.
   ```

   Il gestore code viene creato e arrestato. È necessario avviare il gestore code prima di gestirlo e prima di poter leggere e scrivere i messaggi dalle relative code.
3. Avviare il gestore code mediante il comando:

   ```
   strmqm QM1
   ```

   Quando il gestore code viene avviato correttamente, viene visualizzato il seguente output:

   ```
   C:\>strmqm QM1
   IBM MQ queue manager 'QM1' starting.
   5 log records accessed on queue manager 'QM1' during the log replay phase.
   Log replay for queue manager 'QM1' complete.
   Transaction manager state recovered for queue manager 'QM1'.
   IBM MQ queue manager 'QM1' started.
   ```

   Il gestore code è avviato.

Operazioni successive

Per creare una coda, consultare “Creazione di una coda denominata LQ1” a pagina 14.

Attività correlate

Creazione e gestione di gestori code su più piattaforme

Creazione di una coda denominata LQ1

Creare una coda utilizzando la CLI (command - line interface). Le code sono strutture di dati utilizzate per memorizzare i messaggi e sono oggetti del gestore code IBM MQ .

Informazioni su questa attività

Esistono tre modi per creare oggetti IBM MQ :

- Riga comandi.
- IBM MQ Explorer.
- Utilizzando un'interfaccia programmabile.

In questa attività è possibile creare oggetti IBM MQ utilizzando la riga comandi.

La CLI (command - line interface) ha un linguaggio di script denominato MQSC (IBM MQ Script Commands). Lo strumento di script, **runmqsc**, viene utilizzato per eseguire lo script su un gestore code. Per creare e avviare una coda utilizzando la CLI (command - line interface), completare la seguente procedura.

Procedura

1. Avviare lo strumento di script immettendo il seguente comando:

   ```
   runmqsc QM1
   ```

   Quando lo strumento di script viene avviato, viene visualizzato il seguente output:

   ```
   C:\>runmqsc QM1
   5724-H72 (C) Copyright IBM Corp. 1994, 2025. ALL RIGHTS RESERVED.
   Starting MQSC for queue manager QM1.
   ```

   Lo strumento è pronto ad accettare i comandi MQSC.
2. Creare una coda locale denominata LQ1 immettendo il seguente comando MQSC:

   ```
   define qlocal(LQ1)
   ```

   Quando la coda viene creata, viene visualizzato il seguente output:

   ```
   define qlocal(LQ1)
   2 : define qlocal(LQ1)
   AMQ8006: IBM MQ queue created.
   ```
3. Arrestare lo strumento di script immettendo il seguente comando MQSC:

   ```
   end
   ```

   Quando lo strumento di script termina, viene visualizzato il seguente output:

   ```
   One MQSC command read.
   No commands have a syntax error.
   All valid MQSC commands were processed.

   C:\>
   ```

Operazioni successive

Si è pronti a inserire un messaggio nella coda. Per inserire un messaggio in una coda, consultare “Inserimento di un messaggio nella coda LQ1” a pagina 15.

Inserimento di un messaggio nella coda LQ1

Inserire un messaggio nella coda LQ1 utilizzando la CLI (command - line interface).

Informazioni su questa attività

IBM MQ viene fornito con un'applicazione di esempio denominata **amqsput**. Questa applicazione inserisce un messaggio in una coda predefinita.

Per inserire un messaggio nella coda utilizzando la CLI (command - line interface), completare la seguente procedura.

Procedura

1. Utilizzare l'applicazione di esempio **amqsput** per inserire un messaggio nella coda LQ1, immettendo il seguente comando:

   ```
   amqsput LQ1 QM1
   ```

   Quando l'applicazione di esempio viene avviata, viene visualizzato il seguente output:

   ```
   C:\>amqsput LQ1 QM1
   Sample AMQSPUT0 start
   target queue is LQ1
   ```

2. Immettere `Hello World` e premere Invio. È stato inserito un messaggio che contiene il testo "Hello World" sulla coda LQ1 gestita dal gestore code denominato QM1.
3. Per terminare **amqsput**, premere **Invio**. Viene visualizzato il seguente output:

   ```
   C:\>amqsput LQ1 QM1
   Sample AMQSPUT0 start
   target queue is LQ1
   Hello World

   Sample AMQSPUT0 end
   ```

Operazioni successive

Per ottenere un messaggio dalla coda, vedere “Richiamo di un messaggio dalla coda LQ1” a pagina 16.

Richiamo di un messaggio dalla coda LQ1

Ottenere un messaggio dalla coda LQ1 utilizzando la CLI (command - line interface).

Informazioni su questa attività

IBM MQ viene fornito con un'applicazione di esempio denominata **amqsget**. Questa applicazione legge i messaggi da una coda.

Per ottenere un messaggio dalla coda utilizzando la CLI (command - line interface), completare la seguente procedura.

Procedura

Utilizzare l'applicazione di esempio **amqsget** per leggere un messaggio sulla coda LQ1, immettendo il seguente comando:

```
amqsget LQ1 QM1
```

Quando l'applicazione di esempio viene avviata, viene visualizzato il seguente output:

```
C:\>amqsget LQ1 QM1
Sample AMQSGET0 start
message <Hello World>
no more messages
Sample AMQSGET0 end
```

L'applicazione **amqsget** termina 30 secondi dopo la lettura del messaggio.

Operazioni successive

Seguire le istruzioni negli scenari successivi per esplorare ulteriormente le funzionalità di IBM MQ .

Per informazioni sulla scrittura di applicazioni di accodamento, sulla connessione e sulla disconnessione da un gestore code, sulla pubblicazione / sottoscrizione e sull'apertura e la chiusura di oggetti, consultare Scrittura di un'applicazione procedurale per l'accodamento.

disinstallazioneIBM MQ

Arrestare e quindi disinstallare IBM MQ, inclusa la rimozione dei gestori code e dei relativi oggetti. Alla fine di questa attività, si è pronti a reinstallare IBM MQ.

Informazioni su questa attività

Questa attività descrive i passaggi per disinstallare IBM MQ su Windows utilizzando l'immagine di installazione scaricata.

Lo scenario Introduzione descrive le opzioni per l'installazione di IBM MQ utilizzando il launchpad o la riga comandi. Sebbene sia possibile avere più di un'installazione di IBM MQ, questo scenario si basa su una nuova installazione su un singolo server. Di conseguenza, se si desidera ripetere lo scenario o provare un metodo di installazione diverso, è necessario prima disinstallare i componenti IBM MQ esistenti, inclusi i gestori code esistenti e i relativi oggetti, in modo da poter iniziare nuovamente con una nuova installazione.

Potrebbe anche essere necessario disinstallarlo in modo da poter eseguire una nuova installazione per alcuni degli altri scenari in questa sezione.

Procedura

1. Arresta il servizio IBM MQ.
   a) Fare clic con il pulsante destro del mouse sull'icona **IBM MQ** nella barra delle applicazioni, quindi selezionare **Arresta IBM MQ** per arrestare il servizio IBM MQ .

      Viene visualizzata una finestra di dialogo con il seguente messaggio:

      ```
      La chiusura dell'installazione di "Installation1" di IBM MQ termina tutti i gestori code in esecuzione e
      I processi IBM MQ per tale installazione, tranne quelli sotto il controllo Microsoft Failover Cluster.
      Si è certi di voler proseguire?
      ```

   b) Fare clic su **Sì** e attendere l'arresto di IBM MQ .

   c) Quando IBM MQ si arresta, fare clic con il tasto destro del mouse sull'icona **IBM MQ** nella barra delle applicazioni, quindi fare clic su **Esci**
2. Iniziare il processo di disinstallazione.

   Scaricare il file compresso che contiene l'immagine di installazione, quindi decomprimerlo in una directory temporanea. Passare a tale directory, quindi fare doppio clic su `setup.exe`.

   Viene visualizzata la finestra IBM MQ **Launchpad di installazione** .
3. Rimuovere IBM MQ.
   a) Fare clic su **IBM MQ Installazione**.

   b) Fare clic su **Avvia IBM MQ Installer** e fare clic su **Avanti** finché non viene visualizzato il IBM MQ **riquadro Manutenzione programma** con un messaggio di benvenuto.

      Se questo pannello non viene visualizzato, IBM MQ for Windows non è attualmente installato.

   c) Fare clic su **Gestisci o aggiorna un'istanza esistente**. Selezionare **Installation1** per rimuoverlo. Fare clic su **Avanti** e nel **pannello Manutenzione programma**, fare clic su **Rimuovi**, quindi su **Avanti**.

      Viene visualizzata la funzione Rimozione del server.

   d) Selezionare **Rimuovi**: per rimuovere i gestori code esistenti e i relativi oggetti.

      Fare clic su **Avanti**.

      Viene visualizzato il riquadro Rimuovi IBM MQ , con un riepilogo dell'installazione da eliminare.

   e) Fare clic su **Rimuovi** per continuare.

      Se viene visualizzato un messaggio che indica che i file bloccati sono stati trovati, verificare che nessun programma IBM MQ sia in esecuzione; consultare Disinstallazione di IBM MQ su sistemi Windows.

Quando IBM MQ viene disinstallato, un messaggio indica il completamento.

f) Fare clic su **Fine**.

IBM MQè stato disinstallato correttamente.

Attività correlate

Disinstallare IBM MQ su sistemi Windows

Cosa fare successivamente

Cosa fare dopo il completamento dello scenario Introduzione a IBM MQ .

ALW Per le esercitazioni che consentono di installare e aggiornare, consultare Una raccolta di esercitazioni per l'installazione e l'aggiornamento di IBM MQ su AIX, Linux® e Windows. Le esercitazioni coprono:

- Preparazione di un host per IBM MQ.
- Download del codice IBM MQ .
- Installazione e disinstallazione del codice IBM MQ e applicazione dei fix pack.
- Aggiornamento da una versione di IBM MQ a un'altra e spostamento di un gestore code da un host a un altro.

Esistono ulteriori argomenti da visualizzare nella documentazione del prodotto IBM MQ . È possibile esaminare le seguenti sezioni:

- AmministrazioneIBM MQ

  IBM MQ fornisce comandi di controllo che è possibile utilizzare. Si utilizzano due di questi comandi in questo scenario: **crtmqm** e **strmqm**. Questa sezione fornisce anche una buona panoramica sull'accodamento dei messaggi.

- Gestione IBM MQ utilizzando i comandi MQSC

  In questo scenario, utilizzare il comando `define qlocal('LQ1')` per definire una coda locale denominata LQ1. Questo comando è un comando MQSC. Gli amministratori di sistema IBM MQ utilizzano questi comandi per gestire i propri gestori code. Questa sezione introduce i comandi e mostra come utilizzarli. I comandi sono descritti in dettaglio, in ordine alfabetico, nella sezione di riferimento Comandi MQSC .

- Configurazione di un cluster di gestori code

  Questa sezione descrive come organizzare, utilizzare e gestire i gestori code in gruppi virtuali noti come cluster. Il clustering garantisce che ogni gestore code all'interno di un cluster sia a conoscenza di tutti gli altri gestori code nello stesso cluster. Il clustering rende inoltre più semplice la gestione di reti di gestori code complesse.

Scenario point - to - point

Connettere due gestori code IBM MQ in una topologia point-to-point per abilitare l'accodamento distribuito.

Informazioni su questa attività

Creare due gestori code e le code e i canali appropriati per creare un'infrastruttura di messaggistica point - to - point unidirezionale. Creare i gestori code su host separati per consentire la comunicazione su una rete. Come estensione dello scenario, aggiungere Transport Layer Security al canale per consentire la comunicazione sicura dei dati.

Pianificazione della soluzione

La messaggistica point - to - point è la forma più semplice di messaggistica in IBM MQ. Nella messaggistica point - to - point, l'applicazione mittente deve conoscere determinate informazioni

sull'applicazione ricevente prima che i messaggi possano essere inviati. L'applicazione mittente richiederà un modo per indirizzare la coda remota. Utilizzare la messaggistica punto a punto per inviare un messaggio a un gestore code remoto con un'applicazione di esempio.

Panoramica: la topologia logica fornita

La topologia logica fornita dopo il completamento dello scenario.

L'infrastruttura point-to-point consente una messaggistica direzionale tra i gestori code su macchine host differenti. Il gestore code uno, sull'host uno invia messaggi al gestore code due, sull'host due. Una volta completato questo scenario, la topologia fornita sarà simile alla Figura 1.

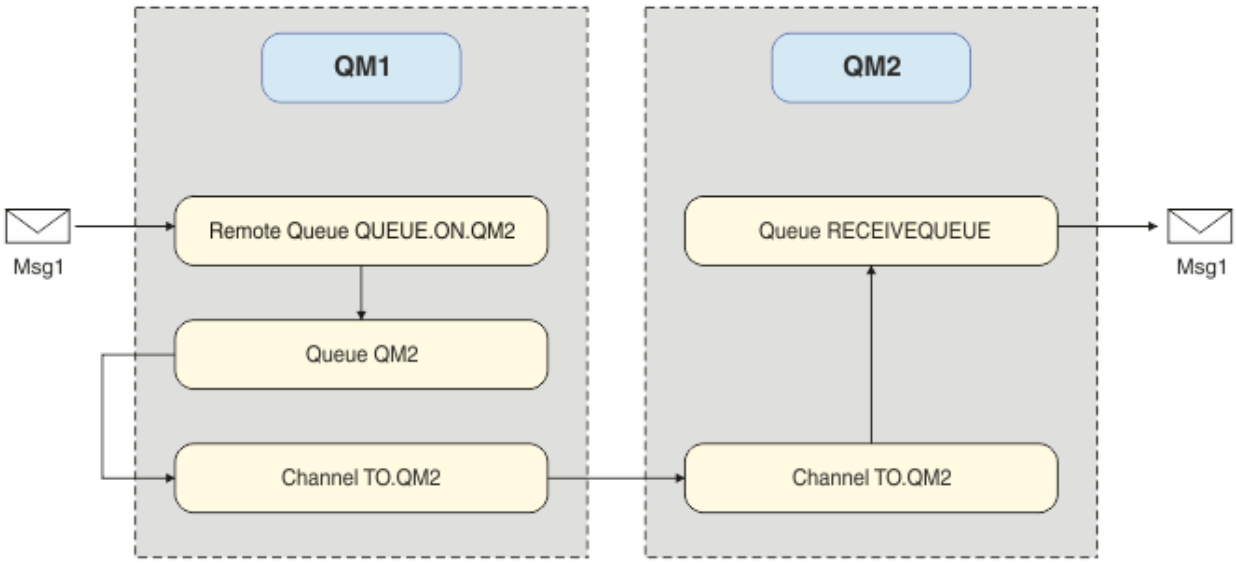


Figura 2. QM1 invia un messaggio a QM2

Concetti di base e termini chiave

Descrizioni dei concetti di base e dei termini chiave che è necessario conoscere per completare lo scenario punto a punto.

Concetti di base

IBM MQ consente alle applicazioni di leggere e scrivere messaggi in una coda. L'applicazione di lettura e quella di scrittura dei messaggi sono indipendenti. Non è richiesta l'esecuzione simultanea delle due applicazioni. Se non è disponibile alcuna applicazione per la lettura del messaggio, esso viene inserito nella coda IBM MQ finché l'applicazione non lo legge.

Termini chiave

Il seguente è un elenco dei termini chiave sulla coda dei messaggi.

Termini chiave sulla coda dei messaggi.

Termine	Descrizione
Gestori code	Il gestore code è responsabile della gestione delle code di sua proprietà e della memorizzazione di tutti i messaggi ricevuti nelle code appropriate.
Messaggi	Un messaggio è una stringa di byte significativa per l'applicazione che la utilizza. I messaggi vengono utilizzati per trasferire informazioni da un programma applicativo a un altro. Le applicazioni possono essere in esecuzione in un solo computer o su computer diversi.
Code locali	Una coda locale è una struttura di dati utilizzata per memorizzare i messaggi. La coda può essere di tipo normale o di trasmissione. Una coda normale contiene messaggi che devono essere letti da un'applicazione che sta leggendo il messaggio direttamente dal gestore code. Una coda di trasmissione memorizza i messaggi che sono in transito verso un altro gestore code.
Code remote	Una coda remota viene utilizzata per indirizzare un messaggio a un altro gestore code.
Canali	I canali vengono utilizzati per inviare e ricevere messaggi tra i gestori code.
Listener	I listener sono processi che accettano le richieste di rete da altri gestori code o applicazioni client e avviano i canali associati.

Implementazione della soluzione

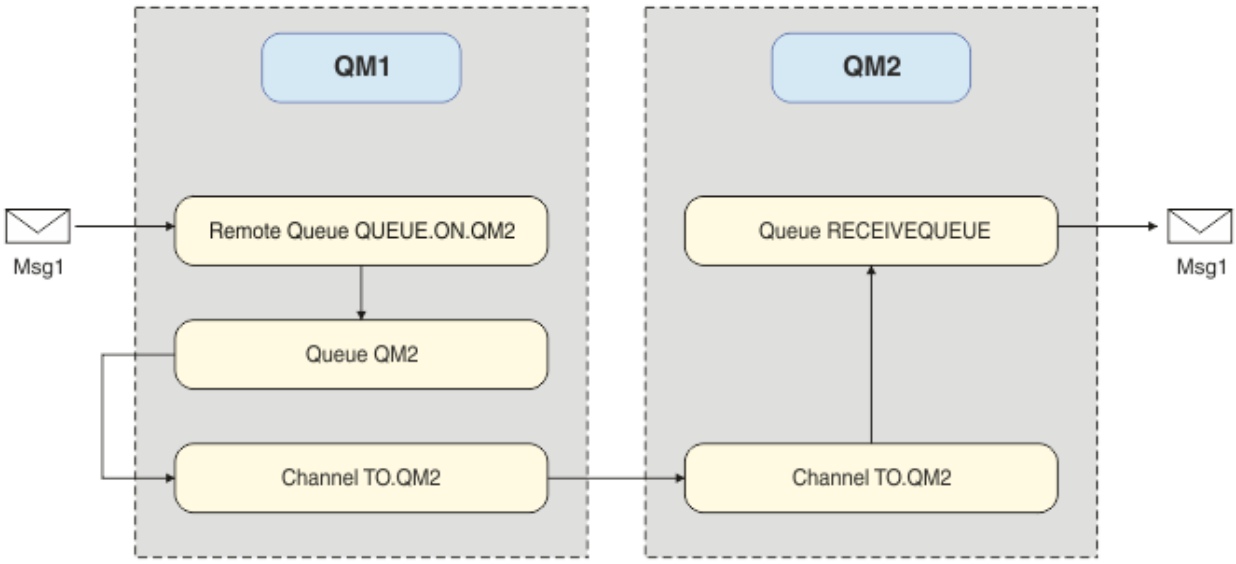
Implementa la soluzione allo scenario. Creare due gestori code IBM MQ su due host separati, il gestore code di origine per inviare messaggi e il gestore code di destinazione per ricevere messaggi.

Prima di iniziare

Il punto di partenza per questo scenario è un'installazione IBM MQ verificata e esistente. Per istruzioni sull'installazione di IBM MQ, attenersi alla procedura descritta in Installazione di un server IBM MQ su Windows.

Informazioni su questa attività

Creare due gestori code utilizzando la CLI, definire i listener, le code e i canali richiesti. La topologia logica fornita mostra le funzioni aggiunte implementando la soluzione.



Creazione del gestore code

Creare un gestore code IBM MQ per inviare messaggi al gestore code di destinazione.

Prima di iniziare

- È necessario che IBM MQ sia installato. Per ulteriori informazioni sull'installazione di IBM MQ, consultare Installazione e disinstallazione.

Informazioni su questa attività

Creare il gestore code IBM MQ utilizzando la CLI (command - line interface).

Procedura

1. Creare un gestore code denominato QM1. Sulla riga comandi, immettere:

   ```
   crtmqm QM1
   ```

   Vengono visualizzati i seguenti messaggi per confermare che il gestore code è stato creato:

   ```
   IBM MQ queue manager created.
   Creating or replacing default objects for QM1.
   Default objects statistics : 61 created. 0 replaced. 0 failed.
   Completing setup.
   Setup completed.
   ```

2. Avviare il gestore code. Sulla riga comandi, immettere:

   ```
   strmqm QM1
   ```

   Vengono visualizzati i seguenti messaggi per confermare che il gestore code è stato avviato:

   ```
   IBM MQ queue manager 'QM1' starting.
   5 log records accessed on queue manager 'QM1' during the log replay phase.
   Log replay for queue manager 'QM1' complete.
   Transaction manager state recovered for queue manager 'QM1'.
   IBM MQ queue manager 'QM1' started.
   ```

Risultati

Il gestore code IBM MQ QM1 viene creato e avviato.

Operazioni successive

Per creare le code da utilizzare con QM1, attenersi alle istruzioni in “Creazione delle code” a pagina 21.

Creazione delle code

Creare code IBM MQ gestite dal gestore code IBM MQ .

Prima di iniziare

È necessario disporre di un gestore code IBM MQ configurato come descritto in “Creazione del gestore code” a pagina 21.

Informazioni su questa attività

Avviare l'interfaccia **MQSC** per gestire gli oggetti connessi al gestore code. Creare una coda di trasmissione e una definizione di coda remota. Uscire dall'interfaccia **MQSC** .

Procedura

1. Sulla riga comandi, immettere:

```
runmqsc QM1
```

Dopo un messaggio di conferma, lo strumento è pronto per accettare i comandi.

2. Creare una coda di trasmissione denominata QM2. Si consiglia di assegnare alla coda di trasmissione lo stesso nome del gestore code remoto. Nell'interfaccia MQSC, immettere:

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

Viene creata la coda di trasmissione.

3. Creare una definizione di coda remota denominata QUEUE.ON.QM2QM2. La definizione della coda remota deve fare riferimento al nome fornito alla coda locale sull'host remoto. Nell'interfaccia MQSC, immettere:

```
DEFINE QREMOTE(QUEUE.ON.QM2) DESCR('Remote queue for QM2') XMITQ(QM2) RNAME(RECEIVEQUEUE)
RQMNAME(QM2)
```

Viene creata la definizione della coda remota.

4. Immettere end per uscire dall'interfaccia MQSC.

Operazioni successive

Per creare il canale mittente utilizzato per la connessione al gestore code di destinazione, seguire le istruzioni in “Creare il canale del mittente” a pagina 22.

Creare il canale del mittente

Creare il canale del mittente sul gestore di code di origine; il canale viene utilizzato per connettersi al gestore di code di destinazione.

Prima di iniziare

Per creare un canale che utilizza TLS, seguire le istruzioni in '“Creazione dei canali per utilizzare TLS” a pagina 28. Questa operazione può essere eseguita in seguito, se si desidera testare la soluzione senza la sicurezza TLS.

Informazioni su questa attività

Avviare l'interfaccia '**MQSC** per amministrare gli oggetti collegati al gestore di code e creare il canale del mittente. Questo canale viene utilizzato per connettersi al gestore di code di destinazione chiamato QM2.

Procedura

1. Alla riga di comando, digitare:

```
runmqsc QM1
```

Dopo un messaggio di conferma, lo strumento è pronto ad accettare i comandi.

2. Creare il canale mittente, chiamato TO.QM2. Nell'interfaccia MQSC, digitare:

```
DEFINE CHANNEL(TO.QM2) CHLTYPE(SDR) CONNAME(' remoteHost ') TRPTYPE(TCP) XMITQ(QM2)
```

Nota: La variabile *remoteHost* è il nome host o l'indirizzo IP del gestore di code di destinazione.

Viene creato il canale del mittente.

Operazioni successive

Per creare la topologia del gestore di code distribuito, seguire le istruzioni del '“Creazione della topologia del gestore code distribuito” a pagina 23.

Creazione della topologia del gestore code distribuito

La messaggistica point - to - point è la forma più semplice di messaggistica in IBM MQ. Nella messaggistica point - to - point, l'applicazione mittente deve conoscere determinate informazioni sull'applicazione ricevente prima che i messaggi possano essere inviati. L'applicazione mittente richiederà un modo per indirizzare la coda remota. Utilizzare la messaggistica point - to - point per inviare un messaggio ad un secondo gestore code con un'applicazione di esempio.

Prima di iniziare

È necessario aver impostato il gestore code di origine come descritto in “Creazione del gestore code” a pagina 21.

Informazioni su questa attività

Creare il gestore code di destinazione su un host remoto. Utilizzare le applicazioni di esempio per verificare la comunicazione tra i gestori code di origine e di destinazione.

Creazione del gestore code

Creare un gestore code IBM MQ per ricevere messaggi dal gestore code remoto.

Prima di iniziare

È necessario che IBM MQ sia installato. Per ulteriori informazioni sull'installazione di IBM MQ, consultare Installazione di un server IBM MQ su Windows.

Informazioni su questa attività

Creare il gestore code IBM MQ utilizzando la CLI (command - line interface).

Procedura

1. Creare un gestore code con il nome QM2. Sulla riga comandi, immettere:

   ```
   crtmqm QM2
   ```

   Vengono visualizzati i seguenti messaggi:

   ```
   IBM MQ queue manager created.
   Creating or replacing default objects for QM2.
   Default objects statistics : 61 created. 0 replaced. 0 failed.
   Completing setup.
   Setup completed.
   ```

2. Avviare il gestore code. Sulla riga comandi, immettere:

   ```
   strmqm QM2
   ```

   Vengono visualizzati i seguenti messaggi per confermare che il gestore code è stato avviato:

   ```
   IBM MQ queue manager 'QM2' starting.
   5 log records accessed on queue manager 'QM2' during the log replay phase.
   Log replay for queue manager 'QM2' complete.
   Transaction manager state recovered for queue manager 'QM2'.
   IBM MQ queue manager 'QM2' started.
   ```

Risultati

Il IBM MQ gestore code QM2 viene creato e avviato.

Operazioni successive

Per creare la coda da utilizzare con QM2, seguire le istruzioni riportate in “Creazione della coda” a pagina 24.

Creazione della coda

Creare la coda locale utilizzata per ricevere i messaggi sul gestore code di destinazione e il listener che accetta la connessione del canale in ingresso.

Informazioni su questa attività

Dopo aver avviato lo strumento di script **runmqsc** , è possibile utilizzare i comandi MQSC per creare una coda locale e un listener.

Procedura

1. Avviare lo strumento di script immettendo il seguente comando:

   ```
   runmqsc QM2
   ```

   Viene visualizzato un messaggio per confermare che lo strumento è stato avviato.
2. Creare una coda locale denominata RECEIVEQUEUE. La coda deve avere lo stesso nome a cui si fa riferimento nella definizione della coda remota sul gestore code di origine. Nell'interfaccia MQSC, immettere:

   ```
   DEFINE QLOCAL(RECEIVEQUEUE) DESCR('Receiving queue')
   ```

   Viene creata la coda locale.
3. Creare un listener denominato LISTENER1. Nell'interfaccia MQSC, immettere:

   ```
   DEFINE LISTENER(LISTENER1) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)
   ```

   Nota: La porta 1414 è la porta predefinita per IBM MQ. Se è stato scelto un altro numero di porta, è necessario aggiungerlo al CONNAME del canale mittente sul gestore code di invio.
4. Avviare il listener in modo che sia pronto ad accettare connessioni in ingresso. Nell'interfaccia MQSC, immettere:

   ```
   START LISTENER(LISTENER1)
   ```

   Nota: Dal momento che il listener è stato creato con l'opzione CONTROL (QMGR), al successivo avvio del gestore code, anche il listener verrà avviato automaticamente.
5. Immettere end per uscire dall'interfaccia **MQSC** .

Operazioni successive

Per creare il canale ricevente per creare la connessione tra i gestori code di origine e di destinazione, seguire le istruzioni in “Creazione del canale ricevente” a pagina 24.

Creazione del canale ricevente

Creare il canale ricevente per il gestore code di destinazione per consentire la comunicazione tra i gestori code di origine e di destinazione.

Prima di iniziare

Per creare un canale che utilizza TLS, seguire le istruzioni in '“Creazione dei canali per utilizzare TLS” a pagina 28. Questa operazione può essere eseguita successivamente se si desidera testare la soluzione senza la sicurezza TLS.

Informazioni su questa attività

Utilizzare l'interfaccia **MQSC** per creare un canale destinatario gestito da QM2.

Procedura

1. Sulla riga comandi, immettere:

   ```
   runmqsc QM2
   ```

   Dopo un messaggio di conferma, lo strumento è pronto per accettare i comandi.
2. Creare un canale ricevente denominato TO.QM2QM2. Il canale deve avere lo stesso nome del canale mittente sul gestore code di origine. Nell'interfaccia MQSC, immettere:

   ```
   DEFINE CHANNEL(TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP)
   ```

   Il canale destinatario viene creato.

Operazioni successive

Per avviare il canale del mittente sul gestore di code di origine, che a sua volta avvia il canale del destinatario sul gestore di code di destinazione, seguire le istruzioni in '“Avvio del canale mittente” a pagina 25.

Avvio del canale mittente

Avviare il canale mittente sul gestore code di origine, viene avviato anche il canale ricevente sul gestore code di destinazione. I messaggi possono essere inviati dal gestore code di origine al gestore code di destinazione.

Informazioni su questa attività

Avviare l'interfaccia **MQSC** per gestire gli oggetti connessi al gestore code. Avviare il canale mittente per connettersi al gestore code di destinazione, abilitando la comunicazione. Il canale ricevente viene avviato automaticamente all'avvio del canale di origine.

Procedura

1. Sulla riga comandi, immettere:

   ```
   runmqsc QM1
   ```

   Dopo un messaggio di conferma, lo strumento è pronto per accettare i comandi.
2. Avviare il canale mittente sul gestore code di origine. Nell'interfaccia MQSC, immettere:

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

   Viene avviato anche il canale mittente, il canale ricevente sul gestore code di destinazione.
3. Verificare che il canale sia in esecuzione. Nell'interfaccia MQSC, immettere:

   ```
   DISPLAY CHSTATUS(TO.QM2)
   ```

   Se il canale è in esecuzione, si vedrà che riporta STATUS （RUNNING). Se riporta qualsiasi altro valore in STATUS , controllare il log degli errori.

Operazioni successive

Per verificare che il gestore code di origine possa inviare messaggi al gestore code di destinazione, seguire le istruzioni in “Verifica della soluzione” a pagina 25.

Verifica della soluzione

Verificare che il gestore di code di origine possa inserire un messaggio nella coda remota. Verificare che il gestore delle code di destinazione possa ottenere il messaggio dalla coda.

Informazioni su questa attività
Utilizzate le applicazioni di esempio, '**amqsput** e '**amqsget** per verificare la soluzione.

Procedura
1. Invia un messaggio al gestore di code di destinazione, QM2, dal gestore di code di origine.
   a) Nell'interfaccia a riga di comando, digitare:

   ```
   amqsput QUEUE.ON.QM2 QM1
   ```

   È necessario utilizzare il nome della definizione di coda remota per inviare il messaggio al gestore di coda di destinazione.

   Viene visualizzato il seguente messaggio:

   ```
   Sample AMQSPUT0 start
   target queue is QUEUE.ON.QM2
   ```

   b) Digitare " `Hello world.` e premere due volte Invio.
2. Ottenere il messaggio sul gestore di code di destinazione.
   a) Nell'interfaccia a riga di comando, digitare:

   ```
   amqsget RECEIVEQUEUE QM2
   ```

   Viene visualizzato il seguente messaggio:

   ```
   Sample AMQSGET0 start
   message <Hello world.>
   no more messages
   Sample AMQSGET0 end
   ```

Risultati
Il gestore delle code di destinazione ha ricevuto il messaggio dal gestore delle code di origine, verificando che la comunicazione punto a punto è stata raggiunta.

Operazioni successive
Se si desidera aggiungere la sicurezza alla soluzione, seguire le istruzioni in '“Protezione della topologia point - to - point” a pagina 26.

Protezione della topologia point - to - point

Proteggere la topologia point-to-point in modo che i messaggi possano essere trasmessi in un ambiente di produzione.

Informazioni su questa attività
Proteggere gli oggetti del gestore code di origine e di destinazione in modo che sia concesso il corretto livello di accesso. Definire quali gruppi di utenti hanno accesso alle code e ai gestori code. Proteggi la connessione di rete utilizzando certificati firmati digitalmente per connettersi utilizzando TLS (Transport Layer Security).

Proteggere gli oggetti del gestore delle code di origine

Impostare i valori di autorizzazione per gli oggetti sul gestore di code di origine.

Informazioni su questa attività
Usare il comando '**setmqaut** per concedere le autorità al gruppo di utenti che esegue l'applicazione.

Procedura

1. Per concedere al gruppo di utenti specificato l'autorizzazione di *connessione* al gestore di code, digitare sull'interfaccia della riga di comando:

```
setmqaut -m QM1 -t qmgr -g userGroup +connect
```

2. Per concedere al gruppo di utenti specificato l'autorizzazione a *mettere* sulla definizione di coda remota, digitare sull'interfaccia della riga di comando:

```
setmqaut -m QM1 -t q -n "QUEUE.ON.QM2" -g userGroup +put
```

Protezione degli oggetti del gestore delle code di destinazione

Impostare i valori di autorizzazione per gli oggetti sul gestore di code di destinazione.

Informazioni su questa attività

Usare il comando '**setmqaut** per concedere le autorità al gruppo di utenti che esegue l'applicazione.

Procedura

1. Per concedere al gruppo di utenti specificato l'autorizzazione di *connessione* al gestore di code, digitare sull'interfaccia della riga di comando:

```
setmqaut -m QM2 -t qmgr -g userGroup +connect
```

2. Per concedere al gruppo di utenti specificato l'autorizzazione *get* sulla definizione di coda remota, nell'interfaccia a riga di comando digitare:

```
setmqaut -m QM2 -t q -n "RECEIVEQUEUE" -g userGroup +get
```

Protezione della rete

Proteggere le connessioni di rete tra i gestori code di origine e remoti.

Informazioni su questa attività

Utilizzare i certificati firmati per verificare l'autenticità dei gestori code di origine e remoti. Trasferire i messaggi utilizzando una rete TLS per codificare i messaggi.

Preparazione dei gestori code all'utilizzo di TLS

Il repository delle chiavi del gestore code IBM MQ viene utilizzato per memorizzare il certificato personale del gestore code e il certificato CA (Certificate Authority) pubblico. La richiesta di certificato personale dal gestore code IBM MQ deve essere firmata da una CA, il certificato pubblico viene utilizzato da altre entità per autenticare il gestore code IBM MQ .

Prima di iniziare

È necessario disporre del certificato CA (Certificate Authority) pubblico in un file.

Informazioni su questa attività

Creare il repository delle chiavi del gestore code IBM MQ , importare il certificato del firmatario dell'autorità di certificazione e creare la richiesta di certificato personale del gestore code.

Procedura

1. Creare un file di repository delle chiavi CMS per il gestore code denominato `key.kdb`. Passare alla cartella `Qmgrs\QM1\ssl` e, sulla riga comandi, immettere:

```
runmqakm -keydb -create -db key.kdb -pw passw0rd -type cms -stash
```

Nota: Per questo semplice esempio è stata usata una password di `passw0rd`. È possibile scegliere una parola d'ordine differente e modificare ciascuno dei seguenti comandi per utilizzare la propria parola d'ordine.

2. Aggiungere il certificato CA, presente in un file, al repository di chiavi, sulla riga comandi, immettere:

```
runmqakm -cert -add -file CA-certificate-file -db key.kdb -pw passw0rd -label TrustedCA
```

3. Richiedere un certificato personale che verrà scritto in un file di richiesta denominato `QM1req.req`.
   Sulla riga comandi, immettere:

```
runmqakm -certreq -create -db key.kdb -pw passw0rd -label ibmwebspheremqqm1
         -dn CN="QM1" -size 1024 -file QM1req.req -sig_alg SHA1WithRSA
```

   Il nome dell'etichetta del certificato predefinito viene mostrato in questo esempio. È possibile impostare il proprio nome, se si preferisce. Per i dettagli, consultare Etichetta certificato digitale.

4. Invia il file di richiesta di certificato alla tua CA, emetterà un certificato firmato digitalmente. Inserire il file del certificato firmato ricevuto in un percorso appropriato da ricevere nel repository delle chiavi del gestore code.
5. Ricevere il certificato personale firmato nel repository delle chiavi del gestore code.

```
runmqakm -cert -receive -file Signed-certificate-file -db key.kdb -pw passw0rd -format ascii
```

6. Completare la seguente procedura per ogni gestore code, modificando di conseguenza il relativo nome.

Operazioni successive

Per abilitare la comunicazione protetta sui canali mittente e destinatario, seguire le istruzioni in “Creazione dei canali per utilizzare TLS” a pagina 28.

Creazione dei canali per utilizzare TLS

Crea un nuovo canale che utilizza TLS per creare un collegamento.

Prima di iniziare

Per comunicare su un canale che utilizza TLS, devi prima avere i certificati richiesti per ogni estremità di connessione. Per creare i certificati richiesti, seguire le istruzioni riportate in “Preparazione dei gestori code all'utilizzo di TLS” a pagina 27.

Informazioni su questa attività

Utilizzare l'interfaccia MQSC per definire i canali con gli attributi TLS impostati. Questa attività può essere eseguita anche se i canali sono stati definiti senza TLS in un passo precedente tramite l'utilizzo della parola chiave REPLACE .

Procedura

1. Sulla riga comandi, immettere:

```
runmqsc QM1
```

2. Creare il canale mittente su QM1, denominato `TO.QM2`, nell'interfaccia MQSC, immettere:

```
DEFINE CHANNEL(TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP)
CONNAME('remoteHost') XMITQ(QM2)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
DESCR('Sender channel using TLS from QM1 to QM2')
REPLACE
```

Nota: La variabile *remoteHost* è il nome host o l'indirizzo IP del gestore code di destinazione.

È possibile specificare un attributo CERTLABL per il canale. In tal caso, deve corrispondere al valore del parametro **-label** del comando **runmqakm** precedentemente eseguito nel passo "3" a pagina 28 di "Preparazione dei gestori code all'utilizzo di TLS" a pagina 27. Per ulteriori informazioni sulle etichette certificato, consultare Etichette certificato digitale, comprensione dei requisiti.

3. Immettere end per uscire dall'interfaccia MQSC.
4. Sulla riga comandi, immettere:

```
runmqsc QM2
```

5. Creare un canale ricevente su QM2, denominato TO.QM2, nell'interfaccia MQSC, immettere:

```
DEFINE CHANNEL(TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) SSLCAUTH(REQUIRED)
DESCR('Receiver channel using TLS from QM1 to QM2')
REPLACE
```

6. Immettere end per uscire dall'interfaccia MQSC.

Operazioni successive

Per verificare che il gestore code di origine possa inviare messaggi al gestore code di destinazione utilizzando TLS, seguire le istruzioni in "Verifica della soluzione" a pagina 25.

Code di streaming

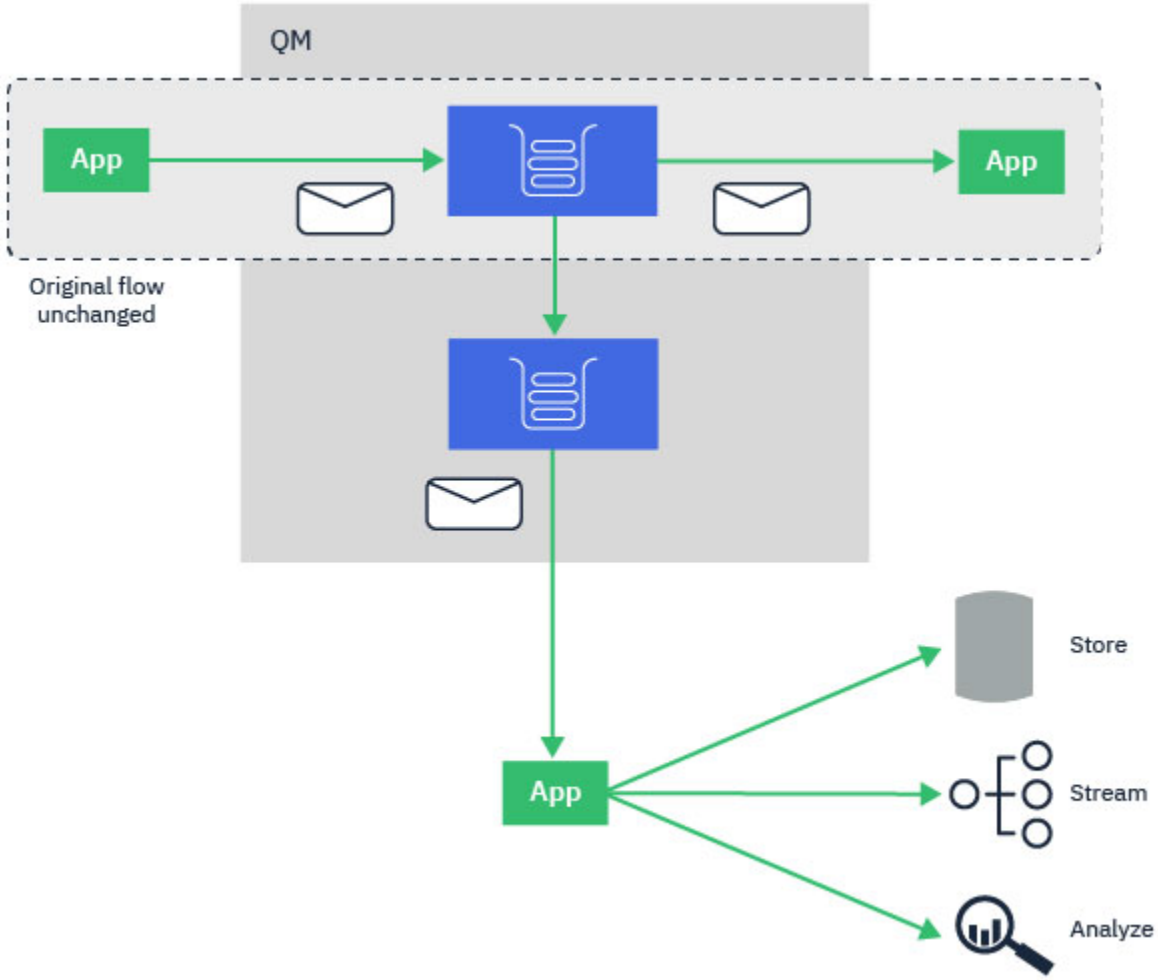
La funzione delle code di flusso di IBM MQ consente di configurare una coda per inserire una copia quasi identica di ogni messaggio in una seconda coda.

Le code di streaming possono essere utili in alcuni scenari, in cui è necessario creare una copia dei messaggi. Ad esempio:

- Flusso di messaggi a Apache Kafka utilizzando il connettore origine Kafka Connect per IBM MQ. Per ulteriori informazioni, consultare kafka_connect_mq_source.
- Esecuzione dell'analisi sui dati che passano attraverso il sistema.
- Memorizzazione dei messaggi per il ripristino in un momento successivo.
- Acquisizione di una serie di messaggi da utilizzare nei sistemi di test e di sviluppo.
- Utilizzo dei messaggi di evento IBM MQ dalle code eventi del sistema e invio di copie aggiuntive ad altre code o argomenti.

In tutti questi scenari, è possibile configurare le code di streaming per garantire che i messaggi originali non vengano influenzati dal processo di streaming. Ciò garantisce che le applicazioni core business non osservino alcun impatto dal flusso.

La seguente illustrazione illustra quanto segue:



Concetti correlati
Sicurezza delle code di flusso
Code di flusso e AMS

Configurazione delle code di flusso

La funzione delle code di streaming di IBM MQ è configurata dall'amministratore su singole code e i messaggi vengono trasmessi dal gestore code, non dall'applicazione stessa.

Ciò significa che in quasi tutti i casi l'applicazione che mette i messaggi nella coda originale è completamente ignora che lo streaming è in corso. Allo stesso modo, l'applicazione che utilizza i messaggi dalla coda originale non è consapevole che il flusso di messaggi è stato effettuato.

Nota: La versione della libreria client IBM MQ non richiede l'aggiornamento per utilizzare le code di flusso e i messaggi originali sono completamente invariati dal processo di flusso.

È possibile configurare le code di flusso in una delle due seguenti modalità:

Massimo sforzo
In questa modalità, il gestore code considera più importante che la consegna del messaggio originale non sia influenzata dalla consegna del messaggio in streaming.

Se il messaggio originale può essere consegnato, ma il messaggio trasmesso in streaming non può, il messaggio originale viene ancora consegnato alla sua coda. Questa modalità è più adatta a quelle applicazioni, in cui è importante che l'applicazione di business originale non venga influenzata dal processo di streaming.

Deve duplicare
In questa modalità, il gestore code garantisce che il messaggio originale e il messaggio di flusso vengano consegnati correttamente alle relative code.

Se, per qualche motivo, il messaggio di flusso non può essere consegnato alla sua coda, ad esempio, perché la seconda coda è piena, anche il messaggio originale non viene consegnato alla sua coda. L'applicazione di inserimento riceve un codice di errore e deve provare a inserire nuovamente il messaggio.

Consultare Modalità di configurazione delle code di flusso per informazioni sugli attributi aggiuntivi aggiunti alle code locali e modello che abilitano il flusso di messaggi.

Messaggi trasmessi

Nella maggior parte dei casi, la copia del messaggio consegnato alla seconda coda è un duplicato del messaggio originale. Ciò include tutti i campi del descrittore del messaggio, inclusi ID messaggio e ID correlazione. I messaggi trasmessi in streaming sono destinati a essere copie molto vicine dei messaggi originali, in modo che siano più facili da trovare e, se necessario, riprodurli in un altro sistema IBM MQ .

Ci sono alcuni campi descrittori di messaggi che non sono conservati nel messaggio di flusso. Le seguenti modifiche vengono apportate al messaggio di flusso prima che venga inserito nella seconda coda:

- La scadenza del messaggio in streaming è impostata su MQEI_UNLIMITED, indipendentemente dalla scadenza del messaggio originale. Se **CAPEXPRY** è stato impostato sulla coda secondaria, il suo valore viene utilizzato per impostare la scadenza del messaggio di flusso.
- Se una delle seguenti opzioni di report è impostata sul messaggio originale, non sono abilitate sul messaggio di flusso. Ciò per garantire che non vengano consegnati messaggi di report non previsti alle applicazioni che non sono progettate per riceverli:
  - Report di attività
  - Report di scadenza
  - Report di eccezioni
  - Conferma all'arrivo (COA)
  - Conferma alla consegna (COD)

A causa della natura quasi identica dei messaggi trasmessi, la maggior parte degli attributi della coda secondaria non hanno alcun effetto sui campi del descrittore del messaggio del messaggio trasmesso. Ad esempio, gli attributi **DEFPSIST** e **DEFPRTY** della coda secondaria non hanno alcun effetto sul messaggio trasmesso.

Le seguenti eccezioni si applicano al messaggio di flusso:

- **CAPEXPRY** attributo

  Se la coda secondaria è stata configurata con un attributo **CAPEXPRY** , questo limite di scadenza viene applicato alla scadenza del messaggio di flusso.
- **DEFBIND** per code cluster

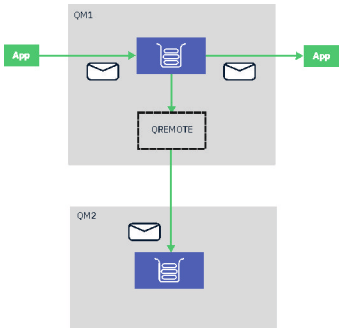
  Se la coda secondaria è una coda cluster, il messaggio di flusso viene inserito utilizzando l'opzione di collegamento impostata nell'attributo **DEFBIND** della coda secondaria.

Flusso a code remote e alias

È possibile trasmettere i messaggi alle code remote e alle code alias. Ad esempio, Q1 potrebbe essere configurato con STREAMQ (MY.REMOTE.Q) dove MY.REMOTE.Q è una definizione di coda remota.

Flusso alle code remote

Trasmettendo i messaggi da una coda locale a una coda remota, i messaggi duplicati possono essere inviati a una coda su un altro gestore code nella rete IBM MQ come mostrato nella seguente figura:



Flusso alle code alias

Trasmettendo i messaggi a una coda alias, è possibile inviare i messaggi duplicati alla destinazione della coda alias. Poiché la destinazione di una coda alias può essere anche un argomento, è quindi possibile inviare i messaggi duplicati a un argomento di pubblicazione / sottoscrizione. Tutti i sottoscrittori dell'argomento alias riceveranno una copia del messaggio duplicato. In questo modo, è possibile creare più copie del messaggio originale. Tuttavia, le regole esistenti per il messaggio di pubblicazione / sottoscrizione vengono applicate al messaggio duplicato. Ciò significa che i messaggi inviati ai sottoscrittori non saranno identici al messaggio originale, incluso:

- Avere un nuovo ID messaggio.
- Avere un ID di correlazione generato, a seconda della configurazione della sottoscrizione.
- Il campo UserIdentifier viene impostato sull'utente con cui è in esecuzione il gestore code e non sull'utente che ha inserito il messaggio.
- Il nome PutApplche mostra il nome del gestore code, non il nome dell'applicazione di inserimento.

Note:

1. Non è possibile configurare l'attributo **STREAMQ** sulle code remote o sulle code alias stesse. È possibile trasmettere messaggi solo a loro, non da loro.
2. Se i messaggi vengono trasmessi in un alias della coda, la destinazione dell'alias della coda non può avere il relativo attributo **STREAMQ** impostato.

Limitazioni della coda di flusso

Alcune configurazioni non sono supportate quando si utilizzano code di flusso in IBM MQ, e queste sono documentate qui.

Il seguente elenco specifica le configurazioni non supportate:

- Definizione di una catena di code che si scambiano, ad esempio, Q1->Q2, Q2->Q3, Q3->Q4
- Definizione di un ciclo di code di flusso, ad esempio Q1->Q2, Q2->Q1
- Definizione di una sottoscrizione con una destinazione fornita, dove tale destinazione ha un STREAMQ definito
- Definizione di STREAMQ in una coda configurata con USAGE (XMITQ)

  Nota: STREAMQ può essere una coda remota, ma non è possibile configurare l'attributo STREAMQ su una definizione di coda remota.
- Modifica dell'attributo STREAMQ di una coda dinamica
- Impostazione di STREAMQ su qualsiasi valore che inizia con SYSTEM. *, ad eccezione di SYSTEM.DEFAULT.LOCAL.QUEUE
- Definizione di STREAMQ su qualsiasi coda denominata SYSTEM. *, con le eccezioni seguenti:
  - SYSTEM.DEFAULT.LOCAL.QUEUE
  - SYSTEM.ADMIN.ACCOUNTING.QUEUE
  - SYSTEM.ADMIN.ACTIVITY.QUEUE

  - SYSTEM.ADMIN.CHANNEL.EVENT
  - SYSTEM.ADMIN.COMMAND.EVENT
  - SYSTEM.ADMIN.CONFIG.EVENT
  - SYSTEM.ADMIN.LOGGER.EVENT
  - SYSTEM.ADMIN.PERFM.EVENT
  - SYSTEM.ADMIN.PUBSUB.EVENT
  - SYSTEM.ADMIN.QMGR.EVENT
  - SYSTEM.ADMIN.STATISTICS.QUEUE
  - SYSTEM.DEFAULT.MODEL.QUEUE
  - SYSTEM.JMS.TEMPQ.MODEL
- Impostazione di STREAMQ sul nome di una coda modello

Transazioni e code di flusso

La funzione delle code di flusso consente di inserire un messaggio in una coda, da duplicare in una seconda coda. Nella maggior parte dei casi, i due messaggi vengono inseriti nelle rispettive code sotto un'unità di lavoro.

Se il messaggio originale è stato inserito utilizzando MQPMO_SYNCPOINT, il messaggio duplicato viene inserito nella coda di flusso nella stessa unità di lavoro avviata per l'inserimento originale.

Se l'originale è stato inserito con MQPMO_NO_SYNCPOINT, verrà avviata un'unità di lavoro anche se l'inserimento originale non ne ha richiesto uno. Ciò viene fatto per due motivi:

1. Garantisce che il messaggio duplicato non venga consegnato se non è stato possibile consegnare il messaggio originale. La funzione delle code di flusso consegna i messaggi solo alle code di flusso se anche il messaggio originale è stato consegnato.
2. È possibile migliorare le prestazioni effettuando entrambe le operazioni all'interno di un'unità di lavoro

L'unica volta in cui i messaggi non vengono consegnati all'interno di un'unità di lavoro è quando MQPUT originale è non persistente con MQPMO_NO_SYNCPOINT e l'attributo **STRMQOS** della coda è impostato su BESTEF (massimo sforzo).

Note:

1. L'inserimento aggiuntivo nella coda di flusso non viene conteggiato nel limite MAXUMSGS.
2. nel caso di una coda configurata con STRMQOS (BESTEF), l'errore di consegna del messaggio duplicato non causa il rollback dell'unità di lavoro.

Flusso verso e da code cluster

È possibile inviare messaggi da una coda locale a una coda cluster e trasmettere messaggi da istanze della coda cluster a una coda locale.

Flusso a una coda cluster

Ciò può essere utile se si dispone di una coda locale in cui vengono consegnati i messaggi originali e si desidera inviare una copia di ogni messaggio a una o più istanze di una coda cluster. Ciò potrebbe essere per bilanciare il carico di lavoro dell'elaborazione dei messaggi duplicati o semplicemente per fare in modo che i messaggi duplicati vengano trasmessi a un'altra coda altrove nel cluster.

Quando si inviano messaggi a una coda cluster, i messaggi vengono distribuiti utilizzando l'algoritmo di bilanciamento del carico di lavoro del cluster. Un'istanza della coda cluster viene selezionata in base all'attributo DEFBIND della coda cluster.

Ad esempio, se la coda del cluster è configurata con DEFBIND (OPEN), viene scelta un'istanza della coda del cluster quando viene aperta la coda originale. Tutti i messaggi duplicati vengono inviati alla stessa istanza della coda cluster, finché la coda originale non viene riaperta dall'applicazione.

Se la coda cluster è configurata con DEFBIND (NOTFIXED), verrà scelta un'istanza della coda cluster per ogni operazione MQPUT.

Nota: Si consiglia di configurare tutte le istanze della coda cluster con lo stesso valore per l'attributo DEFBIND.

Flusso da una coda cluster

Ciò può essere utile se si inviano già messaggi a diverse istanze di una coda cluster e si desidera che una copia di ciascun messaggio venga consegnata a una coda di flusso, sullo stesso gestore code, dell'istanza della coda cluster.

Quando il messaggio originale viene consegnato a una delle istanze della coda cluster, un messaggio duplicato viene consegnato alla coda di flusso dal canale ricevente del cluster.

V 9.4.0 Multi Utilizzo delle code di streaming per memorizzare una cronologia di messaggi

È possibile utilizzare le code di flusso per conservare una cronologia di messaggi per un periodo di tempo limitato, configurando l'attributo CAPEXPRY sulla coda a cui vengono trasmessi i messaggi.

Introduzione

Quando i messaggi vengono trasmessi da una coda a un'altra, qualsiasi valore di scadenza impostato sul messaggio viene reimpostato sul valore MQEI_UNLIMITED per la copia duplicata. Per impostazione predefinita, ciò si traduce in un accumulo costante di messaggi sulla coda a cui si sta eseguendo il flusso, se non vi è alcuna applicazione che li utilizza.

In questo scenario si desidera conservare una copia dei messaggi per un periodo di tempo limitato in modo da potervi accedere. Ad esempio, se il messaggio originale è stato accidentalmente rimosso da un'applicazione di consumo.

Non è possibile conservare una copia di ogni messaggio a tempo indeterminato, e per evitare che la coda a cui si sta trasmettendo in streaming diventi piena ci sono due opzioni:

- Eseguire un'applicazione per rimuovere i messaggi ogni tanto
- Configurare i messaggi con una scadenza, facendoli rimuovere da IBM MQ dopo un periodo di tempo.

La seconda opzione può essere molto più conveniente in quanto non richiede di eseguire e mantenere un'applicazione, solo per evitare che la coda si riempia.

Configurazione di CAPEXPRY

L'argomento Applicazione di tempi di scadenza inferiori descrive come configurare CAPEXPRY su una coda. Per questo scenario, è necessario impostare l'attributo CAPEXPRY sulla coda a cui si stanno trasmettendo i messaggi.

Nota: Non è necessario modificare il valore dell'attributo CAPEXPRY nella coda da cui vengono trasmessi i messaggi.

Scegliere un'ora di scadenza adatta per i messaggi duplicati, tenendo conto delle seguenti considerazioni:

1. Per quanto tempo potrebbe essere necessario accedere ai messaggi per
2. Quale deve essere l'attributo MAXDEPTH della coda, in base al numero di messaggi inseriti nella coda originale
3. La quantità di memoria necessaria per memorizzare i messaggi duplicati.

   Ciò potrebbe richiedere la considerazione della dimensione del file system del gestore code e dell'attributo MAXFSIZE della coda.

Accesso ai messaggi duplicati se sono necessari

Se si verifica un problema che richiede l'accesso e il ripristino di alcuni o di tutti i messaggi duplicati, utilizzare il comando **dmpmqmsg** per facilitare l'accesso a tali messaggi.

dmpmqmsg dispone di opzioni per:

- Lettura dei messaggi dalla coda e scrittura di una copia nel file per l'accesso in un secondo momento
- Lettura dei messaggi da un file e riscrittura in una coda per l'utilizzo da parte delle applicazioni

È possibile modificare le intestazioni del messaggio una volta che **dmpmqmsg** le ha scritte in un file. Ad esempio, è possibile reimpostare la scadenza dei messaggi su MQEI_UNLIMITED, prima che **dmqmqmsg** li rimetta in una coda per l'elaborazione, modificando il valore EXP di ogni messaggio nel file su *-1*.

Considerazioni sulle prestazioni

C'è un piccolo costo per lo streaming di messaggi duplicati in un'altra coda e la loro scadenza quando non sono più necessari. Tuttavia, il costo è molto più basso rispetto all'inserimento manuale di una copia in una seconda coda e alla rimozione distruttiva di un'applicazione dopo un periodo di tempo. Il Report prestazioni code di flusso fornisce ulteriori informazioni sulle prestazioni di questo scenario.

Concetti correlati

Sicurezza delle code di flusso

Code di flusso e AMS

Scenari di pubblicazione / sottoscrizione

Due serie di scenari che dimostrano l'uso dei cluster di pubblicazione / sottoscrizione e delle gerarchie di pubblicazione / sottoscrizione.

Gli scenari di pubblicazione / sottoscrizione disponibili sono descritti nei seguenti topic secondari:

Scenario: creazione di un cluster di pubblicazione / sottoscrizione

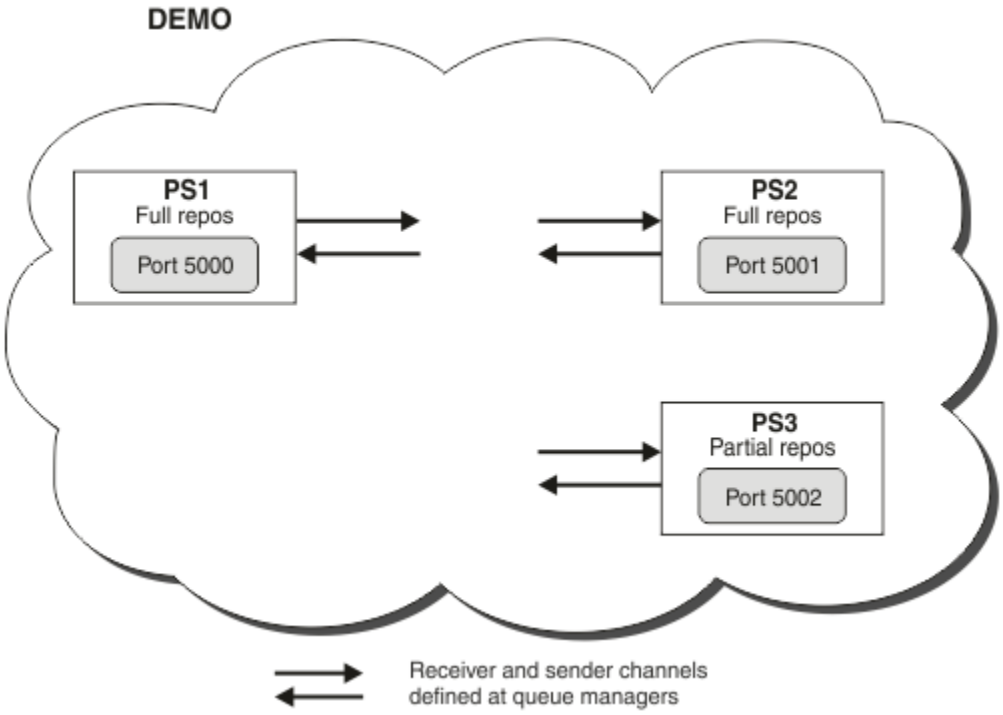
In questo scenario si crea un cluster di tre gestori code semplici e si configura per consentire alle sottoscrizioni create su un gestore code di ricevere i messaggi pubblicati da un'applicazione connessa a un altro gestore code.

Prima di iniziare

Il punto di partenza per questo scenario è un'installazione di IBM MQ esistente. Per istruzioni sull'installazione di IBM MQ , attenersi alla procedura descritta in Installazione di un server IBM MQ su Windows.

Informazioni su questa attività

Completando la procedura in questo scenario, si crea prima il seguente cluster:



Questo cluster è composto da due gestori code, due dei quali sono definiti come gestori code con repository completo.

Definire quindi un argomento cluster sul gestore code PS3. Creando l'argomento cluster, il cluster è stato reso un cluster di pubblicazione / sottoscrizione. Per verificare il cluster di pubblicazione / sottoscrizione, sottoscrivere l'argomento su qualsiasi gestore code, quindi pubblicare un messaggio sull'argomento da un altro gestore code e controllare che la propria sottoscrizione riceva il messaggio.

Attività correlate

Progettazione di cluster di pubblicazione / sottoscrizione

Configurazione di un cluster di gestore code

Creazione e avvio dei gestori di code

Creare e avviare tre gestori di code, chiamati PS1, PS2 e PS3.

Procedura

1. Creare e avviare il gestore di code PS1.
   a) Creare il gestore code.

      Nella riga di comando, immettere il seguente comando:

      ```
      crtmqm PS1
      ```

   b) Avviare il gestore code.

      Nella riga di comando, immettere il seguente comando:

      ```
      strmqm PS1
      ```

2. Ripetere il passo 1 per creare e avviare il gestore di code PS2.
3. Ripetere il passaggio 1 per creare e avviare il gestore di code PS3.

Operazioni successive
Ora si è pronti a configurare il primo gestore di code.

Configurazione del primo gestore code

Utilizzare l'interfaccia di MQSC per definire un listener e un canale ricevente per PS1, per impostare il gestore code come un repository completo per il cluster e per definire un canale mittente da PS1 a PS2 in modo che i due repository completi possano scambiare informazioni.

Prima di iniziare

Questa attività presuppone che siano state completate le operazioni in "Creazione e avvio dei gestori di code" a pagina 36.

Procedura

1. Definire e avviare un listener per PS1.
   a) Avviare l'interfaccia MQSC.

      Nella riga comandi, immettere il comando seguente:

      ```
      runmqsc PS1
      ```

   b) Definire un listener.

      Immettere il comando MQSC riportato di seguito:

      ```
      DEFINE LISTENER(PS1_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(5000)
      ```

   c) Avviare il listener.

      Immettere il comando MQSC riportato di seguito:

      ```
      START LISTENER(PS1_LS)
      ```

2. Impostare il gestore code come repository completo per il cluster.

   Immettere il comando MQSC riportato di seguito:

   ```
   ALTER QMGR REPOS(DEMO)
   ```

3. Definire un canale ricevente per PS1, per consentire ad altri gestori code nel cluster di comunicare con esso.

   Immettere il comando MQSC riportato di seguito:

   ```
   DEFINE CHANNEL(DEMO.PS1) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5000)')
   CLUSTER(DEMO)
       DESCR('TCP Cluster-receiver channel for queue manager PS1')
   ```

4. Definire un canale mittente da PS1 a PS2, per consentire ai due repository completi di scambiare informazioni.

   Immettere il comando MQSC riportato di seguito:

   ```
   DEFINE CHANNEL(DEMO.PS2) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5001)')
   CLUSTER(DEMO)
       DESCR('TCP Cluster-sender channel from PS1 to queue manager PS2')
   ```

Operazioni successive
È ora possibile configurare il secondo gestore code.

Configurazione del secondo gestore di code

Usate l'interfaccia MQSC per definire un ascoltatore e un canale di ricezione per PS2, per impostare il gestore di code come repository completo per il cluster e per definire un canale di invio da PS2 a PS1, in modo che i due repository completi possano scambiarsi informazioni.

Prima di iniziare

Questo compito presuppone che siano stati completati i passaggi in '"Configurazione del primo gestore code" a pagina 37.

Procedura

1. Definire e avviare un ascoltatore per PS2.
   a) Avviare l'interfaccia MQSC.

      Nella riga di comando, immettere il seguente comando:

      ```
      runmqsc PS2
      ```

   b) Definire un ascoltatore.

      Immettere il seguente comando MQSC:

      ```
      DEFINE LISTENER(PS2_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(5001)
      ```

   c) Avviare l'ascoltatore.

      Immettere il seguente comando MQSC:

      ```
      START LISTENER(PS2_LS)
      ```

2. Impostare il gestore di code come repository completo per il cluster.

   Immettere il seguente comando MQSC:

   ```
   ALTER QMGR REPOS(DEMO)
   ```

3. Definire un canale di ricezione per PS2, per consentire agli altri gestori di code del cluster di comunicare con lui.

   Immettere il seguente comando MQSC:

   ```
   DEFINE CHANNEL(DEMO.PS2) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5001)')
   CLUSTER(DEMO)
       DESCR('TCP Cluster-receiver channel for queue manager PS2')
   ```

4. Definire un canale mittente da PS2 a PS1, per consentire ai due archivi completi di scambiare informazioni.

   Immettere il seguente comando MQSC:

   ```
   DEFINE CHANNEL(DEMO.PS1) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5000)')
   CLUSTER(DEMO)
       DESCR('TCP Cluster-sender channel from PS2 to PS1')
   ```

Operazioni successive

Ora si è pronti a configurare il terzo gestore di code.

Configurazione del terzo gestore di code

Utilizzare l'interfaccia MQSC per definire un canale ascoltatore e un canale ricevitore per PS3. Unire PS3 al cluster definendo un canale mittente da PS3 a uno dei gestori di code del repository completo.

Prima di iniziare

Questo compito presuppone che siano stati completati i passaggi in '"Configurazione del secondo gestore di code" a pagina 38.

Procedura

1. Definire e avviare un ascoltatore per PS3.
   a) Avviare l'interfaccia MQSC.

      Nella riga di comando, immettere il seguente comando:

      ```
      runmqsc PS3
      ```

   b) Definire un ascoltatore.

      Immettere il seguente comando MQSC:

      ```
      DEFINE LISTENER(PS3_LS) TRPTYPE(TCP) CONTROL(QMGR) PORT(5002)
      ```

   c) Avviare l'ascoltatore.

      Immettere il seguente comando MQSC:

      ```
      START LISTENER(PS3_LS)
      ```

2. Definire un canale di ricezione per PS3, per consentire agli altri gestori di code del cluster di comunicare con esso.

   Immettere il seguente comando MQSC:

   ```
   DEFINE CHANNEL(DEMO.PS3) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5002)')
   CLUSTER(DEMO)
       DESCR('TCP Cluster-receiver channel for queue manager PS3')
   ```

3. Definire un canale mittente da PS3 a uno dei gestori di coda del deposito completo (ad esempio, PS1). Questo unisce PS3 al cluster.

   Immettere il seguente comando MQSC:

   ```
   DEFINE CHANNEL(DEMO.PS1) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('$HOSTNAME(5000)')
   CLUSTER(DEMO)
       DESCR('TCP Cluster-sender channel from PS3 to PS1')
   ```

4. Convalidare che PS3 si sia unito con successo al cluster.

   Immettere il seguente comando MQSC:

   ```
   DISPLAY CLUSQMGR(*) QMTYPE
   ```

   Questo comando restituisce tre voci, una ciascuna per QM1, QM2 e QM3. QM1 e QM2 devono avere un " **QMTYPE** di REPOS e QM3 deve avere un " **QMTYPE** di NORMAL.

Operazioni successive

Ora si è pronti a definire un argomento del cluster.

Definizione degli argomenti del cluster

Le applicazioni di pubblicazione e sottoscrizione possono essere pubblicate in qualsiasi stringa di argomenti, senza che sia necessario definire un oggetto argomento gestito. Tuttavia, se le applicazioni di pubblicazione sono connesse a un gestore code del cluster diverso dai gestori code in cui vengono create le sottoscrizioni, è necessario definire e aggiungere al cluster un oggetto argomento gestito. Per rendere un argomento un argomento cluster, specificare il nome del cluster nella relativa definizione.

Prima di iniziare

Questa attività presuppone che siano state completate le operazioni in "Configurazione del terzo gestore di code" a pagina 38.

Informazioni su questa attività

L'oggetto argomento gestito identifica il punto nella struttura ad albero dell'argomento che viene raggruppato tramite la relativa stringa di argomento. Le applicazioni di pubblicazione e sottoscrizione possono utilizzare qualsiasi stringa di argomenti in quel punto o al di sotto di tale punto e i relativi messaggi vengono trasmessi automaticamente tra i gestori code.

Quando si definisce un argomento del cluster, si sceglie anche il modello di instradamento. Per ulteriori informazioni sull'instradamento delle pubblicazioni nei cluster, consultare Progettazione dei cluster di pubblicazione / sottoscrizione.

Per questo scenario viene utilizzato l'instradamento predefinito *DIRECT*. Ciò significa che i messaggi vengono inviati direttamente da un gestore code di pubblicazione ai gestori code di sottoscrizione.

Procedura

1. Definire l'argomento del cluster SCORES su PS3.

   Per rendere l'argomento un argomento cluster, specificare il nome del cluster e impostare l'instradamento del cluster (**CLROUTE**) che si desidera utilizzare per pubblicazioni e sottoscrizioni per questo argomento.

   a) Avviare l'interfaccia MQSC.

      Nella riga comandi, immettere il comando seguente:

      ```
      runmqsc PS3
      ```

   b) Definire l'argomento del cluster SCORES.

      Immettere il comando MQSC riportato di seguito:

      ```
      DEFINE TOPIC(SCORES) TOPICSTR('/Sport/Scores') CLUSTER(DEMO) CLROUTE(DIRECT)
      ```

   c) Immettere end per uscire dall'interfaccia MQSC per PS3.
2. Verificare la definizione dell'argomento su PS1.

   a) Avviare l'interfaccia MQSC per PS1.

      Nella riga comandi, immettere il comando seguente:

      ```
      runmqsc PS1
      ```

   b) Visualizzare lo stato del cluster per l'argomento del cluster SCORES.

      Immettere il comando MQSC riportato di seguito:

      ```
      DISPLAY TCLUSTER(SCORES) CLSTATE
      ```

   L'argomento **CLSTATE** per cluster SCORES viene visualizzato come ACTIVE.

Operazioni successive

Per un'esplorazione più dettagliata di questa attività, consultare Configurazione di un cluster di pubblicazione / sottoscrizione.

Si è ora pronti a verificare la soluzione. Consultare "Verifica del cluster di pubblicazione / sottoscrizione" a pagina 41.

Verifica del cluster di pubblicazione / sottoscrizione

Verificare il cluster di pubblicazione / sottoscrizione pubblicando e sottoscrivendo una stringa di argomenti da gestori code differenti nel cluster.

Prima di iniziare

Questa attività presuppone che siano state completate le operazioni in“Definizione degli argomenti del cluster” a pagina 39.

Informazioni su questa attività

Utilizzando la riga comandi e le applicazioni di esempio `amqspub` e `amqssub` incluse con IBM MQ , è possibile pubblicare un argomento da un gestore code e sottoscrivere l'argomento con gli altri gestori code. Quando un messaggio viene pubblicato nell'argomento, viene ricevuto dai gestori code di sottoscrizione.

Procedura

1. Nella riga comandi, immettere il comando seguente:

   ```
   amqspub /Sport/Scores/Football PS1
   ```

2. Contemporaneamente, in righe comandi separate, immettere i seguenti comandi:

   ```
   amqssub /Sport/Scores/Football PS2
   ```

   ```
   amqssub /Sport/Scores/Football PS3
   ```

3. Nella prima riga comandi, immettere un messaggio.

   Il messaggio viene visualizzato in entrambe le righe comandi di sottoscrizione.

   Nota: L'applicazione `amqssub` andrà in timeout se una pubblicazione non viene ricevuta per dieci secondi.

Risultati

La configurazione del cluster di pubblicazione / sottoscrizione è completa.

Operazioni successive

Provare a definire oggetti argomento diversi per rami differenti della struttura ad albero degli argomenti e con modelli di instradamento differenti.

Scenari di gerarchia di pubblicazione / sottoscrizione

Tre scenari che dimostrano l'uso di gerarchie di pubblicazione / sottoscrizione. Ciascuno dei tre scenari configura la stessa semplice topologia di pubblicazione / sottoscrizione. In ogni scenario, i gestori code si basano su un metodo differente per la connessione ai gestori code vicini nella gerarchia.

Gli scenari di gerarchia di pubblicazione / sottoscrizione disponibili sono descritti nei seguenti topic secondari:

Concetti correlati

Gerarchie di pubblicazione / sottoscrizione

Scenario 1 della gerarchia publish/subscribe: utilizzo di canali point-to-point con alias del nome del gestore di code

Questo è il primo di una serie di tre scenari che configurano una gerarchia publish/subscribe in modi diversi per stabilire la connessione tra i gestori di code. Questo scenario configura una gerarchia publish/subscribe che utilizza canali point-to-point con alias di nomi di gestori di code.

Informazioni su questa attività

Questo insieme di scenari utilizza un gestore di code padre chiamato 'QM1 e due gestori di code figlio chiamati 'QM2 e 'QM3.

Lo Scenario 1 è suddiviso in sezioni più piccole per rendere il processo più facile da seguire.

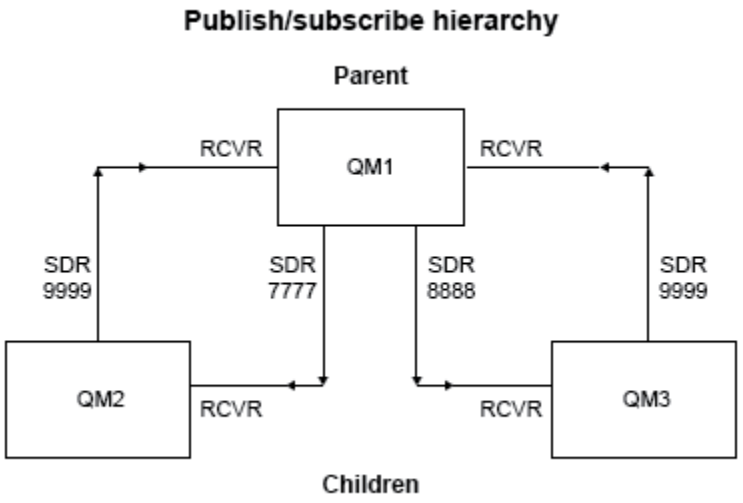


Figura 3. Diagramma topologico che mostra la relazione tra i gestori di code in una tipica gerarchia publisher/subscribe.

Procedura

1. Creare i gestori delle code.
   a) Creare e avviare tre gestori di code chiamati 'QM1, 'QM2 e 'QM3 utilizzando i seguenti comandi:

```
crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM1
strmqm QM1

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM2
strmqm QM2

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM3
strmqm QM3
```

   b) Abilitare la modalità publish/subscribe del gestore di code utilizzando il seguente comando su tutti e tre i gestori di code:

```
ALTER QMGR PSMODE(ENABLED)
```

2. Stabilire connessioni di canale punto-punto tra i gestori di code utilizzando un alias di gestore di code con lo stesso nome del gestore di code padre.
   a) Definire una coda di trasmissione e un alias di gestore di coda su 'QM2 e 'QM1. Definire un canale mittente su 'QM1 e un canale ricevitore per il canale mittente creato su 'QM1 per 'QM2:

```
DEFINE QLOCAL(QM1.XMITQ) USAGE(XMITQ)

DEFINE QREMOTE (QM1) RNAME('') RQMNAME(QM1) XMITQ(QM1.XMITQ)

DEFINE CHANNEL('QM2.TO.QM1') CHLTYPE(SDR) CONNAME('localhost(9999)') XMITQ(QM1.XMITQ)
TRPTYPE(TCP)

DEFINE CHANNEL('QM1.TO.QM2') CHLTYPE(RCVR) TRPTYPE(TCP)
```

   b) Definire una coda di trasmissione e un alias di gestore di coda su 'QM3 e 'QM1. Definire un canale mittente su 'QM1 e un canale ricevitore per il canale mittente creato su 'QM1 per 'QM3:

```
DEFINE QLOCAL(QM1.XMITQ) USAGE(XMITQ)

DEFINE QREMOTE (QM1) RNAME('') RQMNAME(QM1) XMITQ(QM1.XMITQ)

DEFINE CHANNEL('QM3.TO.QM1') CHLTYPE(SDR) CONNAME('localhost(9999)') XMITQ(QM1.XMITQ)
TRPTYPE(TCP)

DEFINE CHANNEL('QM1.TO.QM3') CHLTYPE(RCVR) TRPTYPE(TCP)
```

c) Definire una coda di trasmissione e un alias di gestore di coda su 'QM1 a 'QM2 e 'QM3. Definire un canale mittente per 'QM2 e 'QM3 e un canale ricevitore per i canali mittente creati su 'QM2 e 'QM3 per 'QM1:

```
DEFINE QLOCAL(QM2.XMITQ) USAGE(XMITQ)

DEFINE QREMOTE (QM2) RNAME('') RQMNAME(QM2) XMITQ(QM2.XMITQ)

DEFINE CHANNEL('QM1.TO.QM2') CHLTYPE(SDR) CONNAME('localhost(7777)') XMITQ(QM2.XMITQ)
TRPTYPE(TCP)

DEFINE CHANNEL('QM2.TO.QM1') CHLTYPE(RCVR) TRPTYPE(TCP)

DEFINE QLOCAL(QM3.XMITQ) USAGE(XMITQ)

DEFINE QREMOTE (QM3) RNAME('') RQMNAME(QM3) XMITQ(QM3.XMITQ)

DEFINE CHANNEL('QM1.TO.QM3') CHLTYPE(SDR) CONNAME('localhost(8888)') XMITQ(QM3.XMITQ)
TRPTYPE(TCP)

DEFINE CHANNEL('QM3.TO.QM1') CHLTYPE(RCVR) TRPTYPE(TCP)
```

d) Avviare gli ascoltatori appropriati sui gestori di coda:

```
runmqlsr -m QM1 -t TCP -p 9999 &
runmqlsr -m QM2 -t TCP -p 7777 &
runmqlsr -m QM3 -t TCP -p 8888 &
```

e) Avviare i seguenti canali:

i) Su QM1:

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

START CHANNEL('QM1.TO.QM3')
```

ii) Su QM2:

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

iii) Su QM3:

```
START CHANNEL('QM3.TO.QM1')
```

f) Verificare che tutti i canali siano stati avviati:

```
DISPLAY CHSTATUS('QM1.TO.QM2')

DISPLAY CHSTATUS('QM1.TO.QM3')

DISPLAY CHSTATUS('QM2.TO.QM1')

DISPLAY CHSTATUS('QM3.TO.QM1')
```

g)

3. Collegare i gestori di coda e definire un argomento.

Collegare i gestori di code figlio 'QM2 e 'QM3 al gestore di code padre 'QM1.

a) Su 'QM2 e 'QM3, impostare il gestore della coda padre su 'QM1:

```
ALTER QMGR PARENT (QM1)
```

b) Eseguire il seguente comando su tutti i gestori di code per verificare che i gestori di code figli siano connessi al gestore di code padre:

```
DISPLAY PUBSUB TYPE(ALL)
```

Viene visualizzato l'output del comando. Ad esempio, ecco l'output per QM1, con i dettagli principali evidenziati:

```
DISPLAY PUBSUB ALL
1 : DISPLAY PUBSUB ALL
AMQ8723: Display pub/sub status details.
QMNAME(QM1)               TYPE(LOCAL)
STATUS(ACTIVE)             SUBCOUNT(6)
TPCOUNT(9)
AMQ8723: Display pub/sub status details.
QMNAME(QM2) TYPE(CHILD)
STATUS(ACTIVE) SUBCOUNT(NONE)
TPCOUNT(NONE)
AMQ8723: Display pub/sub status details.
QMNAME(QM3) TYPE(CHILD)
STATUS(ACTIVE) SUBCOUNT(NONE)
TPCOUNT(NONE)
```

4. Utilizzare le applicazioni " amqspub.exe e " amqssub.exe per pubblicare e sottoscrivere l'argomento.
   a) Eseguite questo comando nella prima finestra di comando:

   ```
   amqspub Sport/Soccer QM2
   ```

   b) Eseguite questo comando nella seconda finestra di comando:

   ```
   amqssub Sport/Soccer QM1
   ```

   c) Eseguire questo comando nella terza finestra di comando:

   ```
   amqssub Sport/Soccer QM3
   ```

Risultati

Le applicazioni 'amqssub.exe nella seconda e terza finestra di comando ricevono i messaggi pubblicati nella prima finestra di comando.

Gerarchia di pubblicazione / sottoscrizione scenario 2: utilizzo di canali point - to - point con lo stesso nome per la coda di trasmissione e il gestore code remoto

Questo è il secondo di una serie di tre scenari che impostano una gerarchia di pubblicazione / sottoscrizione in modi diversi per stabilire la connessione tra gestori code. Questo scenario imposta una gerarchia di pubblicazione / sottoscrizione che utilizza canali point-to-point con il nome della coda di trasmissione uguale al gestore code remoto.

Informazioni su questa attività

Questo insieme di scenari utilizza un gestore di code padre chiamato 'QM1 e due gestori di code figlio chiamati 'QM2 e 'QM3.

Questo scenario riutilizza i passi 1, 3 e 4 da “Scenario 1 della gerarchia publish/subscribe: utilizzo di canali point-to-point con alias del nome del gestore di code” a pagina 41.

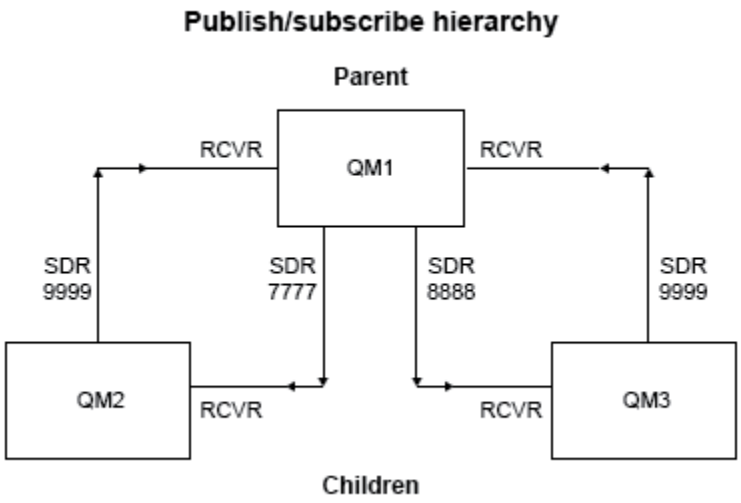


Figura 4. Diagramma della topologia che illustra la relazione tra i gestori code in una tipica gerarchia di pubblicazione / sottoscrizione.

Procedura

1. Creare i gestori delle code.
   a) Creare e avviare tre gestori di code chiamati 'QM1, 'QM2 e 'QM3 utilizzando i seguenti comandi:

```
crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM1
strmqm QM1

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM2
strmqm QM2

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM3
strmqm QM3
```

   b) Abilitare la modalità publish/subscribe del gestore di code utilizzando il seguente comando su tutti e tre i gestori di code:

```
ALTER QMGR PSMODE(ENABLED)
```

2. Stabilire connessioni canale point-to-point tra un gestore code utilizzando una coda di trasmissione con lo stesso nome del gestore code principale.
   a) Definire una coda di trasmissione su QM2 in QM1. Definire un canale mittente per QM1 e un canale destinatario per il canale mittente per QM2 creato su QM1:

```
DEFINE QLOCAL(QM1) USAGE(XMITQ)

DEFINE CHANNEL('QM2.TO.QM1') CHLTYPE(SDR) CONNAME('localhost(9999)') XMITQ(QM1)
TRPTYPE(TCP)

DEFINE CHANNEL('QM1.TO.QM2') CHLTYPE(RCVR) TRPTYPE(TCP)
```

   b) Definire una coda di trasmissione su QM3 in QM1. Definire il canale mittente in QM1 e un canale ricevente per il canale mittente creato su QM1 per QM3:

```
DEFINE QLOCAL(QM1) USAGE(XMITQ)

DEFINE CHANNEL('QM3.TO.QM1') CHLTYPE(SDR) CONNAME('localhost(9999)') XMITQ(QM1)
TRPTYPE(TCP)

DEFINE CHANNEL('QM1.TO.QM3') CHLTYPE(RCVR) TRPTYPE(TCP)
```

c) Definire le code di trasmissione su QM1 in QM2 e QM3. Definire i canali mittenti su QM2 e QM3e un canale ricevente per i canali mittenti creati su QM2 e QM3 per QM1:

```
DEFINE QLOCAL(QM2) USAGE(XMITQ)

DEFINE CHANNEL('QM1.TO.QM2') CHLTYPE(SDR) CONNAME('localhost(7777)') XMITQ(QM2)
TRPTYPE(TCP)

DEFINE CHANNEL('QM2.TO.QM1') CHLTYPE(RCVR) TRPTYPE(TCP)

DEFINE QLOCAL(QM3) USAGE(XMITQ)

DEFINE CHANNEL('QM1.TO.QM3') CHLTYPE(SDR) CONNAME('localhost(8888)') XMITQ(QM3)
TRPTYPE(TCP)

DEFINE CHANNEL('QM3.TO.QM1') CHLTYPE(RCVR) TRPTYPE(TCP)
```

d) Avviare i listener appropriati sui gestori code:

```
runmqlsr -m QM1 -t TCP -p 9999 &
runmqlsr -m QM2 -t TCP -p 7777 &
runmqlsr -m QM3 -t TCP -p 8888 &
```

e) Avviare i canali seguenti:

i) Su QM1:

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

START CHANNEL('QM1.TO.QM3')
```

ii) Su QM2:

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

iii) Su QM3:

```
START CHANNEL('QM3.TO.QM1')
```

f) Verificare che tutti i canali siano stati avviati:

```
DISPLAY CHSTATUS('QM1.TO.QM2')

DISPLAY CHSTATUS('QM1.TO.QM3')

DISPLAY CHSTATUS('QM2.TO.QM1')

DISPLAY CHSTATUS('QM3.TO.QM1')
```

3. Collegare i gestori di coda e definire un argomento.

Collegare i gestori di code figlio 'QM2 e 'QM3 al gestore di code padre 'QM1.

a) Su 'QM2 e 'QM3, impostare il gestore della coda padre su 'QM1:

```
ALTER QMGR PARENT (QM1)
```

b) Eseguire il seguente comando su tutti i gestori di code per verificare che i gestori di code figli siano connessi al gestore di code padre:

```
DISPLAY PUBSUB TYPE(ALL)
```

Viene visualizzato l'output del comando. Ad esempio, ecco l'output per QM1, con i dettagli principali evidenziati:

```
DISPLAY PUBSUB ALL
1 : DISPLAY PUBSUB ALL
AMQ8723: Display pub/sub status details.
QMNAME(QM1)               TYPE(LOCAL)
STATUS(ACTIVE)             SUBCOUNT(6)
TPCOUNT(9)
AMQ8723: Display pub/sub status details.
QMNAME(QM2) TYPE(CHILD)
```

```
STATUS(ACTIVE) SUBCOUNT(NONE)
TPCOUNT(NONE)
AMQ8723: Display pub/sub status details.
QMNAME(QM3) TYPE(CHILD)
STATUS(ACTIVE) SUBCOUNT(NONE)
TPCOUNT(NONE)
```

4. Utilizzare le applicazioni " amqspub.exe e " amqssub.exe per pubblicare e sottoscrivere l'argomento.
   a) Eseguite questo comando nella prima finestra di comando:

   ```
   amqspub Sport/Soccer QM2
   ```

   b) Eseguite questo comando nella seconda finestra di comando:

   ```
   amqssub Sport/Soccer QM1
   ```

   c) Eseguire questo comando nella terza finestra di comando:

   ```
   amqssub Sport/Soccer QM3
   ```

Risultati

Le applicazioni amqssub.exe nella finestra del secondo e terzo comando ricevono i messaggi pubblicati nella finestra del primo comando.

Attività correlate

“Scenario 1 della gerarchia publish/subscribe: utilizzo di canali point-to-point con alias del nome del gestore di code” a pagina 41
Questo è il primo di una serie di tre scenari che configurano una gerarchia publish/subscribe in modi diversi per stabilire la connessione tra i gestori di code. Questo scenario configura una gerarchia publish/subscribe che utilizza canali point-to-point con alias di nomi di gestori di code.

“Scenario di gerarchia di pubblicazione / sottoscrizione 3: utilizzo di un canale cluster per aggiungere un gestore code” a pagina 47
Questo è il terzo di una serie di tre scenari che impostano una gerarchia di pubblicazione / sottoscrizione in modi diversi per stabilire la connessione tra gestori code. Questo scenario utilizza un canale cluster per aggiungere un gestore code a una gerarchia.

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

Scenario di gerarchia di pubblicazione / sottoscrizione 3: utilizzo di un canale cluster per aggiungere un gestore code

Questo è il terzo di una serie di tre scenari che impostano una gerarchia di pubblicazione / sottoscrizione in modi diversi per stabilire la connessione tra gestori code. Questo scenario utilizza un canale cluster per aggiungere un gestore code a una gerarchia.

Informazioni su questa attività

Questo insieme di scenari utilizza un gestore di code padre chiamato 'QM1 e due gestori di code figlio chiamati 'QM2 e 'QM3.

Nota: Questo scenario utilizza solo la configurazione del cluster per connettere i gestori code e non per propagare il traffico di pubblicazione / sottoscrizione attraverso gli argomenti del cluster. Quando si definiscono relazioni di gerarchia child / parent tra gestori code nello stesso cluster, la diffusione delle pubblicazioni tra gestori code avverrà in base alle impostazioni dell'ambito di pubblicazione e sottoscrizione degli argomenti nella struttura ad albero degli argomenti. È importante non utilizzare l'impostazione del nome cluster di un argomento per aggiungere gli argomenti al cluster. Se si utilizza il nome cluster, la topologia diventa un cluster di pubblicazione / sottoscrizione e non richiede le relazioni di gerarchia child / parent definite. Consultare “Scenario: creazione di un cluster di pubblicazione / sottoscrizione” a pagina 35 e Pianificazione della rete di pubblicazione / sottoscrizione distribuita.

Questo scenario riutilizza i passi 1, 3 e 4 da “Scenario 1 della gerarchia publish/subscribe: utilizzo di canali point-to-point con alias del nome del gestore di code” a pagina 41.

Questo scenario crea un cluster denominato DEMO dove QM1 e QM2 sono repository completi e QM3 è un repository parziale. Il gestore code QM1 è l'elemento principale dei gestori code QM2 e QM3.

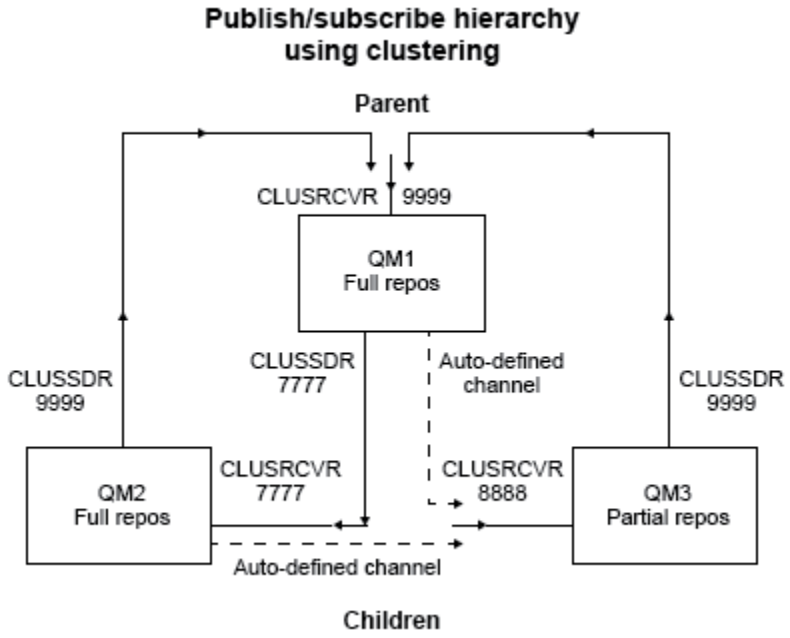


Figura 5. Diagramma della topologia che mostra la relazione tra gestori code che utilizzano un canale cluster.

Procedura

1. Creare i gestori delle code.
   a) Creare e avviare tre gestori di code chiamati 'QM1, 'QM2 e 'QM3 utilizzando i seguenti comandi:

```
crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM1
strmqm QM1

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM2
strmqm QM2

crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM3
strmqm QM3
```

   b) Abilitare la modalità publish/subscribe del gestore di code utilizzando il seguente comando su tutti e tre i gestori di code:

```
ALTER QMGR PSMODE(ENABLED)
```

2. Stabilire le connessioni del canale point-to-point tra i gestori code di un cluster.
   a) Su QM1 e QM2, impostare il parametro **REPOS** sul nome del cluster DEMO:

```
ALTER QMGR REPOS(DEMO)
```

   b) Avviare i listener appropriati sui gestori code:

```
runmqlsr -m QM1 -t TCP -p 9999 &
runmqlsr -m QM2 -t TCP -p 7777 &
runmqlsr -m QM3 -t TCP -p 8888 &
```

   c) Definire il canale ricevente del cluster su ciascun gestore code:

i) Su QM1:

```
DEFINE CHANNEL(TO.QM1) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('localhost(9999)')
CLUSTER(DEMO)
```

ii) Su QM2:

```
DEFINE CHANNEL(TO.QM2) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('localhost(7777)')
CLUSTER(DEMO)
```

iii) Su QM3:

```
DEFINE CHANNEL(TO.QM3) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CONNAME('localhost(8888)')
CLUSTER(DEMO)
```

d) Definire un canale mittente del cluster per un repository completo su ciascun gestore code nel cluster:

i) Su QM1:

```
DEFINE CHANNEL(TO.QM2) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('localhost(7777)')
CLUSTER(DEMO)
```

ii) Su QM2:

```
DEFINE CHANNEL(TO.QM1) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('localhost(9999)')
CLUSTER(DEMO)
```

iii) QM3 può avere un canale mittente del cluster per il repository completo su QM1 o QM2. Questo esempio definisce il canale per QM1:

```
DEFINE CHANNEL(TO.QM1) CHLTYPE(CLUSSDR) TRPTYPE(TCP) CONNAME('localhost(9999)')
CLUSTER(DEMO)
```

3. Collegare i gestori di coda e definire un argomento.

Collegare i gestori di code figlio 'QM2 e 'QM3 al gestore di code padre 'QM1.

a) Su 'QM2 e 'QM3, impostare il gestore della coda padre su 'QM1:

```
ALTER QMGR PARENT (QM1)
```

b) Eseguire il seguente comando su tutti i gestori di code per verificare che i gestori di code figli siano connessi al gestore di code padre:

```
DISPLAY PUBSUB TYPE(ALL)
```

Viene visualizzato l'output del comando. Ad esempio, ecco l'output per QM1, con i dettagli principali evidenziati:

```
DISPLAY PUBSUB ALL
1 : DISPLAY PUBSUB ALL
AMQ8723: Display pub/sub status details.
QMNAME(QM1)               TYPE(LOCAL)
STATUS(ACTIVE)             SUBCOUNT(6)
TPCOUNT(9)
AMQ8723: Display pub/sub status details.
QMNAME(QM2) TYPE(CHILD)
STATUS(ACTIVE) SUBCOUNT(NONE)
TPCOUNT(NONE)
AMQ8723: Display pub/sub status details.
QMNAME(QM3) TYPE(CHILD)
STATUS(ACTIVE) SUBCOUNT(NONE)
TPCOUNT(NONE)
```

4. Utilizzare le applicazioni " amqspub.exe e " amqssub.exe per pubblicare e sottoscrivere l'argomento.

a) Eseguite questo comando nella prima finestra di comando:

```
amqspub Sport/Soccer QM2
```

b) Eseguite questo comando nella seconda finestra di comando:

```
amqssub Sport/Soccer QM1
```

c) Eseguire questo comando nella terza finestra di comando:

```
amqssub Sport/Soccer QM3
```

Risultati

Le applicazioni `amqssub.exe` nella finestra del secondo e terzo comando ricevono i messaggi pubblicati nella finestra del primo comando.

Attività correlate

"Scenario 1 della gerarchia publish/subscribe: utilizzo di canali point-to-point con alias del nome del gestore di code" a pagina 41
Questo è il primo di una serie di tre scenari che configurano una gerarchia publish/subscribe in modi diversi per stabilire la connessione tra i gestori di code. Questo scenario configura una gerarchia publish/subscribe che utilizza canali point-to-point con alias di nomi di gestori di code.

"Gerarchia di pubblicazione / sottoscrizione scenario 2: utilizzo di canali point - to - point con lo stesso nome per la coda di trasmissione e il gestore code remoto" a pagina 44
Questo è il secondo di una serie di tre scenari che impostano una gerarchia di pubblicazione / sottoscrizione in modi diversi per stabilire la connessione tra gestori code. Questo scenario imposta una gerarchia di pubblicazione / sottoscrizione che utilizza canali point-to-point con il nome della coda di trasmissione uguale al gestore code remoto.

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

Scenari di supporto transazionale

Utilizzando il supporto transazionale, è possibile consentire alle proprie applicazioni di lavorare in modo affidabile con database.

Questa sezione introduce il supporto transazionale. Il lavoro richiesto per abilitare le proprie applicazioni all'utilizzo di IBM MQ con un prodotto database abbraccia le aree di programmazione delle applicazioni e di gestione del sistema. Utilizzare le informazioni qui riportate insieme a Commit e backout delle unità di lavoro.

Iniziamo introducendo le unità di lavoro che formano le transazioni, quindi descriviamo i modi in cui si abilita IBM MQ a coordinare le transazioni con i database.

Concetti correlati

"Introduzione delle unità di lavoro" a pagina 50
Questo argomento introduce e definisce i concetti generali di unità di lavoro, commit, backout e punto di sincronizzazione. Contiene inoltre due scenari che illustrano le unità di lavoro globali.

Introduzione delle unità di lavoro

Questo argomento introduce e definisce i concetti generali di unità di lavoro, commit, backout e punto di sincronizzazione. Contiene inoltre due scenari che illustrano le unità di lavoro globali.

Quando un programma inserisce i messaggi nelle code all'interno di un'unità di lavoro, tali messaggi vengono resi visibili ad altri programmi solo quando il programma *esegue il commit* dell'unità di lavoro. Per eseguire il commit di un'unità di lavoro, tutti gli aggiornamenti devono essere eseguiti correttamente per preservare l'integrità dei dati.

Se il programma rileva un errore e decide di non rendere l'operazione di inserimento permanente, può *eseguire il backout* dell'unità di lavoro. Quando un programma esegue un backout, IBM MQ ripristina le code rimuovendo i messaggi inseriti nelle code da tale unità di lavoro.

Allo stesso modo, quando un programma riceve messaggi da una o più code all'interno di un'unità di lavoro, tali messaggi rimangono nelle code fino a quando il programma non esegue il commit dell'unità di lavoro, ma i messaggi non sono disponibili per essere richiamati da altri programmi. I messaggi vengono eliminati permanentemente dalle code quando il programma esegue il commit dell'unità di lavoro. Se il programma esegue il backout dell'unità di lavoro, IBM MQ ripristina le code rendendo i messaggi disponibili per essere richiamati da altri programmi.

La decisione di eseguire il commit o il backout delle modifiche viene presa, nel caso più semplice, alla fine di un'attività. Tuttavia, può essere più utile per un'applicazione sincronizzare le modifiche dei dati in altri punti logici all'interno di un'attività. Questi punti logici sono denominati punti di sincronizzazione (o punti di sincronizzazione) e il periodo di elaborazione di una serie di aggiornamenti tra due punti di sincronizzazione è denominato *unità di lavoro*. Diverse chiamate MQGET e MQPUT possono essere parte di una singola unità di lavoro.

Con IBM MQ, dobbiamo distinguere tra unità di lavoro *locali* e *globali* :

Unità di lavoro locali
Sono quelle in cui le sole azioni vengono immesse e richiamate dalle code IBM MQ e il coordinamento di ciascuna unità di lavoro viene fornito all'interno del gestore code utilizzando un processo *commit a fase singola* .

Utilizzare le unità di lavoro locali quando le uniche risorse da aggiornare sono le code gestite da un unico gestore code IBM MQ . Viene eseguito il commit degli aggiornamenti utilizzando il verbo MQCMIT o il backout utilizzando MQBACK.

Non sono presenti attività di gestione del sistema, diverse dalla gestione log, coinvolte nell'utilizzo delle unità di lavoro locali. Nelle applicazioni, in cui si utilizzano le chiamate MQPUT e MQGET con MQCMIT e MQBACK, provare utilizzando le opzioni MQPMO_SYNCPOINT e MQGMO_SYNCPOINT. (Per informazioni sulla gestione dei log, consultare Gestione dei file di log.)

Unità di lavoro globali
Sono quelle in cui vengono aggiornate anche altre risorse, come le tabelle in un database relazionale. Quando è coinvolto più di un *gestore risorse* , è necessario il software *gestore transazioni* che utilizza un processo di *commit a due fasi* per coordinare l'unità di lavoro globale.

Utilizzare le unità di lavoro globali quando è necessario includere aggiornamenti al software del gestore database relazionale, come Db2, Oracle, Sybasee Informix.

Esistono diversi scenari possibili per l'utilizzo delle unità di lavoro globali. Di seguito sono riportati due scenari:

1. Nel primo, il gestore code stesso funge da gestore transazioni. In questo scenario, i verbi MQI controllano le unità di lavoro globali; vengono avviati nelle applicazioni che utilizzano il verbo MQBEGIN e quindi ne viene eseguito il commit utilizzando MQCMIT o ne viene eseguito il backout utilizzando MQBACK.
2. Nel secondo, il ruolo di gestore transazioni viene eseguito da altri software, come TXSeries, Encina o Tuxedo. In questo scenario, un'API fornita dal software del gestore transazioni viene utilizzata per controllare l'unità di lavoro (ad esempio, EXEC CICS SYNCPOINT per TXSeries).

Le seguenti sezioni descrivono tutte le fasi necessarie per utilizzare le unità di lavoro globali, organizzate in base ai due scenari:

- “Scenario 1: il gestore code esegue il coordinamento” a pagina 51
- “Scenario 2: Altri software forniscono il coordinamento” a pagina 76

Multi Scenario 1: il gestore code esegue il coordinamento

Nello scenario 1, il gestore code agisce come gestore transazioni. In questo scenario, i verbi MQI controllano le unità di lavoro globali; vengono avviati nelle applicazioni che utilizzano il verbo MQBEGIN e quindi ne viene eseguito il commit utilizzando MQCMIT o ne viene eseguito il backout utilizzando MQBACK.

Multi Livello di isolamento

In IBM MQ, un messaggio su una coda potrebbe essere visibile prima di un aggiornamento del database, a seconda della progettazione di isolamento della transazione implementata nel database.

Quando un gestore code IBM MQ funziona come un gestore transazioni XA, per coordinare gli aggiornamenti ai gestori risorse XA, viene seguito il seguente protocollo di commit:

1. Preparare tutti i gestori risorse XA.
2. Eseguire il commit del gestore risorse del gestore code IBM MQ .
3. Eseguire il commit di altri gestori risorse.

Tra i passi 2 e 3, un'applicazione potrebbe visualizzare un messaggio di cui è stato eseguito il commit nella coda, ma la riga corrispondente nel database non riflette questo messaggio.

Non si tratta di un problema se il database è configurato in modo che le chiamate dell'API del database dell'applicazione siano in attesa del completamento degli aggiornamenti in sospeso.

È possibile risolvere questo problema configurando il database in maniera diversa. Il tipo di configurazione necessaria viene definito "livello di isolamento". Per ulteriori informazioni sui livelli di isolamento, fare riferimento alla documentazione del database. In alternativa, è possibile configurare il gestore code per eseguire il commit dei gestori risorse nel seguente ordine inverso:

1. Preparare tutti i gestori risorse XA.
2. Eseguire il commit di altri gestori risorse.
3. Eseguire il commit del gestore risorse del gestore code IBM MQ .

Quando si modifica il protocollo, viene eseguito l'ultimo commit del gestore code IBM MQ , in modo che le applicazioni che leggono i messaggi dalle code visualizzino un messaggio solo dopo il completamento dell'aggiornamento del database corrispondente.

Per configurare il gestore code per utilizzare questo protocollo modificato, impostare la variabile di ambiente **AMQ_REVERSE_COMMIT_ORDER** .

Impostare questa variabile di ambiente nell'ambiente da cui viene eseguito il **strmqm** per avviare il gestore code. Ad esempio, eseguire quanto segue nella shell appena prima di avviare il gestore code:

```
export AMQ_REVERSE_COMMIT_ORDER=1
```

Nota: L'impostazione di questa variabile di ambiente potrebbe causare una voce di log supplementare per transazione, quindi ciò avrà un piccolo impatto sulle prestazioni di ciascuna transazione.

Multi Coordinamento database

Quando il gestore code coordina le unità di lavoro globali, diventa possibile integrare gli aggiornamenti del database all'interno delle unità di lavoro. Ossia, è possibile scrivere un'applicazione MQI e SQL mista e utilizzare i verbi MQCMIT e MQBACK per eseguire il commit o il rollback delle modifiche alle code e ai database insieme.

Il gestore code ottiene questo risultato utilizzando il protocollo di commit a due fasi descritto in *X/Open Distributed Transaction Processing: The XA Specification*. Quando deve essere eseguito il commit di un'unità di lavoro, il gestore code chiede prima a ciascun gestore database partecipante se è pronto a eseguire il commit dei propri aggiornamenti. Solo se tutti i partecipanti, incluso il gestore code stesso, sono pronti per il commit, viene eseguito il commit di tutti gli aggiornamenti della coda e del database. Se un partecipante non può preparare gli aggiornamenti, viene eseguito il backout dell'unità di lavoro.

In generale, un'unità di lavoro globale viene implementata in un'applicazione con il seguente metodo (in pseudocodice):

```
MQBEGIN
MQGET (includere l'indicatore MQGMO_SYNCPOINT nelle opzioni del messaggio)
MQPUT (includere l'indicatore MQPMO_SYNCPOINT nelle opzioni del messaggio)
```

INSERT SQL
MQCMIT

Lo scopo di MQBEGIN è di indicare l'inizio di un'unità di lavoro globale. Lo scopo di MQCMIT è di indicare la fine dell'unità di lavoro globale e di completarla con tutti i gestori risorse partecipanti, utilizzando il protocollo di commit a due fasi.

Quando l'unità di lavoro (nota anche come *transazione*) è stato completato correttamente utilizzando MQCMIT, tutte le azioni intraprese all'interno di tale unità di lavoro sono rese permanenti o irreversibili. Se, per qualsiasi motivo, l'unità di lavoro ha esito negativo, tutte le azioni vengono invece ripristinate. Non è possibile rendere permanente un'azione in un'unità di lavoro, mentre ne viene ripristinata un'altra. Questo è il principio di un'unità di lavoro: o tutte le azioni all'interno dell'unità di lavoro sono rese permanenti o nessuna di esse lo è.

Nota:

1. Il programmatore dell'applicazione può forzare il ripristino di un'unità di lavoro richiamando MQBACK. L'unità di lavoro viene ripristinata dal gestore code anche se l'applicazione o il database *ha esito negativo* prima di richiamare MQCMIT.
2. Se un'applicazione richiama MQDISC senza richiamare MQCM, il gestore code si comporta come se MQCMIT fosse stato richiamato ed esegue il commit dell'unità di lavoro.

Tra MQBEGIN e MQCMIT, il gestore code non effettua alcuna chiamata al database per aggiornare le sue risorse. In altre parole, l'unico modo in cui le tabelle di un database vengono modificate è mediante il codice (ad esempio, SQL INSERT nello pseudocodice).

Il supporto di ripristino completo viene fornito se il gestore code perde il contatto con uno dei gestori database durante il protocollo di commit. Se un gestore database diventa non disponibile mentre è in dubbio, ovvero è stato preparato correttamente per il commit, ma deve ancora ricevere una decisione di commit o di backout, il gestore code ricorda il risultato dell'unità di lavoro fino a quando tale risultato non è stato consegnato correttamente al database. Allo stesso modo, se il gestore code termina con operazioni di commit incomplete in sospeso, tali operazioni vengono ricordate al riavvio del gestore code. Se un'applicazione termina in modo imprevisto, l'integrità dell'unità di lavoro non viene compromessa, ma il risultato dipende da dove nel processo l'applicazione è terminata, come descritto in Tabella 2 a pagina 54.

Ciò che accade quando il database o il programma applicativo ha esito negativo viene riepilogato nelle seguenti tabelle:

Tabella 1. Cosa accade quando un server di database ha esito negativo

Ricorrenza di errore	**Risultato**
Prima della chiamata dell'applicazione a MQCMIT.	L'unità di lavoro viene ripristinata.
Durante la chiamata dell'applicazione a MQCMIT, **prima** tutti i database hanno indicato che sono stati preparati correttamente.	Viene eseguito il backout dell'unità di lavoro con un codice motivo MQRC_BACKED_OUT.
Durante la chiamata dell'applicazione a MQCMIT, **dopo** tutti i database hanno indicato di aver preparato correttamente, ma prima di tutti hanno indicato di aver eseguito correttamente il commit.	L'unità di lavoro è conservata in uno stato ripristinabile dal gestore code, con un codice motivo MQRC_OUTCOME_PENDING.
Durante la chiamata dell'applicazione a MQCMIT, **dopo** che tutti i database hanno indicato di aver eseguito correttamente il commit.	L'unità di lavoro viene sottoposta a commit con un codice motivo MQRC_NONE.
Dopo la chiamata dell'applicazione a MQCMIT.	L'unità di lavoro viene sottoposta a commit con un codice motivo MQRC_NONE.

Tabella 2. Cosa succede quando un programma di applicazione ha esito negativo	
Ricorrenza di errore	**Risultato**
Prima della chiamata dell'applicazione a MQCMIT.	L'unità di lavoro viene ripristinata.
Durante la chiamata dell'applicazione a MQCMIT, **prima** che il gestore code abbia ricevuto la richiesta MQCMIT dell'applicazione.	L'unità di lavoro viene ripristinata.
Durante la chiamata dell'applicazione a MQCMIT, **dopo** che il gestore code ha ricevuto la richiesta MQCMIT dell'applicazione.	Il gestore code tenta di eseguire il commit utilizzando il commit a due fasi (in base al fatto che i prodotti database eseguano e eseguano correttamente il commit delle loro parti dell'unità di lavoro).

Nel caso in cui il codice motivo restituito da MQCMIT sia MQRC_OUTCOME_PENDING, l'unità di lavoro viene ricordata dal gestore code fino a quando non è stato in grado di ristabilire il contatto con il server di database e di eseguire il commit della sua parte dell'unità di lavoro. Fare riferimento a "Considerazioni quando si perde il contatto con il gestore risorse XA" a pagina 70 per informazioni su come e quando viene eseguito il ripristino.

Il gestore code comunica con i gestori database utilizzando l'interfaccia XA come descritto in *X/Open Distributed Transaction Processing: The XA Specification*. Esempi di queste chiamate di funzione sono xa_open, xa_start, xa_end, xa_prepare e xa_commit. Vengono utilizzati i termini *gestore transazioni* e *gestore risorse* nello stesso modo in cui vengono utilizzati nella specifica XA.

Multi *Limitazioni*

Esistono delle limitazioni al supporto di coordinamento del database.

Sono applicate le seguenti limitazioni:

- La capacità di coordinare gli aggiornamenti del database all'interno di IBM MQ unità di lavoro **non** è supportata in un'applicazione client MQI. L'utilizzo di MQBEGIN in un'applicazione client non riesce. Un programma che richiama MQBEGIN deve essere eseguito come applicazione *server* sulla stessa macchina del gestore code.

  Nota: Un'applicazione *server* è un programma che è stato collegato alle librerie del server IBM MQ necessarie; un'applicazione *client* è un programma che è stato collegato alle librerie del client IBM MQ necessarie. Consultare Creazione di applicazioni per IBM MQ MQI clients e Creazione di un'applicazione procedurale per dettagli sulla compilazione e il collegamento di programmi scritti in un linguaggio procedurale.
- Il server di database può risiedere su una macchina diversa dal server del gestore code, purché il client del database sia installato sulla stessa macchina del gestore code e supporti questa funzione. Consultare la documentazione del prodotto database per determinare se il software client può essere utilizzato per i sistemi di commit a due fasi.
- Sebbene il gestore code si comporti come un gestore risorse (per essere coinvolto nelle unità di lavoro globali dello Scenario 2), non è possibile fare in modo che un gestore code coordini un altro gestore code all'interno delle relative unità di lavoro globali dello Scenario 1.

Multi *File di caricamento switch*

Il file di caricamento switch è una libreria condivisa (una DLL su sistemi Windows) caricata dal codice nell'applicazione IBM MQ e dal gestore code. Il suo scopo è semplificare il caricamento della libreria condivisa del client del database e restituire i puntatori alle funzioni XA.

I dettagli del file di caricamento switch devono essere specificati prima dell'avvio del gestore code. I dettagli vengono inseriti nel file qm.ini sui sistemi AIX, Linux, and Windows .

- Su sistemi Windows e Linux (x86 e x86-64), utilizzare IBM MQ Explorer per aggiornare il file qm.ini .
- Su tutti gli altri sistemi modificare il file, qm.ini, direttamente.

L'origine C per il file di caricamento switch viene fornita con l'installazione di IBM MQ se supporta le unità di lavoro globali Scenario 1. L'origine contiene una funzione denominata MQStart. Quando il file di caricamento switch viene caricato, il gestore code richiama questa funzione, che restituisce l'indirizzo di una struttura denominata *switch XA*.

La struttura di commutazione XA esiste nella libreria condivisa del client del database e contiene una serie di puntatori di funzione, come descritto in Tabella 3 a pagina 55:

Tabella 3. Puntatori funzione switch XA

Nome puntatore funzione	**funzione XA**	**Finalità**
xa_open_entry	xa_open	Connetti al database
xa_close_entry	xa_close	Disconnetti dal database
xa_start_entry	xa_start	Avviare un ramo di un'unità di lavoro globale
xa_end_entry	xa_end	Sospende un ramo di un'unità di lavoro globale
xa_rollback_entry	xa_rollback	Eseguire il rollback di un ramo di un'unità di lavoro globale
xa_prepare_entry	xa_prepare	Preparazione al commit di un ramo di un'unità di lavoro globale
xa_commit_entry	xa_commit	Eseguire il commit di un ramo di un'unità di lavoro globale
xa_recover_entry	xa_recover	Scopri dal database se ha un'unità di lavoro in dubbio
xa_forget_entry	xa_forget	Consente a un database di dimenticare un ramo di un'unità di lavoro globale
xa_complete_entry	xa_complete	Completare un ramo di un'unità di lavoro globale

Durante la prima chiamata MQBEGIN nell'applicazione, il codice IBM MQ che viene eseguito come parte di MQBEGIN carica il file di caricamento switch e richiama la funzione xa_open nella libreria condivisa del database. Allo stesso modo, durante l'avvio del gestore code e in altre successive occasioni, alcuni processi del gestore code caricano il file di caricamento switch e richiamano xa_open.

È possibile ridurre il numero di chiamate xa_ * utilizzando la *registrazione dinamica*. Per una descrizione completa di questa tecnica di ottimizzazione, consultare “Registrazione dinamica XA” a pagina 74.

Multi *Configurazione del sistema per il coordinamento del database*

È necessario eseguire diverse attività prima che un gestore database possa partecipare a unità globali di lavori coordinate dal gestore code. Questi sono descritti qui di seguito:

- “Installazione e configurazione del database” a pagina 56
- “Creazione di file di caricamento switch” a pagina 56
- “Aggiunta di informazioni di configurazione al gestore code” a pagina 57
- “Scrittura e modifica delle applicazioni” a pagina 59
- “Verifica del sistema” a pagina 59

Multi *Installazione e configurazione del database*
Per installare e configurare il prodotto database, consultare la documentazione del prodotto. Questi argomenti in questa sezione descrivono i problemi di configurazione generali e il modo in cui sono correlati all'interoperabilità tra IBM MQ e il database.

Connessioni database

Un'applicazione che stabilisce una connessione standard al gestore code è associata a un thread in un processo dell'agent del gestore code locale separato. Una connessione che non è una connessione *fastpath* è una connessione *standard* in questo contesto. Consultare Connessione a un gestore code mediante la chiamata MQCONNX.)

Quando l'applicazione emette **MQBEGIN**, sia il processo agent che il processo richiamano la funzione **xa_open** nella libreria del client database. In risposta a ciò, il codice della libreria client database *connette* al database che deve essere coinvolto nell'unità di lavoro *sia dall'applicazione che dai processi del gestore code*. Queste connessioni al database vengono mantenute finché l'applicazione rimane connessa al gestore code.

Si tratta di una considerazione importante se il database supporta solo un numero limitato di utenti o connessioni, poiché vengono effettuate due connessioni al database per supportare l'unico programma applicativo.

Configurazione client/server

La libreria del client del database caricata nel IBM MQ gestore code e nei processi dell'applicazione **deve** essere in grado di inviare e ricevere dal server. Accertarsi che:

- I file di configurazione client/server del database hanno i dettagli corretti
- Le variabili di ambiente pertinenti sono impostate nell'ambiente del gestore code **e** i processi dell'applicazione

Multi *Creazione di file di caricamento switch*
IBM MQ viene fornito con un makefile di esempio, utilizzato per creare file di caricamento switch per i gestori database supportati.

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

Il makefile di esempio, insieme a tutti i file di origine C associati richiesti per creare i file di caricamento switch, viene installato nelle seguenti directory:

- Per IBM MQ for Windows, nella directory *MQ_INSTALLATION_PATH*`\tools\c\samples\xatm\`
- Per sistemi IBM MQ for UNIX e Linux , nella directory *MQ_INSTALLATION_PATH*`/samp/xatm/`

Le destinazioni di esempio utilizzate per creare i file di caricamento switch sono:

- Per Db2, db2swit.
- Per Oracle, oraswit
- Per Informix, infswit
- Per Sybase, sybswit

Windows Il file switch generato viene inserito in `C:\Program Files\IBM\MQ\exits`.

Linux UNIX Se si dispone di gestori code a 32 bit, il file make di esempio, xaswit.mak, installa un file di caricamento switch a 32 bit in `/var/mqm/exits`.

Linux UNIX Se si dispone di gestori code a 64 bit, il file make di esempio, xaswit.mak, installa un file di caricamento switch a 32 bit in `/var/mqm/exitse` un file di caricamento switch a 64 bit in `/var/mqm/exits64`.

Linux UNIX Se il sistema non supporta la compilazione a 32 bit, utilizzare solo la destinazione a 64 bit per il database:

- Per Db2, db2swit64
- Per Oracle, oraswit64
- Per Informix, infswit64
- Per Sybase, sybswit64

Sicurezza file

È possibile che il proprio sistema operativo non riesca a caricare il file di caricamento switch da IBM MQ, per motivi esterni al controllo di IBM MQ. Se ciò si verifica, i messaggi di errore vengono scritti nei log di errore IBM MQ e potenzialmente la chiamata MQBEGIN potrebbe non riuscire. Per garantire che il sistema operativo non abbia esito negativo nel caricamento del file di caricamento switch, è necessario soddisfare i seguenti requisiti:

1. Il file di caricamento switch deve essere disponibile nell'ubicazione fornita nel file qm.ini .
2. Il file di caricamento switch deve essere accessibile a tutti i processi che devono caricarlo, inclusi i processi del gestore code e i processi dell'applicazione.
3. Tutte le librerie da cui dipende il file di caricamento switch, incluse le librerie fornite dal database, devono essere presenti e accessibili.

Multi *Aggiunta di informazioni di configurazione al gestore code*

Una volta creato un file di caricamento switch per il gestore database e collocato in un percorso sicuro, è necessario specificare tale ubicazione per il gestore code.

Per specificare l'ubicazione, effettuare quanto segue:

- Su sistemi Windows e Linux (x86 e x86-64), utilizzare IBM MQ Explorer. Specificare i dettagli del file di caricamento switch nel pannello delle proprietà del gestore code, nel gestore risorse XA.
- Su tutti gli altri sistemi specificare i dettagli del file di caricamento switch nella stanza XAResourceManager nel file qm.ini del gestore code.

Aggiungere una sezione XAResourceManager per il database che verrà coordinato dal gestore code. Il caso più comune è che ci sia solo un database e quindi solo una stanza XAResourceManager . Per i dettagli delle configurazioni più complicate che coinvolgono più database, consultare “Configurazioni di più database” a pagina 69. Gli attributi della stanza XAResourceManager sono i seguenti:

Nome=nome

Stringa scelta dall'utente che identifica il gestore risorse. In effetti, fornisce un nome alla stanza XAResourceManager . Il nome è obbligatorio e può avere una lunghezza massima di 31 caratteri.

Il nome scelto deve essere univoco; deve esistere solo una stanza XAResourceManager con questo nome in questo file qm.ini . Anche il nome deve essere significativo, poiché il gestore code lo utilizza per fare riferimento a questo gestore risorse sia nei messaggi di log degli errori del gestore code che nell'output quando viene utilizzato il comando `dspmqtrn` . (Per ulteriori informazioni, consultare “Visualizzazione delle unità di lavoro in sospeso con il comando dspmqtrn” a pagina 71 .)

Una volta scelto un nome e avviato il gestore code, non modificare l'attributo Nome. Per ulteriori dettagli sulla modifica delle informazioni di configurazione, consultare “Modifica delle informazioni di configurazione” a pagina 73.

SwitchFile= nome

Questo è il nome del file di caricamento switch XA creato in precedenza. Questo è un attributo obbligatorio. Il codice nel gestore code e nei processi dell'applicazione IBM MQ tenta di caricare il file di caricamento switch in due occasioni:

1. All'avvio del gestore code
2. Quando si effettua la prima chiamata a MQBEGIN nel processo dell'applicazione IBM MQ

Gli attributi di sicurezza e di autorizzazioni del file di caricamento switch devono consentire a questi processi di eseguire questa azione.

XAOpenString= stringa
Si tratta di una stringa di dati che il codice IBM MQ trasmette nelle chiamate alla funzione xa_open del gestore database. Questo è un attributo facoltativo; se viene omesso, viene utilizzata una stringa di lunghezza zero.

Il codice nel gestore code e nei processi dell'applicazione IBM MQ richiama la funzione xa_open in due occasioni:

1. All'avvio del gestore code
2. Quando si effettua la prima chiamata a MQBEGIN nel processo dell'applicazione IBM MQ

Il formato per questa stringa è particolare per ogni prodotto database e verrà descritto nella relativa documentazione. In generale, la stringa xa_open contiene le informazioni di autenticazione (nome utente e password) per consentire una connessione al database sia nel gestore code che nei processi dell'applicazione.

Da IBM MQ 8.0.0 Fix Pack 4, quando XAOpenString contiene una password, è possibile ottenere IBM MQ per proteggere tali informazioni, anziché avere la password visibile in testo semplice nel file `qm.ini` . IBM MQ memorizza il nome utente e la password (in formato codificato) in un file differente e utilizza queste credenziali per connettersi al database. Per i dettagli, consultare Protezione dei dettagli di autenticazione del database.

XACloseString= stringa
Si tratta di una stringa di dati che il codice IBM MQ trasmette alle chiamate alla funzione xa_close del gestore database. Questo è un attributo facoltativo; se viene omesso, viene utilizzata una stringa di lunghezza zero.

Il codice nel gestore code e i processi dell'applicazione IBM MQ richiamano la funzione xa_close in due occasioni:

1. All'avvio del gestore code
2. Quando si effettua una chiamata a MQDISC nel proprio processo dell'applicazione IBM MQ , dopo aver precedentemente effettuato una chiamata a MQBEGIN

Il formato per questa stringa è particolare per ogni prodotto database e verrà descritto nella relativa documentazione. In generale, la stringa è vuota ed è comune omettere l'attributo XACloseString dalla stanza XAResourceManager .

ThreadOfControl=THREAD |PROCESS (predefinito)
Il valore di controllo ThreadOfpuò essere THREAD o PROCESS. Il gestore code lo utilizza per scopi di serializzazione. Questo è un attributo facoltativo; se viene omesso, viene utilizzato il valore PROCESS.

Se il codice client del database consente ai thread di richiamare le funzioni XA senza serializzazione, il valore per il controllo ThreadOfpuò essere THREAD. Il gestore code presuppone che possa richiamare le funzioni XA nella libreria condivisa del client del database da più thread contemporaneamente, se necessario.

Se il codice client del database non consente ai thread di richiamare le funzioni XA in questo modo, il valore per ThreadOfControl deve essere PROCESS. In questo caso, il gestore code serializza tutte le chiamate alla libreria condivisa del client database in modo che venga effettuata una sola chiamata alla volta dall'interno di un determinato processo. È anche necessario assicurarsi che l'applicazione esegua una serializzazione simile se viene eseguita con più thread.

Si noti che questo problema, relativo alla capacità del prodotto database di gestire in questo modo i processi a più thread, è un problema per il fornitore del prodotto. Consultare la documentazione del prodotto database per i dettagli su come impostare l'attributo di controllo ThreadOfsu THREAD o PROCESS. Si consiglia, se possibile, di impostare il controllo ThreadOfsu THREAD. In caso di dubbio, l'opzione *safer* consiste nell'impostarla su PROCESS, anche se si perderanno i potenziali vantaggi di prestazioni dell'utilizzo di THREAD.

Multi *Scrittura e modifica delle applicazioni*

Come implementare un'unità di lavoro globale.

I programmi applicativi di esempio per le unità di lavoro globali Scenario 1 forniti con un'installazione IBM MQ sono descritti in “Introduzione delle unità di lavoro” a pagina 50.

In generale, un'unità di lavoro globale viene implementata in un'applicazione con il seguente metodo (in pseudocodice):

```
MQBEGIN
MQGET
MQPUT
Inserimento SQL
MQCMIT
```

Lo scopo di MQBEGIN è di indicare l'inizio di un'unità di lavoro globale. Lo scopo di MQCMIT è di indicare la fine dell'unità di lavoro globale e di completarla con tutti i gestori risorse partecipanti, utilizzando il protocollo di commit a due fasi.

Tra MQBEGIN e MQCMIT, il gestore code non effettua alcuna chiamata al database per aggiornare le sue risorse. In altre parole, l'unico modo in cui le tabelle di un database vengono modificate è mediante il codice (ad esempio, SQL INSERT nello pseudocodice).

Il ruolo del gestore code, per quanto riguarda il database, è quello di indicare quando è stata avviata un'unità di lavoro globale, quando è stata terminata e se è necessario eseguire il commit o il rollback dell'unità di lavoro globale.

Per quanto riguarda l'applicazione, il gestore code esegue due ruoli: un gestore risorse (dove le risorse sono messaggi sulle code) e il gestore transazioni per l'unità di lavoro globale.

Iniziare con i programmi di esempio forniti e utilizzare le varie chiamate API IBM MQ e database effettuate in tali programmi. Le chiamate API in questione sono completamente documentate in Using the sample procedural programs for Multiplatforms, Data types used in the MQI e (nel caso delle API del database) nella documentazione del database stesso.

Multi *Verifica del sistema*

L'utente sa se l'applicazione e il sistema sono configurati correttamente solo eseguendoli durante il test. È possibile verificare la configurazione del sistema (la comunicazione corretta tra il gestore code e il database) creando ed eseguendo un programma di esempio fornito.

Multi Configurazione di Db2

Informazioni di supporto e configurazione di Db2 .

I livelli supportati di Db2 sono definiti nella pagina Requisiti di sistema per 'IBM MQ .

Nota: Le istanze a 32 bit di Db2 non sono supportate su piattaforme in cui il gestore code è a 64 bit.

Eseguire quanto segue:

1. Controllare le impostazioni della variabile di ambiente.
2. Creare il file di caricamento switch Db2 .
3. Aggiungere le informazioni di configurazione del gestore risorse.
4. Modificare i parametri di configurazione Db2 , se necessario.

Leggere queste informazioni insieme alle informazioni generali fornite in “Configurazione del sistema per il coordinamento del database” a pagina 55.

Avviso: Se si esegue `db2profile` su piattaforme AIX and Linux , vengono impostate le variabili di ambiente LIBPATH e LD_LIBRARY_PATH. È consigliabile `unset` queste variabili di ambiente. Per ulteriori informazioni, consultare crtmqenv o setmqenv .

Verifica delle impostazioni della variabile d'ambiente Db2

Assicurarsi che le variabili di ambiente Db2 siano impostate per i processi del gestore code ***e in*** per i processi dell'applicazione. In particolare, è necessario impostare sempre la Db2variabile di ambiente INSTANCE ***prima di*** avviare il gestore code. La variabile di ambiente DB2INSTANCE identifica l'istanza Db2 contenente i database Db2 in fase di aggiornamento. Ad esempio:

- Su sistemi AIX and Linux , utilizzare:

```
export DB2INSTANCE=db2inst1
```

- Su sistemi Windows , utilizzare:

```
set DB2INSTANCE=DB2"/>
```

Su Windows con database Db2 , è necessario aggiungere l'utente MUSR_MQADMIN al gruppo DB2USERS , per consentire l'avvio del gestore code.

Creazione del file di caricamento switch Db2

Il modo più semplice per creare il Db2 file di caricamento switch è utilizzare il file di esempio xaswit.mak, che IBM MQ fornisce per creare i file di caricamento switch per una varietà di prodotti database.

Su sistemi Windows , è possibile trovare `xaswit.mak` nella directory *MQ_INSTALLATION_PATH*`\tools\c\samples\xatm`. *MQ_INSTALLATION_PATH* rappresenta la directory di livello superiore in cui è installato IBM MQ . Per creare il file di caricamento switch Db2 con Microsoft Visual C + +, utilizzare:

```
nmake /f xaswit.mak db2swit.dll
```

Il file switch generato viene inserito in `C:\Program Files\IBM\MQ\exits`.

È possibile trovare `xaswit.mak` nella directory *MQ_INSTALLATION_PATH*`/samp/xatm`. *MQ_INSTALLATION_PATH* rappresenta la directory di livello superiore in cui è installato IBM MQ .

Modificare `xaswit.mak` per *eliminare il commento* delle righe appropriate alla versione di Db2 che si sta utilizzando. Quindi, eseguire il makefile utilizzando il comando:

```
make -f xaswit.mak db2swit
```

Il file di caricamento switch a 32 bit generato viene inserito in `/var/mqm/exits`.

Il file di caricamento dello switch a 64 bit generato si trova in `/var/mqm/exits64`.

Se il sistema non supporta la compilazione a 32 bit, utilizzare solo la destinazione a 64 bit:

```
make -f xaswit.mak db2swit64
```

Aggiunta delle informazioni di configurazione del gestore risorse per Db2

È necessario modificare le informazioni di configurazione per il gestore code per dichiarare Db2 come partecipante nelle unità di lavoro globali. La modifica delle informazioni di configurazione in questo modo è descritta più dettagliatamente in “Aggiunta di informazioni di configurazione al gestore code” a pagina 57.

- Su sistemi Windows e Linux (x86 e x86-64), utilizzare IBM MQ Explorer. Specificare i dettagli del file di caricamento switch nel pannello delle proprietà del gestore code, nel gestore risorse XA.
- Su tutti gli altri sistemi specificare i dettagli del file di caricamento switch nella stanza XAResourceManager nel file qm.ini del gestore code.

Figura 6 a pagina 61 è un esempio UNIX che mostra una voce XAResourceManager in cui il database da coordinare è denominato mydbname, questo nome è specificato in XAOpenString:

```
XAResourceManager:
  Name=mydb2
  SwitchFile=db2swit
  XAOpenString=mydbname,myuser,mypasswd,toc=t
  ThreadOfControl=THREAD
```

Figura 6. Voce XAResourceManager di esempio per Db2 su UNIX

Nota:

1. ThreadOfControl=THREAD non può essere utilizzato con versioni Db2 precedenti alla 8. Impostare ThreadOfControl e il parametro XAOpenString toc su una delle seguenti combinazioni:
   - ThreadOfControl=THREAD e toc=t
   - ThreadOfControl=PROCESS e toc=p

   Se si utilizza il file di caricamento switch XA jdbcdb2 per abilitare il coordinamento JDBC/JTA, è necessario utilizzare ThreadOfControl=PROCESS e toc=p.

Modifica dei parametri di configurazione Db2

Per ogni database Db2 che il gestore code sta coordinando, è necessario impostare i privilegi del database, modificare il parametro tp_mon_name e reimpostare il parametro maxappls. A tal fine, effettuare i seguenti passi:

Imposta privilegi database

I processi del gestore code vengono eseguiti con mqm utente e gruppo effettivi sui sistemi AIX and Linux . Su sistemi Windows , vengono eseguiti come utente che ha avviato il gestore code. Può essere uno dei seguenti:

1. L'utente che ha immesso il comando strmqm oppure
2. L'utente con cui viene eseguito il server COM del servizio IBM MQ

Per impostazione predefinita, questo utente è denominato MUSR_MQADMIN.

Se non sono stati specificati un nome utente e una password nella stringa xa_open, **l'utente con cui è in esecuzione il gestore code** viene utilizzato da Db2 per autenticare la chiamata xa_open. Se questo utente (ad esempio, l'utente mqm sui sistemi AIX and Linux) non dispone di privilegi minimi nel database, il database rifiuta di autenticare la chiamata xa_open.

Le stesse considerazioni si applicano al processo di applicazione. Se non sono stati specificati un nome utente e una password sulla stringa xa_open, l'utente con cui è in esecuzione l'applicazione viene utilizzato da Db2 per autenticare la chiamata xa_open effettuata durante il primo MQBEGIN. Ancora una volta, questo utente deve disporre di privilegi minimi nel database per funzionare.

Ad esempio, fornire all'utente mqm l'autorizzazione di collegamento nel database mydbname immettendo i comandi Db2 riportati di seguito:

```
db2 connect to mydbname
db2 grant connect on database to user mqm
```

Consultare “Considerazioni sulla sicurezza” a pagina 70 per ulteriori informazioni sulla sicurezza.

Windows **Modificare il parametro TP_MON_NAME**

Solo per i sistemi Db2 su Windows , modificare il parametro di configurazione TP_MON_NAME per denominare la DLL utilizzata da Db2 per richiamare il gestore code per la registrazione dinamica.

Utilizzare il comando `db2 update dbm cfg using TP_MON_NAME mqmax` per denominare MQMAX.DLL come libreria utilizzata da Db2 per richiamare il gestore code. Deve essere presente in una directory all'interno di PATH.

Reimpostare il parametro maxappls
Potrebbe essere necessario rivedere l'impostazione per il parametro *maxappls* , che limita il numero massimo di applicazioni che possono essere connesse a un database. Fare riferimento a “Installazione e configurazione del database” a pagina 56.

Multi Configurazione di Oracle

Informazioni di configurazione e supporto Oracle .

Completare i seguenti passi:

1. Controllare le impostazioni della variabile di ambiente.
2. Creare il file di caricamento switch Oracle .
3. Aggiungere le informazioni di configurazione del gestore risorse.
4. Modificare i parametri di configurazione di Oracle , se necessario.

Per un elenco corrente dei livelli di Oracle supportati da IBM MQ, consultare Requisiti di sistema per 'IBM MQ.

Verifica delle impostazioni delle variabili di ambiente Oracle

Verificare che le variabili di ambiente Oracle siano impostate per i processi del gestore code e per i processi dell'applicazione. In particolare, impostare sempre le seguenti variabili di ambiente prima di avviare il gestore code:

ORACLE_HOME
La directory home Oracle . Ad esempio, su sistemi AIX and Linux , utilizzare:

```
export ORACLE_HOME=/opt/oracle/product/8.1.6
```

Su sistemi Windows , utilizzare:

```
set ORACLE_HOME=c:\oracle\ora81
```

ORACLE_SID
Il SID Oracle utilizzato. Se si utilizza Net8 per la connettività client/server, potrebbe non essere necessario impostare questa variabile di ambiente. Consultare la documentazione Oracle .

L'esempio successivo è un esempio di impostazione di questa variabile di ambiente, su sistemi AIX and Linux :

```
export ORACLE_SID=sid1
```

L'equivalente sui sistemi Windows è:

```
set ORACLE_SID=sid1
```

Nota: La variabile di ambiente PATH deve essere impostata in modo da includere la directory dei file binari (ad esempio, `ORACLE_INSTALL_DIR/VERSION/32BIT_NAME/bin` o `ORACLE_INSTALL_DIR/VERSION/64BIT_NAME/bin`), altrimenti potrebbe essere visualizzato un messaggio che indica che le librerie oraclient mancano dalla macchina.

Se si eseguono gestori code su sistemi Windows a 64 bit, è necessario installare solo client Oracle a 64 bit. Il file di caricamento degli switch, caricato dai gestori code a 64 bit, deve accedere alle librerie client a 64 bit Oracle .

Creazione del file di caricamento switch Oracle

Per creare il file di caricamento switch Oracle , utilizzare il file di esempio `xaswit.mak`, fornito da IBM MQ per creare i file di caricamento switch per diversi prodotti database.

Windows Su sistemi Windows , è possibile trovare `xaswit.mak` nella directory `C:\Program Files\IBM\MQ\tools\c\samples\xatm`. Per creare il file di caricamento switch Oracle con Microsoft Visual C + +, utilizzare:

```
nmake /f xaswit.mak oraswit.dll
```

Nota: Questi file di caricamento switch possono essere utilizzati solo con applicazioni C. Per le applicazioni Java , consultare il coordinamento JTA/JDBC utilizzando IBM MQ classes for Java.

Il file switch generato viene inserito in *MQ_INSTALLATION_PATH*`\exits`. *MQ_INSTALLATION_PATH* rappresenta la directory di livello superiore in cui è installato IBM MQ .

Linux UNIX È possibile trovare `xaswit.mak` nella directory *MQ_INSTALLATION_PATH*`/samp/xatm`. *MQ_INSTALLATION_PATH* rappresenta la directory di livello superiore in cui è installato IBM MQ .

Modificare `xaswit.mak` per eliminare il commento dalle righe appropriate alla versione di Oracle che si sta utilizzando. Quindi, eseguire il makefile utilizzando il comando:

```
make -f xaswit.mak oraswit
```

Il contenuto di `MQ_INSTALLATION_PATH/samp/xatm` è di sola lettura quando IBM MQ è installato, in modo da modificare `xaswit.mak`, copiare tutti i file da `samp/xatm` in un'altra directory, modificare `xaswit.mak`ed eseguire `make -f xaswit.mak`o`raswit` da tale directory.

Il file di caricamento dello switch a 32 bit generato si trova in `/var/mqm/exits`.

Il file di caricamento switch a 64 bit generato viene collocato in `/var/mqm/exits64`.

Se il sistema non supporta la compilazione a 32 bit, utilizzare solo la destinazione a 64 bit:

```
make -f xaswit.mak oraswit64
```

Aggiunta delle informazioni di configurazione del gestore risorse per Oracle

È necessario modificare le informazioni di configurazione per il gestore code per dichiarare Oracle come partecipante alle unità di lavoro globali. La modifica delle informazioni di configurazione per il gestore code in questo modo viene descritta più dettagliatamente in “Aggiunta di informazioni di configurazione al gestore code” a pagina 57.

- Su sistemi Windows e Linux (x86 e x86-64), utilizzare IBM MQ Explorer. Specificare i dettagli del file di caricamento switch nel pannello delle proprietà del gestore code, nel gestore risorse XA.
- Su tutti gli altri sistemi specificare i dettagli del file di caricamento switch nella stanza XAResourceManager del file `qm.ini` del gestore code.

Figura 7 a pagina 63 è un esempio di sistemi AIX and Linux che mostra una voce XAResourceManager . È necessario aggiungere un `LogDir` alla stringa di apertura XA in modo che tutte le informazioni di errore e traccia vengano registrate nello stesso luogo.

```
XAResourceManager:
  Name=myoracle
  SwitchFile=oraswit
  XAOpenString=Oracle_XA+Acc=P/myuser/mypasswd+SesTm=35+LogDir=/tmp+threads=true
  ThreadOfControl=THREAD
```

Figura 7. Voce XAResourceManager di esempio per Oracle su piattaforme AIX and Linux

Nota:

1. In Figura 7 a pagina 63, la stringa xa_open è stata utilizzata con quattro parametri. Ulteriori parametri possono essere inclusi come descritto nella documentazione di Oracle.
2. Quando si utilizza il parametro IBM MQ `ThreadOfControl=THREAD` , è necessario utilizzare il parametro Oracle `+threads=true` nella stanza XAResourceManager .

Consultare *Oracle8 Server Application Developer's Guide* per ulteriori informazioni sulla stringa xa_open.

Modifica dei parametri di configurazione di Oracle

Per ogni database Oracle coordinato dal gestore code, è necessario esaminare il numero massimo di sessioni e impostare i privilegi del database. A tale scopo, effettuare le seguenti operazioni:

Esaminare il numero massimo di sessioni
Potrebbe essere necessario esaminare le impostazioni LICENSE_MAX_SESSIONS e PROCESSES per prendere in considerazione le connessioni aggiuntive richieste dai processi appartenenti al gestore code. Consultare “Installazione e configurazione del database” a pagina 56 per maggiori dettagli.

Imposta privilegi database
Il nome utente Oracle specificato nella stringa xa_open deve disporre dei privilegi per accedere alla vista DBA_PENDING_TRANSACTIONS, come descritto nella documentazione Oracle .

Il privilegio necessario può essere fornito utilizzando il seguente comando di esempio:

```
grant select on DBA_PENDING_TRANSACTIONS to myuser;
```

Multi Configurazione di Informix

Informazioni di supporto e configurazione di Informix .

Completare i seguenti passi:

1. Assicurarsi di aver installato l'SDK client Informix appropriato:
   - Le applicazioni e i gestori code a 32 bit richiedono un SDK client Informix a 32 bit.
   - Le applicazioni e i gestori code a 64 bit richiedono un SDK client Informix a 64 bit.
2. Verificare che i database Informix vengano creati correttamente.
3. Controllare le impostazioni della variabile di ambiente.
4. Creare il file di caricamento switch Informix .
5. Aggiungere le informazioni di configurazione del gestore risorse.

Per un elenco corrente di livelli di Informix supportati da IBM MQ, consultare Requisiti di sistema per 'IBM MQ.

Verifica della creazione corretta dei database Informix

Ogni database Informix che deve essere coordinato da un gestore code IBM MQ deve essere creato specificando il parametro **`log`** . Ad esempio:

```
create database mydbname with log;
```

I gestori code IBM MQ non sono in grado di coordinare i database Informix che non dispongono del parametro `log` specificato durante la creazione. Se un gestore code tenta di coordinare un database Informix che non ha il parametro `log` specificato durante la creazione, la chiamata xa_open a Informix ha esito negativo e viene generato un numero di errori FFST .

Verifica delle impostazioni della variabile d'ambiente Informix

Assicurarsi che le variabili di ambiente Informix siano impostate per i processi del gestore code ***e in*** per i processi dell'applicazione. In particolare, impostare sempre le seguenti variabili di ambiente **prima** di avviare il gestore code:

INFORMIXDIR
La directory di installazione di Informix .

- Per le applicazioni AIX and Linux a 32 bit, utilizzare i seguenti comandi:

```
export INFORMIXDIR=/opt/informix/32-bit
```

- Per le applicazioni AIX and Linux a 64 bit, utilizzare il seguente comando:

```
export INFORMIXDIR=/opt/informix/64-bit
```

- Per le applicazioni Windows , utilizzare i seguenti comandi:

```
set INFORMIXDIR=c:\informix
```

Per i sistemi con gestori code a 64 bit che devono supportare applicazioni a 32 bit e a 64 bit, è necessario che siano installati sia gli SDK client a 32 bit Informix che a 64 bit. Il makefile di esempio `xaswit.mak`, utilizzato per la creazione di un file di caricamento switch, imposta anche entrambe le directory di installazione del prodotto.

SERVER INFORMIX
Il nome del server Informix . Ad esempio, su sistemi AIX and Linux , utilizzare:

```
export INFORMIXSERVER=hostname_1
```

Su sistemi Windows , utilizzare:

```
set INFORMIXSERVER=hostname_1
```

ONCONFIG
Il nome del file di configurazione del server Informix . Ad esempio, su sistemi AIX and Linux , utilizzare:

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

Su sistemi Windows , utilizzare:

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

Creazione del file di caricamento switch Informix

Per creare il file di caricamento switch Informix , utilizzare il file di esempio xaswit.mak, fornito da IBM MQ per creare i file di caricamento switch per vari prodotti database.

Windows Sui sistemi Windows , è possibile trovare xaswit.mak nella directory *MQ_INSTALLATION_PATH*`\tools\c\samples\xatm`. *MQ_INSTALLATION_PATH* rappresenta la directory di livello superiore in cui è installato IBM MQ . Per creare il file di caricamento switch Informix con Microsoft Visual C + +, utilizzare:

```
nmake /f xaswit.mak infswit.dll
```

Il file switch generato viene inserito in `C:\Program Files\IBM\MQ\exits`.

Linux UNIX È possibile trovare xaswit.mak nella directory *MQ_INSTALLATION_PATH*`/samp/xatm`. *MQ_INSTALLATION_PATH* rappresenta la directory di livello superiore in cui è installato IBM MQ .

Modificare xaswit.mak per *rimuovere il commento* dalle righe appropriate alla versione di Informix che si sta utilizzando. Quindi, eseguire il makefile utilizzando il comando:

```
make -f xaswit.mak infswit
```

Il file di caricamento dello switch a 32 bit generato si trova in `/var/mqm/exits`.

Il file di caricamento switch a 64 bit generato viene collocato in `/var/mqm/exits64`.

Se il sistema non supporta la compilazione a 32 bit, utilizzare solo la destinazione a 64 bit:

```
make -f xaswit.mak infswit64
```

Aggiunta delle informazioni di configurazione del gestore risorse per Informix

È necessario modificare le informazioni di configurazione per il gestore code per dichiarare Informix come partecipante nelle unità di lavoro globali. La modifica delle informazioni di configurazione per il gestore code in questo modo viene descritta più dettagliatamente in "Aggiunta di informazioni di configurazione al gestore code" a pagina 57.

- Sui sistemi Windows e Linux (x86 e x86-64), utilizzare IBM MQ Explorer. Specificare i dettagli del file di caricamento switch nel pannello delle proprietà del gestore code, nel gestore risorse XA.
- Su tutti gli altri sistemi specificare i dettagli del file di caricamento switch nella stanza XAResourceManager del file qm.ini del gestore code.

Figura 8 a pagina 66 è un esempio UNIX , che mostra una voce qm.ini XAResourceManager in cui il database da coordinare è denominato `mydbname`, questo nome è specificato in `XAOpenString`:

```
XAResourceManager:
  Name=myinformix
  SwitchFile=infswit
  XAOpenString=DB=mydbname@myinformixserver\;USER=myuser\;PASSWD=mypasswd
  ThreadOfControl=THREAD
```

Figura 8. Voce XAResourceManager di esempio per Informix su UNIX

Nota: Per impostazione predefinita, l'esempio xaswit.mak su UNIX crea un file di caricamento switch che utilizza librerie Informix con thread. È necessario assicurarsi che ThreadOfControl sia impostato su THREAD quando si utilizzano queste librerie 'Informix. In ' Figura 8 a pagina 66, l'attributo ThreadOfControl del file qm.ini XAResourceManager è impostato su THREAD. Quando viene specificato THREAD, le applicazioni devono essere create utilizzando le librerie Informix con thread e le librerie API con thread IBM MQ .

L'attributo XAOpenString deve contenere il nome del database, seguito dal simbolo @ e seguito dal nome del server Informix .

Per utilizzare le librerie non filtrate " Informix, è necessario assicurarsi che l'attributo ThreadOfControl del file qm.ini XAResourceManager sia impostato su PROCESS. È inoltre necessario apportare le modifiche riportate di seguito all'esempio xaswit.mak:

1. Eliminare il commento dalla generazione di un file di caricamento switch senza thread.
2. Impostare come commento la generazione del file di caricamento switch con thread.

Multi Configurazione Sybase

Informazioni di supporto e configurazione Sybase .

Completare i seguenti passi:

1. Assicurarsi di aver installato le librerie XA Sybase , ad esempio installando l'opzione XA DTM.
2. Controllare le impostazioni della variabile di ambiente.

3. Abilitare il supporto XA Sybase
4. Creare il file di caricamento switch Sybase .
5. Aggiungere le informazioni di configurazione del gestore risorse.

Per un elenco corrente dei livelli Sybase supportati da IBM MQ, consultare Requisiti di sistema per 'IBM MQ.

Verifica delle impostazioni delle variabili di ambiente Sybase

Accertarsi che le variabili di ambiente Sybase siano impostate per i processi del gestore code e per i processi dell'applicazione. In particolare, impostare sempre le seguenti variabili di ambiente prima di avviare il gestore code:

Sybase

Linux AIX L'ubicazione dell'installazione del prodotto Sybase . Ad esempio, su sistemi AIX and Linux , utilizzare:

```
export SYBASE=/sybase
```

Windows Su sistemi Windows , utilizzare:

```
set SYBASE=c:\sybase
```

SYBASE_OCS

La directory in SYBASE in cui sono installati i file client Sybase .

Linux AIX Ad esempio, su sistemi AIX and Linux , utilizzare:

```
export SYBASE_OCS=OCS-12_0
```

Windows Su sistemi Windows , utilizzare:

```
set SYBASE_OCS=OCS-12_0
```

Abilitazione del supporto XA Sybase

All'interno del Sybase file di configurazione XA $SYBASE/$SYBASE_OCS/xa_config, definire un LRM (Logical Resource Manager) per ogni connessione al server Sybase in fase di aggiornamento. Di seguito è riportato un esempio del contenuto di $SYBASE/$SYBASE_OCS/xa_config:

```
# The first line must always be a comment

[xa]

  LRM=lrmname
  server=servername
```

Creazione del file di caricamento switch Sybase

Per creare il file di caricamento switch Sybase , utilizzare i file di esempio forniti con IBM MQ.

Windows Su sistemi Windows , è possibile trovare xaswit.mak nella directory C:\Program Files\IBM\MQ\tools\c\samples\xatm. Per creare il file di caricamento switch Sybase con Microsoft Visual C + +, utilizzare:

```
nmake /f xaswit.mak sybswit.dll
```

Il file switch generato viene inserito in C:\Program Files\IBM\MQ\exits.

Linux UNIX È possibile trovare `xaswit.mak` nella directory *MQ_INSTALLATION_PATH*`/samp/xatm`. *MQ_INSTALLATION_PATH* rappresenta la directory di livello superiore in cui è installato IBM MQ .

Modificare `xaswit.mak` per *eliminare il commento* delle righe appropriate alla versione di Sybase che si sta utilizzando. Quindi, eseguire il makefile utilizzando il comando:

```
make -f xaswit.mak sybswit
```

Il file di caricamento switch a 32 bit generato viene inserito in `/var/mqm/exits`.

Il file di caricamento dello switch a 64 bit generato si trova in `/var/mqm/exits64`.

Se il sistema non supporta la compilazione a 32 bit, utilizzare solo la destinazione a 64 bit:

```
make -f xaswit.mak sybswit64
```

Nota: AIX In AIX, il makefile di esempio è stato modificato come mostrato nel seguente esempio in modo da poter selezionare un valore SYBLINKFLAG64 diverso, a seconda se si utilizza Sybase 15 ESD#5 o una versione precedente di Sybase.

```
SYBLINKFLAGS32=-brtl
# The following line is for Sybase 15
#SYBLINKFLAGS64=-brtl
# The following line is for Sybase 16
SYBLINKFLAGS64=-bstatic -bdynamic
```

L'unica modifica che è necessario apportare al makefile è assicurarsi che solo uno dei valori SYBLINKFLAGS64 non sia commentato. Il predefinito è Sybase 16, che è il valore da utilizzare per 15 #ESD5 e versioni successive.

Tutti i file switch XA prodotti sono collegati a quella specifica release di Sybase e non devono essere spostati su altre piattaforme.

Se il livello di Sybase viene modificato, è necessario ricreare il file di commutazione XA.

Aggiunta delle informazioni di configurazione del gestore risorse per Sybase

È necessario modificare le informazioni di configurazione per il gestore code per dichiarare Sybase come partecipante nelle unità di lavoro globali. La modifica delle informazioni di configurazione è descritta più dettagliatamente in “Aggiunta di informazioni di configurazione al gestore code” a pagina 57.

- Linux Windows Su sistemi Windows e Linux (x86 e x86-64), utilizzare IBM MQ Explorer. Specificare i dettagli del file di caricamento switch nel pannello delle proprietà del gestore code, nel gestore risorse XA.
- Su tutti gli altri sistemi specificare i dettagli del file di caricamento switch nella stanza XAResourceManager nel file `qm.ini` del gestore code.

Linux AIX Il seguente esempio mostra una voce XAResourceManager di esempio per Sybase su AIX and Linux, che utilizza il database associato con la definizione lrmname LRM nel file di configurazione Sybase XA $SYBASE/$SYBASE_OCS/`xa_config`. Includere un nome file di log se si desidera che le chiamate della funzione XA vengano registrate:

```
XAResourceManager:
  Name=mysybase
  SwitchFile=sybswit
  XAOpenString=-Uuser -Ppassword -Nlrmname -L/tmp/sybase.log -Txa
  ThreadOfControl=THREAD
```

Utilizzo di programmi a più thread con Sybase

Se si utilizzano programmi multi-thread con unità di lavoro globali 'IBM MQ che incorporano aggiornamenti a Sybase, è necessario utilizzare il valore THREAD per il parametro ThreadOfControl. Assicurarsi inoltre di collegare il proprio programma (e il file di caricamento switch) con le librerie thread - safe Sybase (versioni _r). L'uso del valore THREAD per il parametro ThreadOfControl è mostrato nell'esempio precedente.

Multi Configurazioni di più database

Se si desidera configurare il gestore code in modo che gli aggiornamenti a più database possano essere inclusi nelle unità di lavoro globali, aggiungere una sezione XAResourceManager per ciascun database.

Se i database sono tutti gestiti dallo stesso gestore database, ogni stanza definisce un database separato. Ogni stanza specifica lo stesso *SwitchFile*, ma il contenuto di *XAOpenString* è diverso perché specifica il nome del database da aggiornare. Ad esempio, le strofe mostrate in ' Figura 9 a pagina 69 configurano il gestore di code con i database 'Db2 *MQBankDB* e *MQFeeDB* sui sistemi 'AIX and Linux.

Importante: Non è possibile avere più stanze che puntano allo stesso database. Questa configurazione non funziona in nessuna circostanza e se si prova questa configurazione non riesce.

Si riceveranno errori nel formato `when the MQ code makes its second xa_open call in any process in this environment, the database software fails the second xa_open with a -5 error, XAER_INVAL.`

```
XAResourceManager:
Name=DB2 MQBankDB
SwitchFile=db2swit
XAOpenString=MQBankDB

XAResourceManager:
Name=DB2 MQFeeDB
SwitchFile=db2swit
XAOpenString=MQFeeDB
```

Figura 9. Voci XAResourceManager di esempio per più database Db2

Se i database da aggiornare sono gestiti da gestori database differenti, aggiungere una sezione XAResourceManager per ciascuno. In questo caso, ogni stanza specifica un *SwitchFile*differente. Ad esempio, se *MQFeeDB* è gestito da Oracle invece di Db2, utilizzare le seguenti stanze sui sistemi AIX and Linux :

```
XAResourceManager:
Name=DB2 MQBankDB
SwitchFile=db2swit
XAOpenString=MQBankDB

XAResourceManager:
Name=Oracle MQFeeDB
SwitchFile=oraswit
XAOpenString=Oracle_XA+Acc=P/myuser/mypassword+SesTm=35+LogDir=/tmp/ora.log+DB=MQFeeDB
```

Figura 10. Voci XAResourceManager di esempio per un database Db2 e Oracle

In linea di principio, non esiste un limite al numero di istanze del database che possono essere configurate con un singolo gestore code.

Nota: Per informazioni sul supporto per l'inclusione dei database Informix in più aggiornamenti di database all'interno delle unità di lavoro globali, controllare il file readme del prodotto.

Multi Considerazioni sulla sicurezza

Considerazioni per l'esecuzione del database nel modello XA.

Le seguenti informazioni sono fornite solo come guida. In tutti i casi, fare riferimento alla documentazione fornita con il gestore database per determinare le implicazioni di sicurezza dell'esecuzione del database nel modello XA.

Un processo dell'applicazione indica l'inizio di un'unità di lavoro globale utilizzando il comando `MQBEGIN` . La prima chiamata `MQBEGIN` che un'applicazione emette si connette a tutti i database partecipanti richiamandone il codice della libreria client al punto di entrata xa_open. Tutti i gestori database forniscono un meccanismo per fornire un ID utente e una password in XAOpenString. Questa è l'unica volta che vengono trasmesse le informazioni di autenticazione.

Notare che, sulle piattaforme AIX and Linux , le applicazioni fastpath devono essere eseguite con un ID utente effettivo di mqm durante le chiamate MQI.

Multi Considerazioni quando si perde il contatto con il gestore risorse XA

Il gestore code tollera i gestori database non disponibili. Ciò significa che è possibile avviare e arrestare il gestore code indipendentemente dal server di database. Quando il contatto viene ripristinato, il gestore code e il database vengono risincronizzati. È anche possibile utilizzare il comando rsvmqtrn per risolvere manualmente le unità di lavoro in dubbio.

Nelle normali operazioni, è necessaria solo una quantità minima di gestione dopo aver completato i passi di configurazione. Il lavoro di gestione è reso più semplice perché il gestore code tollera i gestori database non disponibili. Ciò significa in particolare che:

- Il gestore code può essere avviato in qualsiasi momento senza prima avviare ciascun gestore database.
- Il gestore code non deve essere arrestato e riavviato se uno dei gestori database diventa non disponibile.

Ciò consente di avviare e arrestare il gestore code indipendentemente dal server di database.

Ogni volta che si perde il contatto tra il gestore code e un database, è necessario risincronizzarli quando entrambi diventano nuovamente disponibili. La risincronizzazione è il processo mediante il quale vengono completate tutte le unità di lavoro in dubbio che coinvolgono tale database. In generale, ciò si verifica automaticamente senza la necessità di intervento dell'utente. Il gestore code richiede al database un elenco di unità di lavoro in dubbio. Indica quindi al database di eseguire il commit o il rollback di ciascuna di queste unità di lavoro in dubbio.

Quando un gestore code viene avviato, viene risincronizzato con ciascun database. Quando un singolo database diventa non disponibile, solo tale database deve essere risincronizzato la volta successiva che il gestore code nota che è nuovamente disponibile.

Il gestore code riacquista automaticamente il contatto con un database precedentemente non disponibile quando vengono avviate nuove unità di lavoro globali con MQBEGIN. Esegue questa operazione richiamando la funzione xa_open nella libreria del client di database. Se questa chiamata xa_open ha esito negativo, MQBEGIN restituisce un codice di completamento di MQCC_WARNING e un codice motivo di MQRC_PARTICIPANT_NOT_AVAILABLE. È possibile ritentare la chiamata MQBEGIN successivamente.

Non continuare a tentare un'unità di lavoro globale che implica aggiornamenti a un database che ha indicato un errore durante MQBEGIN. Non ci sarà una connessione al database tramite cui è possibile effettuare gli aggiornamenti. Le uniche opzioni disponibili sono la chiusura del programma o la ripetizione periodica di MQBEGIN, nella speranza che il database diventi nuovamente disponibile.

In alternativa, è possibile utilizzare il comando `rsvmqtrn` per risolvere esplicitamente tutte le unità di lavoro in dubbio.

Multi *Unità di lavoro in dubbio*

Un database potrebbe avere unità di lavoro in dubbio se il contatto con il gestore code viene perso dopo che il gestore database è stato istruito per la preparazione. Finché il server di database non riceve

il risultato dal gestore code (commit o rollback), deve mantenere i blocchi del database associati agli aggiornamenti.

Poiché questi blocchi impediscono ad altre applicazioni di aggiornare o leggere i record del database, la risincronizzazione deve essere eseguita il più presto possibile.

Se, per qualche motivo, non è possibile attendere la risincronizzazione automatica del gestore code con il database, è possibile utilizzare le funzioni fornite dal gestore database per eseguire manualmente il commit o il rollback degli aggiornamenti del database. In *X/Open Distributed Transaction Processing: The XA Specification*, ciò viene chiamato prendendo una decisione *euristica* . Utilizzarla solo come ultima risorsa a causa della possibilità di compromettere l'integrità dei dati; è possibile, ad esempio, eseguire erroneamente il rollback degli aggiornamenti del database quando tutti gli altri partecipanti hanno eseguito il commit degli aggiornamenti.

È preferibile riavviare il gestore code o utilizzare il comando `rsvmqtrn` quando il database è stato riavviato, per avviare la risincronizzazione automatica.

Multi *Visualizzazione delle unità di lavoro in sospeso con il comando dspmqtrn*

Quando un gestore di database non è disponibile, si può usare il comando **dspmqtrn** per controllare lo stato delle unità di lavoro globali in sospeso che coinvolgono quel database.

Il comando **dspmqtrn** visualizza solo le unità di lavoro in cui uno o più partecipanti sono in dubbio. I partecipanti sono in attesa della decisione del gestore code di eseguire il commit o il rollback degli aggiornamenti preparati.

Per ciascuna di queste unità di lavoro globali, lo stato di ciascun partecipante viene visualizzato nell'output di **dspmqtrn**. Se l'unità di lavoro non ha aggiornato le risorse di un particolare gestore risorse, non viene visualizzata.

Per quanto riguarda un'unità di lavoro in dubbio, si dice che un gestore risorse abbia eseguito una delle seguenti operazioni:

Preparato
: Il gestore risorse è pronto per eseguire il commit degli aggiornamenti.

Con commit
: Il gestore risorse ha eseguito il commit dei propri aggiornamenti.

Sottoposto a rollback
: Il gestore risorse ha eseguito il rollback dei propri aggiornamenti.

Ha partecipato
: Il gestore risorse è un partecipante, ma non ha preparato, eseguito il commit o eseguito il rollback dei suoi aggiornamenti.

Quando il queue manager viene riavviato, chiede a ogni database che ha una stanza `XAResourceManager` un elenco delle sue unità di lavoro globali in dubbio. Se il database non è stato riavviato o non è disponibile, il gestore code non può ancora consegnare al database i risultati finali per tali unità di lavoro. Il risultato delle unità di lavoro in dubbio viene consegnato al database alla prima occasione quando il database è nuovamente disponibile.

In questo caso, il gestore di database viene segnalato come in stato `prepared` fino a quando non avviene la risincronizzazione.

Ogni volta che il comando **dspmqtrn** visualizza un'unità di lavoro in dubbio, elenca prima tutti i possibili gestori risorse che potrebbero partecipare. A questi viene assegnato un identificatore univoco, `RMId`, che viene utilizzato al posto del *nome* dei gestori delle risorse quando si comunica il loro stato rispetto a un'unità di lavoro in dubbio.

Output dspmqtrn di esempio mostra il risultato dell'immissione del seguente comando:

```
dspmqtrn -m MY_QMGR
```

```
AMQ7107: Resource manager 0 is MQSeries.
AMQ7107: Resource manager 1 is DB2 MQBankDB.
AMQ7107: Resource manager 2 is DB2 MQFeeDB.

AMQ7056: Transaction number 0,1.
    XID: formatID 5067085, gtrid_length 12, bqual_length 4
         gtrid [3291A50600002013746573 74]
         bqual [00000001]
AMQ7105: Resource manager 0 has committed.
AMQ7104: Resource manager 1 has prepared.
AMQ7104: Resource manager 2 has prepared.
```

dove *Numero transazione* è l'ID della transazione che può essere utilizzato con il comando **rsvmqtrn** . Per ulteriori informazioni, consultare AMQ7xxx: IBM MQ product messages . Le variabili *XID* fanno parte della *Specifica X/Open XA* ; per le informazioni più aggiornate su questa specifica, fare riferimento a https://publications.opengroup.org/c193.

Figura 11. Output dspmqtrn di esempio

L'output in Output dspmqtrn di esempio mostra che ci sono tre gestori risorse associati al gestore code. Il primo è il gestore risorse `0`, che è il gestore code stesso. Le altre due istanze del gestore risorse sono i database `MQBankDB` e `MQFeeDB` Db2 .

L'esempio mostra solo una singola unità di lavoro in dubbio. Viene emesso un messaggio per tutti i tre gestori risorse, il che significa che sono stati effettuati aggiornamenti al gestore code e ad entrambi i database Db2 all'interno dell'unità di lavoro.

Gli aggiornamenti apportati al gestore code, il gestore risorse `0`, sono stati `sottoposti a commit`. Gli aggiornamenti ai database Db2 si trovano nello stato `preparato` , il che significa che Db2 deve essere diventato non disponibile prima di essere stato richiamato per eseguire il commit degli aggiornamenti ai database `MQBankDB` e `MQFeeDB` .

L'unità di lavoro in dubbio ha un identificativo esterno denominato XID (*id transazione*). Si tratta di una parte di dati forniti a Db2 dal gestore code per identificare la sua parte dell'unità di lavoro globale.

Per informazioni più complete su **dspmqtrn**, e per un ulteriore esempio di utilizzo (`dspmqtrn -m <qmgrname> -q -a`), vedere **dspmqtrn**.

Multi

Risoluzione delle unità di lavoro in sospeso con il comando rsvmqtrn

Le unità di lavoro in sospeso vengono completate quando il gestore code e Db2 vengono risincronizzati.

L'output mostrato in Figura 11 a pagina 72 mostra una singola unità di lavoro in dubbio in cui la decisione di commit deve ancora essere consegnata a entrambi i database Db2 .

Per completare questa unità di lavoro, il gestore code e Db2 devono risincronizzare quando Db2 diventa disponibile. Il gestore code utilizza l'inizio di nuove unità di lavoro come opportunità per riprendere il contatto con Db2. In alternativa, è possibile indicare al gestore code di risincronizzare esplicitamente utilizzando il comando **rsvmqtrn** .

Eseguire questa operazione subito dopo il riavvio di Db2 , in modo che tutti i blocchi del database associati all'unità di lavoro in dubbio vengano rilasciati il più rapidamente possibile. Utilizzare l'opzione -a, che indica al gestore code di risolvere tutte le unità di lavoro in dubbio. Nel seguente esempio, Db2 è stato riavviato, in modo che il gestore code possa risolvere l'unità di lavoro in dubbio:

```
> rsvmqtrn -m MY_QMGR -a
Any in-doubt transactions have been resolved.
```

Multi

Risultati ed errori misti

Sebbene il gestore code utilizzi un protocollo di commit a due fasi, ciò non elimina completamente la possibilità che alcune unità di lavoro si completino con risultati misti. Questo è il punto in cui alcuni partecipanti eseguono il commit dei propri aggiornamenti e alcuni ne eseguono il backout.

Le unità di lavoro che si completano con un risultato misto hanno implicazioni gravi perché le risorse condivise che avrebbero dovuto essere aggiornate come una singola unità di lavoro non sono più in uno stato coerente.

I risultati contrastanti sono causati principalmente quando vengono prese decisioni euristiche sulle unità di lavoro invece di consentire al gestore code di risolvere le unità di lavoro in dubbio. Tali decisioni sono al di fuori del controllo del gestore code.

Ogni volta che il gestore code rileva un risultato misto, produce informazioni FFST e documenta l'errore nei relativi log degli errori, con uno dei seguenti due messaggi:

- Se un gestore database esegue il rollback invece di eseguire il commit:

```
AMQ7606 A transaction has been committed but one or more resource
        managers have rolled back.
```

- Se un gestore database esegue il commit invece di eseguire il rollback:

```
AMQ7607 A transaction has been rolled back but one or more resource
        managers have committed.
```

Ulteriori messaggi identificano i database che sono danneggiati euristicamente. È quindi responsabilità dell'utente ripristinare localmente la congruenza nei database interessati. Si tratta di una procedura complicata in cui è necessario prima isolare l'aggiornamento di cui è stato eseguito erroneamente il commit o il rollback, quindi annullare o ripetere manualmente la modifica del database.

Multi *Modifica delle informazioni di configurazione*

Dopo che il gestore code è stato avviato correttamente per coordinare le unità di lavoro globali, non modificare le informazioni di configurazione del gestore risorse.

Se è necessario modificare le informazioni di configurazione, è possibile farlo in qualsiasi momento, ma le modifiche non diventano effettive fino a quando il gestore code non viene riavviato.

Se si rimuovono le informazioni di configurazione del gestore risorse per un database, si sta effettivamente eliminando la possibilità per il gestore code di contattare tale gestore database.

Mai modificare l'attributo *Nome* nelle informazioni di configurazione del gestore risorse. Questo attributo identifica in modo univoco tale istanza del gestore database per il gestore code. Se si modifica questo identificativo univoco, il gestore code presume che il database sia stato rimosso e che sia stata aggiunta un'istanza completamente nuova. Il gestore code associa ancora le unità di lavoro in sospeso con il vecchio *Nome*, probabilmente lasciando il database in uno stato in dubbio.

Multi *Rimozione delle istanze del gestore database*

Se è necessario rimuovere definitivamente un database dalla configurazione, assicurarsi che il database non sia in dubbio prima di riavviare il gestore code.

I prodotti database forniscono comandi per elencare le transazioni in dubbio. Se sono presenti transazioni in dubbio, prima consentire al gestore code di risincronizzarsi con il database. Eseguire questa operazione avviando il gestore code. È possibile verificare che la risincronizzazione sia stata eseguita utilizzando il comando **rsvmqtrn** o il comando del database per visualizzare le unità di lavoro in dubbio. Una volta completata la risincronizzazione, chiudere il gestore code e rimuovere le informazioni di configurazione del database.

Se non si riesce a osservare questa procedura, il gestore code ricorda ancora tutte le unità di lavoro in dubbio che coinvolgono tale database. Un messaggio di avviso, AMQ7623, viene emesso ogni volta che il gestore code viene riavviato. Se non si intende più configurare questo database con il gestore di code, usare l'opzione -r del comando **rsvmqtrn** per indicare al gestore di code di dimenticare la partecipazione del database alle sue transazioni in dubbio. Il gestore code dimentica tali transazioni solo quando le transazioni in dubbio sono state completate con tutti i partecipanti.

In alcuni casi potrebbe essere necessario rimuovere temporaneamente alcune informazioni di configurazione del gestore risorse. Sui sistemi AIX and Linux , ciò è possibile impostando come commento

la stanza in modo che possa essere facilmente reintegrata in un secondo momento. È possibile decidere di eseguire questa operazione se si verificano errori ogni volta che il gestore code contatta un determinato database o gestore database. La rimozione temporanea delle informazioni di configurazione del gestore risorse in questione consente al gestore code di avviare le unità di lavoro globali che coinvolgono tutti i partecipanti. Di seguito è riportato un esempio di stanza XA`ResourceManager` commentata:

```
# This database has been temporarily removed
#XAResourceManager:
#  Name=mydb2
#  SwitchFile=db2swit
#  XAOpenString=mydbname,myuser,mypassword,toc=t
#  ThreadOfControl=THREAD
```

Figura 12. Stanza XAResourceManager commentata su sistemi AIX and Linux

Su sistemi Windows , utilizzare IBM MQ Explorer per eliminare le informazioni sull'istanza del gestore database. Prestare particolare attenzione a immettere il nome corretto nel campo *Nome* quando viene ripristinato. Se si digita erroneamente il nome, è possibile che si verifichino problemi in dubbio, come descritto in “Modifica delle informazioni di configurazione” a pagina 73.

Multi Registrazione dinamica XA

La specifica XA consente di ridurre il numero di chiamate `xa_*` effettuate da un gestore transazioni a un gestore risorse. Questa ottimizzazione è nota come *registrazione dinamica*.

La registrazione dinamica è supportata da Db2. Altri database potrebbero supportarlo; consultare la documentazione per il prodotto database per i dettagli.

Perché l'ottimizzazione della registrazione dinamica è utile? Nell'applicazione, alcune unità di lavoro globali potrebbero contenere aggiornamenti alle tabelle del database; altre potrebbero non contenere tali aggiornamenti. Quando non è stato effettuato alcun aggiornamento persistente per le tabelle di un database, non è necessario includere tale database nel protocollo di commit che si verifica durante MQCMIT.

Se il database supporta o meno la registrazione dinamica, l'applicazione richiama `xa_open` durante la prima chiamata MQBEGIN su una connessione IBM MQ . Richiama inoltre `xa_close` sulla successiva chiamata MQDISC. Il modello delle successive chiamate XA dipende dal fatto che il database supporti o meno la registrazione dinamica:

Se il database non supporta la registrazione dinamica ...
Ogni unità di lavoro globale implica diverse chiamate di funzioni XA effettuate dal codice di IBM MQ nella libreria client del database, indipendentemente dal fatto che sia stato effettuato un aggiornamento permanente alle tabelle di tale database all'interno dell'unità di lavoro. Eccone alcune:

- `xa_start` e `xa_end` dal processo dell'applicazione. Vengono utilizzati per dichiarare l'inizio e la fine di un'unità di lavoro globale.
- `xa_prepare`, `xa_commite` `xa_rollback` dal processo dell'agent gestore code, amqzlaa0. Questi vengono utilizzati per consegnare il risultato dell'unità di lavoro globale: la decisione di commit o rollback.

Inoltre, il processo dell'agent del gestore code richiama anche `xa_open` durante la prima MQBEGIN.

Se il database supporta la registrazione dinamica ...
Il codice IBM MQ effettua solo le chiamate di funzione XA necessarie. Per un'unità di lavoro globale che **non** ha implicato aggiornamenti permanenti alle risorse del database, non vi sono **chiamate** XA al database. Per un'unità di lavoro globale che **ha** ha coinvolto tali aggiornamenti persistenti, le chiamate devono:

- `xa_end` dal processo di applicazione per dichiarare la fine dell'unità di lavoro globale.
- `xa_prepare`, `xa_commite` `xa_rollback` dal processo dell'agent gestore code, amqzlaa0. Questi vengono utilizzati per consegnare il risultato dell'unità di lavoro globale: la decisione di commit o rollback.

Per il funzionamento della registrazione dinamica, è fondamentale che il database abbia un modo di comunicare a IBM MQ quando ha eseguito un aggiornamento persistente che desidera essere incluso nell'unità di lavoro globale corrente. IBM MQ fornisce la funzione `ax_reg` per questo scopo.

Il codice client del database che viene eseguito nel tuo processo dell'applicazione trova la funzione `ax_reg` e la richiama, per *registrare dinamicamente* il fatto che ha eseguito un lavoro persistente all'interno dell'unità di lavoro globale corrente. In risposta a questa `ax_reg` chiamata, IBM MQ registra che il database ha partecipato. Se questa è la prima `ax_reg` chiamata su questa connessione IBM MQ , il processo dell'agent del gestore code elabora le chiamate `xa_open`.

Il codice client del database effettua questa chiamata `ax_reg` quando è in esecuzione nel processo, ad esempio, durante una chiamata SQL UPDATE o qualsiasi chiamata nell'API client del database è responsabile

Multi *Condizioni di errore*

Nella registrazione dinamica XA c'è la possibilità di un errore che crea confusione nel gestore code.

Un esempio comune è se si dimentica di impostare correttamente le variabili di ambiente del database prima di avviare il gestore code, le chiamate del gestore code a `xa_open` non riescono. Non è possibile utilizzare unità di lavoro globali.

Per evitare ciò, assicurarsi di aver impostato le relative variabili di ambiente prima di avviare il gestore code. Esaminare la documentazione del prodotto database e i consigli forniti in “Configurazione di Db2” a pagina 59, “Configurazione di Oracle” a pagina 62e “Configurazione Sybase” a pagina 66.

Con tutti i prodotti database, il gestore code richiama `xa_open` una sola volta all'avvio del gestore code, come parte della sessione di recupero (come spiegato in “Considerazioni quando si perde il contatto con il gestore risorse XA” a pagina 70). Questa chiamata `xa_open` non riesce se si impostano le variabili di ambiente del database in modo non corretto, ma non causa l'errore di avvio del gestore code. Questo perché lo stesso codice di errore `xa_open` viene utilizzato dalla libreria del client del database per indicare che il server del database non è disponibile. IBM MQ non considera questo come un errore grave, poiché il gestore code deve essere in grado di continuare l'elaborazione dei dati all'esterno delle unità di lavoro globali che coinvolgono tale database.

Le chiamate successive a `xa_open` vengono effettuate dal gestore code durante la prima MQBEGIN su una connessione IBM MQ (se la registrazione dinamica non viene utilizzata) o durante una chiamata dal codice del client del database alla funzione IBM MQ-fornita `ax_reg` (se viene utilizzata la registrazione dinamica).

La **tempistica** di qualsiasi condizione di errore (o, occasionalmente, di report FFST) dipende dal fatto che si stia utilizzando la registrazione dinamica:

- Se si sta utilizzando la registrazione dinamica, la chiamata MQBEGIN potrebbe avere esito positivo, ma la chiamata al database SQL UPDATE (o simile) avrà esito negativo.
- Se non si sta utilizzando la registrazione dinamica, la chiamata MQBEGIN avrà esito negativo.

Verificare che le variabili di ambiente siano impostate correttamente nei processi dell'applicazione e del gestore code.

Multi *Riepilogo delle chiamate XA*

Di seguito è riportato un elenco delle chiamate effettuate alle funzioni XA in una libreria client del database come risultato delle diverse chiamate MQI che controllano le unità di lavoro globali. Questa non è una descrizione completa del protocollo descritto nella specifica XA; viene fornita come una breve panoramica.

Notare che le chiamate `xa_start` e `xa_end` vengono sempre richiamate dal codice IBM MQ nel processo dell'applicazione, mentre `xa_prepare`, `xa_commite` `xa_rollback` vengono sempre richiamate dal processo dell'agente del gestore code, amqzlaa0.

Le chiamate `xa_open` e `xa_close` visualizzate in questa tabella vengono tutte effettuate dal processo dell'applicazione. Il processo dell'agent del gestore code richiama `xa_open` nelle circostanze descritte in “Condizioni di errore” a pagina 75.

Tabella 4. Riepilogo delle chiamate della funzione XA		
chiamata MQI	**Chiamate XA effettuate con registrazione dinamica**	**Chiamate XA effettuate senza registrazione dinamica**
Primo MQBEGIN	`xa_open`	`xa_open` `xa_start`
MQBEGIN successivo	Nessuna chiamata XA	`xa_start`

MQCMIT (**senza che** `ax_reg` venga chiamato durante l'unità di lavoro globale corrente)	Nessuna chiamata XA	`xa_end`
		`xa_prepare`
		`xa_commit`
		`xa_rollback`

MQCMIT (**con** `ax_reg` richiamato durante l'unità di lavoro globale corrente)	`xa_end`
	`xa_prepare`
	`xa_commit`
	`xa_rollback`
		Non applicabile. Nessuna chiamata viene effettuata a ax_reg in modalità non dinamica.

MQBACK (**senza che** `ax_reg` venga richiamato durante l'unità di lavoro globale corrente)	Nessuna chiamata XA	`xa_end` `xa_rollback`
MQBACK (**con** `ax_reg` richiamato durante l'unità di lavoro globale corrente)	`xa_end` `xa_rollback`	Non applicabile. Nessuna chiamata viene effettuata a ax_reg in modalità non dinamica.
MQDISC, dove MQCMIT o MQBACK è stato richiamato per primo. In caso contrario, l'elaborazione MQCMIT viene eseguita per la prima volta durante MQDISC.	`xa_close`	`xa_close`

Note:

1. Per MQCMIT, `xa_commit` viene richiamato se `xa_prepare` ha esito positivo. Altrimenti, viene richiamato `xa_rollback` .

Scenario 2: Altri software forniscono il coordinamento

Nello scenario 2, un gestore transazioni esterno coordina le unità di lavoro globali, avviandole e eseguendone il commit sotto il controllo dell'API del gestore transazioni. I verbi MQBEGIN, MQCMIT e MQBACK non sono disponibili.

In questa sezione viene descritto questo scenario, incluso:

- “Coordinamento del punto di sincronizzazione esterno” a pagina 76
- “Utilizzo di CICS” a pagina 79
- “Utilizzo di Microsoft Transaction Server (COM +)” a pagina 83

Coordinamento del punto di sincronizzazione esterno

Un'unità di lavoro globale può anche essere coordinata da un gestore transazioni X/Open XA esterno. Qui il gestore code IBM MQ partecipa, ma non coordina, l'unità di lavoro.

Il flusso di controllo in un'unità di lavoro globale coordinata da un gestore transazioni esterno è il seguente:

1. Un'applicazione indica al coordinatore del punto di sincronizzazione esterno (ad esempio, TXSeries) che desidera avviare una transazione.
2. Il coordinatore del punto di sincronizzazione indica ai gestori risorse noti, come IBM MQ, la transazione corrente.
3. L'applicazione emette chiamate ai gestori risorse associati alla transazione corrente. Ad esempio, l'applicazione potrebbe emettere chiamate MQGET a IBM MQ.
4. L'applicazione emette una richiesta di commit o backout al coordinatore del punto di sincronizzazione esterno.
5. Il coordinatore del punto di sincronizzazione completa la transazione emettendo le chiamate appropriate a ciascun gestore risorse, generalmente utilizzando protocolli di commit a due fasi.

I livelli supportati dei coordinatori dei punti di sincronizzazione esterni che possono fornire un processo di commit a due fasi per transazioni in cui IBM MQ partecipa sono definiti in Requisiti di sistema per 'IBM MQ.

Il resto di questa sezione descrive come abilitare le unità di lavoro esterne.

La struttura dello switch IBM MQ XA

Ogni gestore risorse che partecipa a un'unità di lavoro coordinata esternamente deve fornire una struttura di switch XA. Questa struttura definisce sia le capacità del gestore risorse che le funzioni che devono essere richiamate dal coordinatore del punto di sincronizzazione.

IBM MQ fornisce due versioni di questa struttura:

- *MQRMIXASwitch* per la gestione delle risorse XA statiche
- *MQRMIXASwitchDynamic* per la gestione dinamica delle risorse XA

Consultare la documentazione del gestore transazioni per determinare se utilizzare l'interfaccia di gestione delle risorse statica o dinamica. Ovunque un gestore transazioni lo supporti, si consiglia di utilizzare la gestione delle risorse XA dinamica.

Alcuni gestori transazioni a 64 bit considerano il tipo *long* nella specifica XA come 64 bit, mentre altri lo considerano come 32 bit. IBM MQ supporta entrambi i modelli:

- Se il gestore transazioni è a 32 bit o il gestore transazioni è a 64 bit ma considera il tipo `long` come 32 bit, utilizzare il file di caricamento switch elencato in Tabella 5 a pagina 77.
- Se il gestore transazioni è a 64 bit e considera il tipo `long` come a 64 bit, utilizzare il file di caricamento switch elencato in Tabella 6 a pagina 78.

Alcuni gestori transazioni a 64 bit considerano il tipo `long` come 64 bit. I seguenti gestori transazioni a 64 bit richiedono il file di caricamento switch a 64 bit alternativo:

- Tuxedo
- V 9.4.0 V 9.4.0 TXSeries a 64 bit

Consultare la documentazione del gestore transazioni se non si è certi del modello utilizzato dal gestore transazioni.

Tabella 5. Nomi file di caricamento switch XA

Piattaforma	**Nome file di caricamento switch (server)**	**Nome file di caricamento switch (client transazionale esteso)**
Windows Windows	*mqmxa.dll*	*mqcxa.dll*
AIX AIX (senza thread)	*libmqmxa.a*	*libmqcxa.a*

Tabella 5. Nomi file di caricamento switch XA (Continua)		
Piattaforma	**Nome file di caricamento switch (server)**	**Nome file di caricamento switch (client transazionale esteso)**
AIX AIX (con thread)	*libmqmxa_r.a*	*libmqcxa_r.a*
Linux Linux (senza thread)	*libmqmxa.so*	*libmqcxa.so*
Linux Linux (con thread)	*libmqmxa_r.so*	*libmqcxa_r.so*

Tabella 6. Nomi file di caricamento switch XA a 64 bit alternativi		
Piattaforma	**Nome file di caricamento switch (server)**	**Nome file di caricamento switch (client transazionale esteso)**
AIX AIX (senza thread)	*libmqmxa64.a*	*libmqcxa64.a*
AIX AIX (con thread)	*libmqmxa64_r.a*	*libmqcxa64_r.a*
Linux Linux (senza thread)	*libmqmxa64.so*	*libmqcxa64.so*
Linux Linux (con thread)	*libmqmxa64_r.so*	*libmqcxa64_r.so*

Alcuni coordinatori di punti di sincronizzazione esterni (non CICS) richiedere che ogni gestore risorse che partecipa a un'unità di lavoro fornisca il relativo nome nel campo del nome della struttura switch XA. Il nome del gestore risorse IBM MQ è MQSeries_XA_RMI.

Il coordinatore del punto di sincronizzazione definisce il modo in cui la struttura switch XA IBM MQ si collega ad essa. Le informazioni sul collegamento della struttura di switch IBM MQ XA con CICS vengono fornite in "Utilizzo di CICS" a pagina 79. Per informazioni sul collegamento della struttura dello switch IBM MQ XA con altri coordinatori del punto di sincronizzazione conformi a XA, consultare la documentazione fornita con tali prodotti.

Le seguenti considerazioni si applicano all'utilizzo di IBM MQ con tutti i coordinatori del punto di sincronizzazione compatibili con XA:

- Si prevede che il codice della libreria del gestore transazioni (in esecuzione come parte dell'API richiamata dal programmatore dell'applicazione) richiamerà **xa_open** in IBM MQ in un determinato momento, prima di richiamare MQCONN.

  La chiamata **xa_open** deve essere effettuata sullo stesso thread in cui viene effettuata la chiamata MQCONN. Il motivo di questo requisito è che la specifica XA richiede che il thread venga utilizzato per implicare il contesto.

  Notare che questo è l'approccio utilizzato nel programma di esempio `amqstxsx.c`. Questo programma di esempio presuppone che venga effettuata una chiamata **xa_open** in IBM MQ, dal codice libreria del gestore transazioni, all'interno della relativa funzione `tpopen`).

Se non viene effettuata alcuna chiamata **xa_open** sullo stesso thread, prima della chiamata MQCONN, la connessione del gestore code IBM MQ non verrà associata ad un contesto XA.

Per ulteriori informazioni, consultare MQCTL.

- La struttura xa_info passata su qualsiasi chiamata xa_open dal coordinatore del punto di sincronizzazione include il nome di un gestore code IBM MQ . Il nome assume lo stesso formato del nome gestore code passato alla chiamata MQCONN . Se il nome inoltrato alla chiamata xa_open è vuoto, viene utilizzato il gestore code predefinito.

  In alternativa, la struttura xa_info può contenere i valori per i parametri *TPM* e *AXLIB* . Il parametro *TPM* specifica il gestore transazioni utilizzato. I valori validi sono CICS, TUXEDO e ENCINA. Il parametro *AXLIB* specifica il nome della libreria contenente le funzioni ax_reg e ax_unreg del gestore transazioni. Per ulteriori informazioni su questi parametri, consultare Configurazione di un client transazionale esteso. Se la struttura xa_info contiene uno di tali parametri, il nome del gestore code viene specificato nel parametro *QMNAME* , a meno che non venga utilizzato il gestore code predefinito.
- Solo un gestore code alla volta può partecipare a una transazione coordinata da un'istanza di un coordinatore del punto di sincronizzazione esterno. Il coordinatore del punto di sincronizzazione è effettivamente connesso al gestore code ed è soggetto alla regola per cui è supportata una sola connessione alla volta.
- Tutte le applicazioni che includono chiamate a un coordinatore del punto di sincronizzazione esterno possono connettersi solo al gestore code che partecipa alla transazione gestita dal coordinatore esterno (poiché sono già effettivamente connesse a tale gestore code). Tuttavia, tali applicazioni devono emettere una chiamata MQCONN per ottenere un handle di connessione e una chiamata MQDISC prima di uscire.
- Un gestore code con aggiornamenti delle risorse coordinati da un coordinatore del punto di sincronizzazione esterno deve essere avviato prima del coordinatore del punto di sincronizzazione esterno. Allo stesso modo, il coordinatore del punto di sincronizzazione deve terminare prima del gestore code.
- Se il coordinatore del punto di sincronizzazione esterno termina in maniera anomala, arrestare e riavviare il gestore code prima di riavviare il coordinatore del punto di sincronizzazione per garantire che tutte le operazioni di messaggistica di cui non è stato eseguito il commit al momento dell'errore siano risolte correttamente.

Utilizzo di CICS

CICS è uno degli elementi di TXSeries.

Le versioni di TXSeries che sono compatibili con XA (e utilizzano un processo di commit a due fasi) sono definite nelle informazioni Requisiti di sistema per 'IBM MQ .

IBM MQ supporta anche altri gestori transazioni. Consultare la pagina Web Requisiti di sistema per 'IBM MQ per i collegamenti alle informazioni sul software supportato.

Requisiti del processo di commit a due fasi

Requisiti del processo di commit a due fasi quando si utilizza il CICS processo di commit a due fasi con IBM MQ. Questi requisiti non si applicano a z/OS.

tenere presenti i seguenti requisiti:

- IBM MQ e CICS devono risiedere sulla stessa macchina fisica.
- IBM MQ non supporta CICS su un IBM MQ MQI client.
- È necessario avviare il gestore code, con il nome specificato nella stanza di definizione delle risorse XAD, ***prima*** di tentare di avviare CICS. In caso contrario, si impedirà l'avvio di CICS se è stata aggiunta una stanza di definizione della risorsa XAD per IBM MQ alla regione CICS .
- È possibile accedere a un solo gestore code IBM MQ alla volta da una singola regione CICS .
- Una transazione CICS deve emettere una richiesta MQCONN prima di poter accedere a risorse IBM MQ . La chiamata MQCONN deve specificare il nome del gestore code IBM MQ specificato nella voce XAOpen

della stanza di definizione della risorsa XAD per l'area CICS . Se questa voce è vuota, la richiesta MQCONN deve specificare il gestore code predefinito.

- Una transazione CICS che accede alle risorse IBM MQ deve emettere una chiamata MQDISC dalla transazione prima di tornare a CICS. In caso contrario, è possibile che CICS Application Server sia ancora connesso, lasciando aperte le code. Inoltre, se non si installa un'uscita di terminazione attività (consultare "Uscita terminazione attività di esempio" a pagina 83), il server delle applicazioni CICS potrebbe in seguito terminare in modo anomalo, forse durante una transazione successiva.
- È necessario assicurarsi che l'ID utente CICS (cics) sia membro del gruppo mqm, in modo che il codice CICS disponga dell'autorità per richiamare IBM MQ.

  Per le transazioni in esecuzione in un ambiente CICS , il gestore code adatta i propri metodi di autorizzazione e di determinazione del contesto nel modo seguente:

  – Il gestore code interroga l'ID utente con cui CICS esegue la transazione. Questo è l'ID utente controllato da Object Authority Manager e viene utilizzato per le informazioni di contesto.
  – Nel contesto del messaggio, il tipo di applicazione è MQAT_CICS.
  – Il nome dell'applicazione nel contesto viene copiato dal nome della transazione CICS .

ALW *Supporto XA generale*

Viene fornito un modulo di caricamento switch XA per consentire il collegamento di CICS con i sistemi IBM MQ for AIX, Linux, and Windows . Inoltre, vengono forniti dei file di codice sorgente di esempio per consentire lo sviluppo degli switch XA per altri messaggi di transazione. IBM i XA generale non è supportato su IBM i.

I nomi dei moduli di carico switch forniti sono i seguenti:

Tabella 7. Codice essenziale per applicazioni CICS : routine di inizializzazione XA

C (origine)	**C (exec) - aggiungere uno dei seguenti XAD.Stanza**
amqzscix.c	AIX amqzsc - TXSeries per AIX 5.1
amqzscin.c	Windows mqmc4swi - TXSeries per Windows 5.1

Multi *Creazione di librerie da utilizzare con TXSeries for Multiplatforms*

Utilizzare queste informazioni quando si creano librerie da utilizzare con TXSeries for Multiplatforms.

Librerie richieste

Vedere Librerie esterne per un elenco di librerie a 32 e 64 bit che è possibile utilizzare.

I *file di caricamento degli switch preintegrati* sono librerie condivise (denominate *DLL* sul sistema Windows) che è possibile utilizzare con i programmi CICS , che richiedono una transazione di commit a due fasi utilizzando il protocollo XA. I nomi di queste librerie precompilate si trovano nella tabella Codice essenziale per applicazioni CICS : routine di inizializzazione XA. Il codice sorgente di esempio viene fornito anche nelle seguenti directory:

Tabella 8. Directory di installazione su sistemi operativi AIX, Linux, and Windows

Piattaforma	**Directory**	**File di origine**
Linux AIX AIX and Linux	*MQ_INSTALLATION_PATH*/samp/	amqzscix.c

Tabella 8. Directory di installazione su sistemi operativi AIX, Linux, and Windows (Continua)		
Piattaforma	**Directory**	**File di origine**
Windows	*MQ_INSTALLATION_PATH*\Tools\c \ Esempi	amqzscin.c

dove *MQ_INSTALLATION_PATH* è la directory in cui è stato installato IBM MQ.

Nota: È necessario utilizzare un file di caricamento switch CICS creato rispetto alla versione di IBM MQ con cui viene utilizzato il file di caricamento switch.

Per creare il file di caricamento switch dall'origine di esempio, seguire le istruzioni appropriate per il proprio sistema operativo:

AIX **AIX**

Emetti il seguente comando:

```
export MQM_HOME=/usr/mqm
echo "amqzscix" > tmp.exp
xlc_r $MQM_HOME/samp/amqzscix.c -I/usr/lpp/cics/include -I$MQM_HOME/inc -e amqzscix -bE:tmp.exp -bM:SRE
    -o amqzsc /usr/lpp/cics/lib/regxa_swxa.o -L$MQM_HOME/lib -L/usr/lpp/cics/lib -lcicsrt -lEncina
    -lEncServer -lpthreads -lsarpc -lmqmcics_r -lmqmxa_r -lmqzi_r -lmqmcs_r
rm tmp.exp
```

Linux **Linux piattaforme**

Emetti il seguente comando:

```
gcc -m32 -shared -fPIC -o amqzscix amqzscix.c
    \-IMQ_INSTALLATION_PATH/inc -I CICS_INSTALLATION_PATH/include
    \-LMQ_INSTALLATION_PATH/lib -Wl,-rpath=MQ_INSTALLATION_PATH/lib
    \-Wl,-rpath=/usr/lib -Wl,-rpath-link,/usr/lib -Wl,--no-undefined
    -Wl,--allow-shlib-undefined \-L CICS_LIB_PATH/regxa_swxa.o \-lpthread -ldl -lc
    -shared -lmqzi_r -lmqmxa_r -lmqmcics_r -ldl -lc
```

V 9.4.0 Linux V 9.4.0 **TXSeries a 64 bit Linux**

Emetti il seguente comando:

```
gcc -shared -fPIC -o amqzscix amqzscix.c
\-IMQ_INSTALLATION_PATH/inc -I CICS_INSTALLATION_PATH/include
\-LMQ_INSTALLATION_PATH/lib64 -Wl,-rpath=MQ_INSTALLATION_PATH/lib64
\-Wl,-rpath=/usr/lib64 -Wl,-rpath-link,/usr/lib64 -Wl,--no-undefined -Wl,--allow-shlib-undefined
\-L CICS_LIB_PATH/regxa_swxa.o \-lpthread -ldl -lc
-shared -lmqzi_r -lmqmxa64_r -lmqmcics_r -ldl -lc
```

Windows **Windows**

Eseguire queste operazioni:

1. Utilizzare il comando cl per creare amqzscin.obj compilando almeno le seguenti variabili:

   ```
   cl.exe -c -I EncinaPath\include -I MQ_INSTALLATION_PATH\include -Gz -LD amqzscin.c
   ```

2. Creare un file di definizione modulo denominato `mqmc1415.def`, che contiene le seguenti righe:

   ```
   LIBRARY MQMC4SWI
   EXPORTS
   CICS_XA_Init
   ```

3. Utilizzare il comando **lib** per creare un file di esportazione e una libreria di importazione utilizzando almeno la seguente opzione:

   ```
   lib -def:mqmc4swi.def -out:mqmc4swi.lib
   ```

   Se il comando lib ha esito positivo, viene creato anche un file `mqmc4swi.exp` .

4. Utilizzare il comando di collegamento per creare `mqmc4swi.dll` utilizzando almeno la seguente opzione:

```
link.exe -dll -nod -out:mqmc4swi.dll
    amqzscin.obj CicsPath\lib\regxa_swxa.obj
    mqmc4swi.exp mqmcics4.lib
    CicsPath\lib\libcicsrt.lib
    DcePath\lib\libdce.lib DcePath\lib\pthreads.lib
    EncinaPath\lib\libEncina.lib
    EncinaPath\lib\libEncServer.lib
    msvcrt.lib kernel32.lib
```

Supporto IBM MQ XA e Tuxedo
IBM MQ su sistemi AIX, Linux, and Windows può bloccare a tempo indeterminato le applicazioni XA coordinate da Tuxedo in xa_start.

Ciò può verificarsi solo quando due o più processi coordinati da Tuxedo in un singolo tentativo di transazione globale per accedere a IBM MQ utilizzando lo stesso XID (transaction branch ID). Se Tuxedo fornisce a ciascun processo nella transazione globale un XID diverso da utilizzare con IBM MQ, ciò non può verificarsi.

Per evitare il problema, configura ogni applicazione in Tuxedo che accede a IBM MQ con un singolo ID transazione globale (gtrid), all'interno del suo gruppo di server Tuxedo. I processi nello stesso gruppo di server utilizzano lo stesso XID durante l'accesso ai gestori risorse per conto di un singolo gtrid e sono pertanto vulnerabili al blocco in xa_start in IBM MQ. I processi in gruppi di server differenti utilizzano XID separati quando accedono ai gestori risorse e quindi non devono serializzare il proprio lavoro di transazione in IBM MQ.

Abilitazione del processo di commit a due fasi CICS

Per consentire a CICS di utilizzare un processo di commit a due fasi per coordinare transazioni che includono chiamate MQI, aggiungere una voce della stanza di definizione della risorsa CICS XAD alla regione CICS . Nota, questo argomento non è applicabile a z/OS.

Questo è un esempio di aggiunta di una voce della stanza XAD per IBM MQ for Windows, dove *Drive* è l'unità in cui è installato IBM MQ (ad esempio, D:).

```
cicsadd -cxad -rcics_region \
     ResourceDescription="MQM XA Product Description" \
     SwitchLoadFile="Drive:\Program Files\IBM\IBM MQ\bin\mqmc4swi.dll" \
     XAOpen=queue_manager_name
```

Per i client transazionali estesi, utilizzare il file di caricamento switch mqcc4swi.dll.

Di seguito è riportato un esempio di aggiunta di una voce della stanza XAD per sistemi IBM MQ for AIX or Linux , dove *MQ_INSTALLATION_PATH* rappresenta la directory di alto livello in cui è installato IBM MQ :

```
cicsadd -cxad -rcics_region \
      ResourceDescription="MQM XA Product Description" \
      SwitchLoadFile="MQ_INSTALLATION_PATH/lib/amqzsc" \
      XAOpen=queue_manager_name
```

Per i client transazionali estesi, utilizzare il file di caricamento switch `amqczsc`.

Consultare la documentazione CICS per informazioni sull'utilizzo del comando **cicsadd** .

Le chiamate a IBM MQ possono essere incluse in una transazione CICS e verrà eseguito il commit o il rollback delle risorse IBM MQ come indicato da CICS. Questo supporto non è disponibile per le applicazioni client.

È necessario immettere un `MQCONN` dalla transazione CICS per accedere alle risorse IBM MQ , seguito da un `MQDISC` corrispondente all'uscita.

Abilitazione delle uscite utente CICS

Un CICS punto di uscita utente (normalmente definito *uscita utente*) è un posto in un modulo CICS in cui CICS può trasferire il controllo ad un programma che è stato scritto (un programma di uscita utente) e in cui CICS può riprendere il controllo una volta terminato il lavoro del programma di uscita.

Prima di utilizzare un'uscita utente CICS , leggere il manuale *CICS Administration Guide* per la propria piattaforma.

Uscita terminazione attività di esempio
IBM MQ fornisce il codice sorgente di esempio per un'uscita di terminazione dell'attività CICS .

Il codice sorgente di esempio si trova nelle directory seguenti:

Tabella 9. Uscite di terminazione attività CICS		
Piattaforma	**Directory**	**File di origine**
Sistemi AIX and Linux	*MQ_INSTALLATION_PATH*/samp	amqzscgx.c
Windows	*MQ_INSTALLATION_PATH*\Tools\ c \ Esempi	amqzscgn.c

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

Le istruzioni di creazione per l'uscita di fine attività di esempio sono contenute nei commenti in ogni file di origine.

Questa uscita viene richiamata da CICS al termine dell'attività normale e anomala (dopo che è stato eseguito qualsiasi punto di sincronizzazione). Non è consentito alcun lavoro recuperabile nel programma di uscita.

Queste funzioni sono utilizzate solo in un contesto IBM MQ e CICS in cui la versione CICS supporta l'interfaccia XA. CICS fa riferimento a tali librerie come `programs` o `user exits`.

CICS ha un numero di uscite utente e amqzscgx, se utilizzato, è definito e abilitato su CICS come `Task termination user exit (UE014015)`, ossia, l'uscita numero `15`.

Quando l'uscita di terminazione dell'attività viene richiamata da CICS, CICS ha già informato IBM MQ dello stato di terminazione dell'attività e IBM MQ ha intrapreso l'azione appropriata (commit o rollback). L'uscita non fa che emettere un MQDISC per la ripulitura.

Uno scopo dell'installazione e della configurazione del proprio sistema CICS per utilizzare un'uscita di terminazione attività è proteggere il sistema da alcune delle conseguenze del codice dell'applicazione malfunzionante. Ad esempio, se la transazione CICS termina in modo anomalo senza prima richiamare MQDISC e non è installata alcuna uscita di terminazione attività, è possibile che si verifichi (entro circa 10 secondi) un successivo errore irreversibile della regione CICS . Ciò è dovuto al fatto che il thread di integrità IBM MQ , che viene eseguito nel processo cicsas, non sarà stato inviato e non avrà il tempo di eseguire la ripulitura e la restituzione. I sintomi potrebbero essere che il processo cicsas termina immediatamente, dopo aver scritto FFST riporta a /var/mqm/errors o all'ubicazione equivalente su Windows.

Utilizzo di Microsoft Transaction Server (COM +)

COM + (Microsoft Transaction Server) è progettato per consentire agli utenti di eseguire applicazioni di logica aziendale in un tipico server di livello intermedio.

Per informazioni importanti, vedere Funzionalità utilizzabili solo con l'installazione primaria su Windows .

COM + divide il lavoro in *attività*, che in genere sono brevi parti indipendenti della logica aziendale, come ad esempio *trasferire fondi dal conto A al conto B*. COM + si basa fortemente sull'orientamento degli oggetti e in particolare su COM; un'attività COM + è rappresentata da un oggetto COM (business).

COM + è una parte integrata del sistema operativo.

COM + fornisce tre servizi all'amministratore dell'oggetto di business, eliminando gran parte delle preoccupazioni dal programmatore dell'oggetto di business:

- Gestione transazioni

- Sicurezza
- Pool di risorse

Di solito, COM + viene utilizzato con il codice di front-end che è un client COM per gli oggetti contenuti in COM + e i servizi di back-end come un database, con il bridge IBM MQ tra l'oggetto di business COM + e il backend.

Il codice front-end può essere un programma autonomo o un ASP (Active Server Page) ospitato da Microsoft Internet Information Server (IIS). Il codice di frontend può essere sullo stesso computer di COM + e dei suoi oggetti di business, con connessione tramite COM. In alternativa, il codice di frontend può essere su un computer diverso, con connessione tramite DCOM. È possibile utilizzare client diversi per accedere allo stesso business object COM + in situazioni diverse.

Il codice di backend può trovarsi sullo stesso computer di COM + e dei relativi oggetti di business oppure su un computer diverso con connessione tramite uno qualsiasi dei protocolli supportati da IBM MQ .

Unità di lavoro globali in scadenza

Il gestore code può essere configurato per far scadere le unità di lavoro globali dopo un intervallo di inattività.

È necessario abilitare una scansione di scadenza, se il software del gestore transazioni esterno ha problemi in cui termina senza prima completare tutte le transazioni avviate dalle relative applicazioni.

Per abilitare la scansione della scadenza, impostare le variabili seguenti nell'ambiente da cui viene avviato il gestore code:

- **AMQ_TRANSACTION_EXPIRY_RESCAN**=*intervallo di riscansione in millisecondi*
- **AMQ_XA_TRANSACTION_EXPIRY**=*intervallo di timeout in millisecondi*

Esempio per Linux e AIX:

```
# Scan runs every 30 seconds.
# Value is given in milliseconds.
export AMQ_TRANSACTION_EXPIRY_RESCAN=30000

# Transactions of age 60 seconds in the Idle state are regarded as expired.
# Value is given in milliseconds.
export AMQ_XA_TRANSACTION_EXPIRY=60000
```

Esempio per Windows:

```
rem Scan runs every 30 seconds.
rem Value is given in milliseconds.
set AMQ_TRANSACTION_EXPIRY_RESCAN=30000

rem Transactions of age 60 seconds in the Idle state are regarded as expired.
rem Value is given in milliseconds.
set AMQ_XA_TRANSACTION_EXPIRY=60000
```

Nota: La scansione di scadenza interessa solo le transazioni avviate dal software del gestore transazioni esterno che si trovano nello stato Inattivo nella Tabella 6-4 della Specifica XA da Gruppo OPEN.

Le transazioni in stato Inattivo non sono associate su alcun thread dell'applicazione e il software del gestore transazioni esterno non ha ancora richiamato la chiamata della funzione **xa_prepare** per posizionare la transazione nello stato Preparato.

Se il software del gestore transazioni esterno si interrompe e si riavvia, normalmente non consegna un commit o un rollback per le transazioni in questo stato.

Il gestore code eseguirà il rollback dei Puts e dei Gets eseguiti all'interno di una transazione che ha raggiunto lo stato Inattivo, se:

- Riavviare il gestore code.
- Abilitare la scansione di scadenza e viene rilevata una transazione inattiva precedente alla durata specificata.

Impostare **AMQ_XA_TRANSACTION_EXPIRY** per consentire l'intervallo previsto tra un'applicazione che esegue il proprio lavoro all'interno della transazione e il completamento della transazione.

Impostare il valore **AMQ_TRANSACTION_EXPIRY_RESCAN** su un valore inferiore rispetto al valore **AMQ_XA_TRANSACTION_EXPIRY** . Eseguire questa operazione in modo che le scansioni degli elenchi di transazioni si verifichino più di una volta nell'intervallo **AMQ_XA_TRANSACTION_EXPIRY** .

Come decidere se è necessario abilitare le scansioni di scadenza

Le scansioni di scadenza sono necessarie solo se si dispone di un gestore transazioni esterno, che viene terminato o arrestato in modo anomalo senza completare le relative transazioni inattive.

Se il gestore transazioni esterno termina in questo modo, i messaggi immessi e ricevuti dell'applicazione non vengono sottoposti a commit o rollback, a meno che non si riavvii il gestore code o non siano state configurate le scansioni di scadenza.

Se ci sono transazioni in questo stato, l'output di **dspmqtrn -m QMNAME -q -a** include l'output come nell'esempio riportato di seguito. Ci sono alcune cose da considerare, per essere sicuri che questa sia una transazione di preoccupazione:

- TRANSTATE è ATTIVO, non PREPARATO.
- Le registrazioni data / ora mostrano che la transazione è stata avviata molto tempo prima dell'esecuzione di **dspmqtrn**. Se le date / ore sono molto recenti, questa non è una transazione preoccupante.
- EXTURID mostra che si tratta di una transazione XA poiché ha valori non vuoti per XA_FORMATID, XA_GTRID e XA_BQUAL.
- Ci sono uno o più nomi di coda dell'applicazione elencati come record OBJECT, che indicano che i Puts o i Gets sono stati eseguiti su queste code, in questa transazione.
- Non sono presenti informazioni sulla connessione attiva in questo record (ad esempio: CONN, PID, TID, APPLTAG, USERID) perché l'applicazione non è più connessa.

```
TranNum(0,513)
   TRANSTATE(ACTIVE)
   UOWLOGDA(2024-05-23) UOWLOGTI(17.03.22)
   UOWSTDA(2024-05-23)  UOWSTTI(17.03.22)
   UOWLOG( )
   EXTURID(XA_FORMATID[WASD] XA_GTRID[0000018] XA_BQUAL[0000018])
   OBJECT(MY.QUEUE                                          )
```

Unit of recovery disposition

IBM MQ for z/OS provides unit of recovery dispositions. This feature allows you to configure whether the second phase of 2-phase commit transactions can be driven, for example, during recovery, when connected to another queue manager within the same queue sharing group (QSG).

IBM MQ for z/OS V7.0.1 and later supports the unit of recovery disposition.

Unit of recovery disposition

The unit of recovery disposition is related to an application's connection and subsequently any transactions that it starts. There are two possible unit of recovery dispositions.

- A GROUP unit of recovery disposition identifies that a transactional application is logically connected to the queue sharing group and does not have an affinity to any specific queue manager. Any 2-phase commit transactions that it starts that have completed phase-1 of the commit process, that is, they are in doubt, can be inquired and resolved, when connected to any queue manager within the QSG. In a recovery scenario this means that the transaction coordinator does not have to reconnect to the same queue manager, which might be unavailable.
- A QMGR unit of recovery disposition identifies that an application has a direct affinity to the queue manager to which it is connected and any transactions that it starts also have this disposition.

In a recovery scenario the transaction coordinator must reconnect to the same queue manager to inquire, and resolve, any in-doubt transactions, irrespective of whether the queue manager belongs to a queue sharing group.

z/OS For details of how to implement this feature, see Unit of recovery disposition in a queue sharing group.

Scenari di sicurezza

Una serie di scenari che dimostrano l'applicazione della sicurezza a diverse configurazioni.

Gli scenari di sicurezza disponibili sono descritti nei seguenti topic secondari:

Attività correlate

z/OS Impostazione della sicurezza su z/OS

z/OS Security scenario: two queue managers on z/OS

In this scenario, an application uses the **MQPUT1** call to put messages to queues on queue manager QM1. Some of the messages are then forwarded to queues on QM2, using TCP and LU 6.2 channels. The TCP channels can either use SSL/TLS or not. The application could be a batch application or a CICS application, and the messages are put using the MQPMO_SET_ALL_CONTEXT option.

This is illustrated in Figure 13 on page 86.

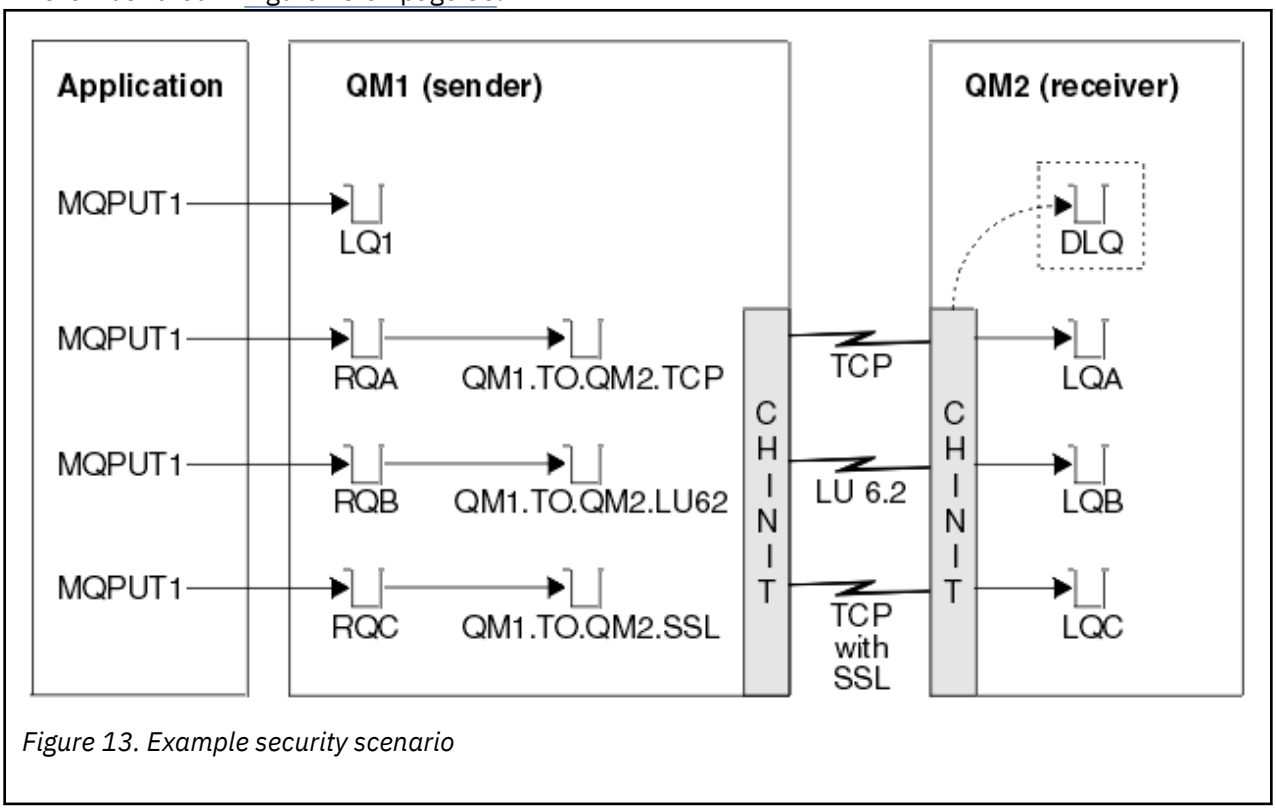


Figure 13. Example security scenario

The following assumptions are made about the queue managers:

- All the required IBM MQ definitions have been predefined or have been made through the CSQINP2 data set processed at queue manager startup.

  If they have not, you need the appropriate access authority to the commands needed to define these objects.
- All the RACF® profiles required have been defined and appropriate access authorities have been granted, before the queue manager and channel initiators started.

If they have not, you need the appropriate authority to issue the RACF commands required to define all the profiles needed and grant the appropriate access authorities to those profiles. You also need the appropriate authority to issue the MQSC security commands to start using the new security profiles.

- All digital certificates required have been created and connected to key rings. The digital certificate sent by QM1 as part of the SSL/TLS handshake is recognized by RACF on QM2's system, either because it is also installed in that RACF profile, or because a matching Certificate Name File (CNF) filter exists.

Related tasks

z/OS Setting up security on z/OS

z/OS Impostazioni dello switch di sicurezza per due scenari del gestore code

Modificare le impostazioni e i profili RACF .

I seguenti switch di sicurezza sono impostati per entrambi i gestori code:

- Sicurezza sottosistema attiva
- Sicurezza coda attiva
- Sicurezza utente alternativo attiva
- Sicurezza contesto su
- Sicurezza processo disattivata
- Sicurezza elenco nomi disattivata
- Sicurezza argomento disattivata
- Sicurezza della connessione attiva
- Sicurezza comando su
- Sicurezza della risorsa del comando attiva

I profili seguenti sono definiti nella classe MQADMIN per disattivare il processo, l'elenco nomi e la topicsecurity:

```
QM1.NO.PROCESS.CHECKS
QM1.NO.NLIST.CHECKS
QM1.NO.TOPIC.CHECKS
QM2.NO.PROCESS.CHECKS
QM2.NO.NLIST.CHECKS
QM2.NO.TOPIC.CHECKS
```

z/OS Queue manager QM1 in two queue manager scenario

Queues and channels for QM1.

The following queues are defined on queue manager QM1:

LQ1
A local queue.

RQA
A remote queue definition, with the following attributes:

- RNAME(LQA)
- RQMNAME(QM2)
- XMITQ(QM1.TO.QM2.TCP)

RQB
A remote queue definition, with the following attributes:

- RNAME(LQB)
- RQMNAME(QM2)

- XMITQ(QM1.TO.QM2.LU62)

RQC
A remote queue definition, with the following attributes:

- RNAME(LQC)
- RQMNAME(QM2)
- XMITQ(QM1.TO.QM2.TLS)

QM1.TO.QM2.TCP
A transmission queue.

QM1.TO.QM2.LU62
A transmission queue.

QM1.TO.QM2.TLS
A transmission queue.

The following channels are defined on QM1:

QM1.TO.QM2.TCP
A sender channel definition, with the following attributes:

- CHLTYPE(SDR)
- TRPTYPE(TCP)
- XMITQ(QM1.TO.QM2.TCP)
- CONNAME(QM2TCP)

QM1.TO.QM2.LU62
A sender channel definition, with the following attributes:

- CHLTYPE(SDR)
- TRPTYPE(LU62)
- XMITQ(QM1.TO.QM2.LU62)
- CONNAME(QM2LU62)

(See Security considerations for the channel initiator on z/OS for information about setting up APPC security.)

QM1.TO.QM2.TLS
A sender channel definition, with the following attributes:

- CHLTYPE(SDR)
- TRPTYPE(TCP)
- XMITQ(QM1.TO.QM2.TLS)
- CONNAME(QM2TCP)
- SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)

z/OS Queue manager QM2 in two queue manager scenario

Queues and channels for QM2.

The following queues have been defined on queue manager QM2:

LQA
A local queue.

LQB
A local queue.

LQC
A local queue.

DLQ
A local queue that is used as the dead-letter queue.

The following channels have been defined on QM2:

QM1.TO.QM2.TCP
A receiver channel definition, with the following attributes:

- CHLTYPE(RCVR)
- TRPTYPE(TCP)
- PUTAUT(CTX)
- MCAUSER(MCATCP)

QM1.TO.QM2.LU62
A receiver channel definition, with the following attributes:

- CHLTYPE(RCVR)
- TRPTYPE(LU62)
- PUTAUT(CTX)
- MCAUSER(MCALU62)

(See Security considerations for the channel initiator on z/OS for information about setting up APPC security.)

QM1.TO.QM2.TLS
A receiver channel definition, with the following attributes:

- CHLTYPE(RCVR)
- TRPTYPE(TCP)
- PUTAUT(CTX)
- MCAUSER(MCASSL)
- SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)

z/OS User IDs used in two queue manager scenario

Explanation of the user IDs in the scenario.

The following user IDs are used:

BATCHID
Batch application (Job or TSO ID)

MSGUSR
UserIdentifier in MQMD (context user ID)

MOVER1
QM1 channel initiator address space user ID

MOVER2
QM2 channel initiator address space user ID

MCATCP
MCAUSER specified on the TCP/IP without SSL/TLS receiver channel definition

MCALU62
MCAUSER specified on the LU 6.2 receiver channel definition

MCASSL
MCAUSER specified on the TCP/IP with SSL/TLS receiver channel definition

CICSAD1
CICS address space ID

CICSTX1
CICS task user ID

CERTID
The user ID associated by RACF with the flowed certificate.

z/OS Security profiles and accesses required for the two queue manager scenario

Information about the security profiles and accesses required for either a batch or CICS implementation of the two queue manager scenario.

The following table shows the security profiles that are required to enable the two queue manager scenario to work. Additional security profiles are also needed, depending on whether you are doing a batch or a CICS implementation of the scenario. For further information see "Security profiles required for a batch application" on page 90 and "Security profiles required for a CICS application" on page 93.

Table 10. Security profiles for the example scenario.

The four columns in this table show the class, the profile, the user ID, and access for the two queue manager scenario.

Class	Profile	User ID	Access
MQCONN	QM1.CHIN	MOVER1	READ
MQADMIN	QM1.RESLEVEL	BATCHID CICSAD1 MOVER1	NONE
MQADMIN	QM1.CONTEXT.**	MOVER1	CONTROL
MQQUEUE	QM1.SYSTEM.COMMAND.INPUT	MOVER1	UPDATE
MQQUEUE	QM1.SYSTEM.CHANNEL.SYNCQ	MOVER1	UPDATE
MQQUEUE	QM1.SYSTEM.CHANNEL.INITQ	MOVER1	UPDATE
MQQUEUE	QM1.SYSTEM.COMMAND.REPLY.MODEL	MOVER1	UPDATE
MQQUEUE	QM1.SYSTEM.ADMIN.CHANNEL.EVENT	MOVER1	UPDATE
MQQUEUE	QM1.QM1.TO.QM2.TCP	MOVER1	ALTER
MQQUEUE	QM1.QM1.TO.QM2.LU62	MOVER1	ALTER
MQQUEUE	QM1.QM1.TO.QM2.TLS	MOVER1	ALTER
MQCONN	QM2.CHIN	MOVER2	READ
MQADMIN	QM2.RESLEVEL	MOVER2	NONE
MQADMIN	QM2.CONTEXT.**	MOVER2	CONTROL
MQQUEUE	QM2.SYSTEM.COMMAND.INPUT	MOVER2	UPDATE
MQQUEUE	QM2.SYSTEM.CHANNEL.SYNCQ	MOVER2	UPDATE
MQQUEUE	QM2.SYSTEM.CHANNEL.INITQ	MOVER2	UPDATE
MQQUEUE	QM2.SYSTEM.COMMAND.REPLY.MODEL	MOVER2	UPDATE
MQQUEUE	QM2.SYSTEM.ADMIN.CHANNEL.EVENT	MOVER2	UPDATE
MQQUEUE	QM2.DLQ	MOVER2	UPDATE

z/OS *Security profiles required for a batch application*

Additional security profiles required for a batch implementation of the two queue manager scenario.

The batch application runs under user ID BATCHID on QM1. It connects to queue manager QM1 and puts messages to the following queues:

- LQ1
- RQA
- RQB
- RQC

It uses the MQPMO_SET_ALL_CONTEXT option. The alternate user ID found in the *UserIdentifier* field of the message descriptor (MQMD) is MSGUSR.

The following profiles are required on queue manager QM1:

Table 11. Sample security profiles for the batch application on queue manager QM1

Class	Profile	User ID	Access
MQCONN	QM1.BATCH	BATCHID	READ
MQADMIN	QM1.CONTEXT.**	BATCHID	CONTROL
MQQUEUE	QM1.LQ1	BATCHID	UPDATE
MQQUEUE	QM1.RQA	BATCHID	UPDATE
MQQUEUE	QM1.RQB	BATCHID	UPDATE
MQQUEUE	QM1.RQC	BATCHID	UPDATE

The following profiles are required on queue manager QM2 for messages put to queue RQA on queue manager QM1 (for the TCP/IP channel not using TLS):

Table 12. Sample security profiles for queue manager QM2 using TCP/IP and not TLS

Class	Profile	User ID	Access
MQADMIN	QM2.ALTERNATE.USER.MSGUSR	MCATCP MOVER2	UPDATE
MQADMIN	QM2.CONTEXT.**	MCATCP MOVER2	CONTROL
MQQUEUE	QM2.LQA	MOVER2 MSGUSR	UPDATE
MQQUEUE	QM2.DLQ	MOVER2 MSGUSR	UPDATE

Notes:

1. The user ID passed in the MQMD of the message is used as the user ID for the MQPUT1 on queue manager QM2 because the receiver channel was defined with PUTAUT(CTX) and MCAUSER(MCATCP).
2. The MCAUSER field of the receiver channel definition is set to MCATCP; this user ID is used in addition to the channel initiator address space user ID for the checks carried out against the alternate user ID and context profile.
3. The MOVER2 user ID and the *UserIdentifier* in the message descriptor (MQMD) are used for the resource checks against the queue.
4. The MOVER2 and MSGUSR user IDs both need access to the dead-letter queue so that messages that cannot be put to the destination queue can be sent there.
5. Two user IDs are checked on all three checks performed because RESLEVEL is set to NONE.

The following profiles are required on queue manager QM2 for messages put to queue RQB on queue manager QM1 (for the LU 6.2 channel):

Table 13. Sample security profiles for queue manager QM2 using LU 6.2			
Class	**Profile**	**User ID**	**Access**
MQADMIN	QM2.ALTERNATE.USER.MSGUSR	MCALU62 MOVER1	UPDATE
MQADMIN	QM2.CONTEXT.**	MCALU62 MOVER1	CONTROL
MQQUEUE	QM2.LQB	MOVER1 MSGUSR	UPDATE
MQQUEUE	QM2.DLQ	MOVER1 MSGUSR	UPDATE

Notes:

1. The user ID passed in the MQMD of the message is used as the user ID for the MQPUT1 on queue manager QM2 because the receiver channel was defined with PUTAUT(CTX) and MCAUSER(MCALU62).
2. The MCA user ID is set to the value of the MCAUSER field of the receiver channel definition (MCALU62).
3. Because LU 6.2 supports security on the communications system for the channel, the user ID received from the network is used as the channel user ID (MOVER1).
4. Two user IDs are checked on all three checks performed because RESLEVEL is set to NONE.
5. MCALU62 and MOVER1 are used for the checks performed against the alternate user ID and Context profiles, and MSGUSR and MOVER1 are used for the checks against the queue profile.
6. The MOVER1 and MSGUSR user IDs both need access to the dead-letter queue so that messages that cannot be put to the destination queue can be sent there.

The following profiles are required on queue manager QM2 for messages put to queue RQC on queue manager QM1 (for the TCP/IP channel using TLS):

Table 14. Sample security profiles for queue manager QM2 using TCP/IP and TLS			
Class	**Profile**	**User ID**	**Access**
MQADMIN	QM2.ALTERNATE.USER.MSGUSR	MCASSL CERTID	UPDATE
MQADMIN	QM2.CONTEXT.**	MCASSL CERTID	CONTROL
MQQUEUE	QM2.LQC	CERTID MSGUSR	UPDATE
MQQUEUE	QM2.DLQ	CERTID MSGUSR	UPDATE

Notes:

1. The user ID passed in the MQMD of the message is used as the user ID for the MQPUT1 on queue manager QM2 because the receiver channel was defined with PUTAUT(CTX) and MCAUSER(MCASSL).
2. The MCA user ID is set to the value of the MCAUSER field of the receiver channel definition (MCASSL).
3. Because the certificate flowed by the channel from QM1 as part of the TLS handshake might be installed on QM2's system, or might match a certificate name filter on QM2's system, the user ID found during that matching is used as the channel user ID (CERTID).
4. Two user IDs are checked on all three checks performed because RESLEVEL is set to NONE.
5. MCASSL and CERTID are used for the checks performed against the alternate user ID and Context profiles, and MSGUSR and MOVER1 are used for the checks against the queue profile.
6. The CERTID and MSGUSR user IDs both need access to the dead-letter queue so that messages that cannot be put to the destination queue can be sent there.

z/OS *Security profiles required for a CICS application*

Additional security profiles required for a CICS implementation of the two queue manager scenario.

The CICS application uses a CICS address space user ID of CICSAD1 and a CICS task user ID of CICSTX1. The security profiles required on queue manager QM1 are different from those profiles required for the batch application. The profiles required on queue manager QM2 are the same as for the batch application.

The following profiles are required on queue manager QM1:

Table 15. Sample security profiles for the CICS application on queue manager QM1

Class	Profile	User ID	Access
MQCONN	QM1.CICS	CICSAD1	READ
MQADMIN	QM1.CONTEXT.**	CICSAD1 CICSTX1	CONTROL
MQQUEUE	QM1.LQ1	CICSAD1 CICSTX1	UPDATE
MQQUEUE	QM1.RQA	CICSAD1 CICSTX1	UPDATE
MQQUEUE	QM1.RQB	CICSAD1 CICSTX1	UPDATE

z/OS Security scenario: queue sharing group on z/OS

In this scenario, an application uses the **MQPUT1** call to put messages to queues on queue manager QM1. Some of the messages are then forwarded to queues on QM2, using TCP and LU 6.2 channels. The application is a batch application, and the messages are put using the MQPMO_SET_ALL_CONTEXT option.

This is illustrated in Figure 13 on page 86.

The following assumptions are made about the queue managers:

- All the required IBM MQ definitions have been predefined or have been made through the CSQINP2 data set processed at queue manager startup.

  If they have not, you need the appropriate access authority to the commands needed to define these objects.
- All the RACF profiles required have been defined and appropriate access authorities have been granted, before the queue manager and channel initiators started.

  If they have not, you need the appropriate authority to issue the RACF commands required to define all the profiles needed and grant the appropriate access authorities to those profiles. You also need the appropriate authority to issue the MQSC security commands to start using the new security profiles.

Related tasks

z/OS Setting up security on z/OS

z/OS Impostazioni del commutatore di sicurezza per lo scenario del gruppo di condivisione code

Modificare le impostazioni e i profili RACF .

I seguenti switch di sicurezza sono impostati per il gruppo di condivisione code:

- Sicurezza sottosistema attiva
- Sicurezza del gruppo di condivisione code attiva
- Sicurezza gestore code disattivata
- Sicurezza coda attiva
- Sicurezza utente alternativo attiva
- Sicurezza contesto su

- Sicurezza processo disattivata
- Sicurezza elenco nomi disattivata
- Sicurezza argomento disattivata
- Sicurezza della connessione attiva
- Sicurezza comando su
- Sicurezza della risorsa del comando attiva

I seguenti profili sono definiti nella classe MQADMIN per disabilitare la sicurezza a livello di processo, elenco nomi, argomento e gestore code:

```
QSGA.NO.PROCESS.CHECKS
QSGA.NO.NLIST.CHECKS
QSGA.NO.TOPIC.CHECKS
QSGA.NO.QMGR.CHECKS
```

z/OS Queue manager QM1 in queue sharing group scenario

Queues and channels for QM1.

The following queues are defined on queue manager QM1:

LQ1
A local queue.

RQA
A remote queue definition, with the following attributes:

- RNAME(LQA)
- RQMNAME(QM2)
- XMITQ(QM1.TO.QM2.TCP)

RQB
A remote queue definition, with the following attributes:

- RNAME(LQB)
- RQMNAME(QM2)
- XMITQ(QM1.TO.QM2.LU62)

QM1.TO.QM2.TCP
A transmission queue.

QM1.TO.QM2.LU62
A transmission queue.

The following channels are defined on QM1:

QM1.TO.QM2.TCP
A sender channel definition, with the following attributes:

- CHLTYPE(SDR)
- TRPTYPE(TCP)
- XMITQ(QM1.TO.QM2.TCP)
- CONNAME(QM2TCP)

QM1.TO.QM2.LU62
A sender channel definition, with the following attributes:

- CHLTYPE(SDR)
- TRPTYPE(LU62)
- XMITQ(QM1.TO.QM2.LU62)

- CONNAME(QM2LU62)

(See Security considerations for the channel initiator on z/OS for information about setting up APPC security.)

z/OS Queue manager QM2 in queue sharing group scenario

Queues and channels for QM2.

The following queues have been defined on queue manager QM2:

LQA
A local queue.

LQB
A local queue.

DLQ
A local queue that is used as the dead-letter queue.

The following channels have been defined on QM2:

QM1.TO.QM2.TCP
A receiver channel definition, with the following attributes:

- CHLTYPE(RCVR)
- TRPTYPE(TCP)
- PUTAUT(CTX)
- MCAUSER(MCATCP)

QM1.TO.QM2.LU62
A receiver channel definition, with the following attributes:

- CHLTYPE(RCVR)
- TRPTYPE(LU62)
- PUTAUT(CTX)
- MCAUSER(MCALU62)

(See Security considerations for the channel initiator on z/OS for information about setting up APPC security.)

z/OS User IDs used in queue sharing group scenario

Explanation of the user IDs in the scenario.

The following user IDs are used:

BATCHID
Batch application (Job or TSO ID)

MSGUSR
UserIdentifier in MQMD (context user ID)

MOVER1
QM1 channel initiator address space user ID

MOVER2
QM2 channel initiator address space user ID

MCATCP
MCAUSER specified on the TCP/IP receiver channel definition

MCALU62
MCAUSER specified on the LU 6.2 receiver channel definition

Security profiles and accesses required for queue sharing group scenario

Security profiles and accesses for either a batch or CICS implementation of the queue sharing group scenario.

The following table shows the security profiles that are required to enable the queue sharing group scenario to work. A batch implementation of this scenario also requires the additional security profiles that are described in “Security profiles required for a batch application” on page 96.

Table 16. Security profiles for the example scenario. z/OS

The four columns in this table show the class, the profile, the user ID, and access for the queue sharing group scenario.

Class	Profile	User ID	Access
MQCONN	QSGA.CHIN	MOVER1 MOVER2	READ
MQADMIN	QSGA.RESLEVEL	BATCHID MOVER1 MOVER2	NONE
MQADMIN	QSGA.CONTEXT.**	MOVER1 MOVER2	CONTROL
MQQUEUE	QSGA.SYSTEM.COMMAND.INPUT	MOVER1 MOVER2	UPDATE
MQQUEUE	QSGA.SYSTEM.CHANNEL.SYNCQ	MOVER1 MOVER	UPDATE
MQQUEUE	QSGA.SYSTEM.CHANNEL.INITQ	MOVER1 MOVER2	UPDATE
MQQUEUE	QSGA.SYSTEM.COMMAND.REPLY.MODEL	MOVER1 MOVER2	UPDATE
MQQUEUE	QSGA.SYSTEM.ADMIN.CHANNEL.EVENT	MOVER1 MOVER2	UPDATE
MQQUEUE	QSGA.SYSTEM.QSG.CHANNEL.SYNCQ	MOVER1 MOVER2	UPDATE
MQQUEUE	QSGA.SYSTEM.QSG.TRANSMIT.QUEUE	MOVER1 MOVER2	UPDATE
MQQUEUE	QSGA.QM1.TO.QM2.TCP	MOVER1	ALTER
MQQUEUE	QSGA.QM1.TO.QM2.LU62	MOVER1	ALTER
MQQUEUE	QSGA.DLQ	MOVER2	UPDATE

z/OS *Security profiles required for a batch application*

Additional security profiles required for a batch implementation of the queue sharing group scenario.

The batch application runs under user ID BATCHID on QM1. It connects to queue manager QM1 and puts messages to the following queues:

- LQ1
- RQA
- RQB

It uses the MQPMO_SET_ALL_CONTEXT option. The user ID found in the *UserIdentifier* field of the message descriptor (MQMD) is MSGUSR.

The following profiles are required on queue manager QM1:

Table 17. Sample security profiles for the batch application on queue manager QM1

Class	Profile	User ID	Access
MQCONN	QSGA.BATCH	BATCHID	READ
MQADMIN	QSGA.CONTEXT.**	BATCHID	CONTROL
MQQUEUE	QSGA.LQ1	BATCHID	UPDATE
MQQUEUE	QSGA.RQA	BATCHID	UPDATE
MQQUEUE	QSGA.RQB	BATCHID	UPDATE

The following profiles are required on queue manager QM2 for messages put to queue RQA on queue manager QM1 (for the TCP/IP channel):

Table 18. Sample security profiles for queue manager QM2 using TCP/IP

Class	Profile	User ID	Access
MQADMIN	QSGA.ALTERNATE.USER.MSGUSR	MCATCP MOVER2	UPDATE
MQADMIN	QSGA.CONTEXT.**	MCATCP MOVER2	CONTROL
MQQUEUE	QSGA.LQA	MOVER2 MSGUSR	UPDATE
MQQUEUE	QSGA.DLQ	MOVER2 MSGUSR	UPDATE

Notes:

1. The user ID passed in the MQMD of the message is used as the user ID for the MQPUT1 on queue manager QM2 because the receiver channel was defined with PUTAUT(CTX) and MCAUSER(MCATCP).
2. The MCAUSER field of the receiver channel definition is set to MCATCP; this user ID is used in addition to the channel initiator address space user ID for the checks carried out against the alternate user ID and context profile.
3. The MOVER2 user ID and the *UserIdentifier* in the message descriptor (MQMD) are used for the resource checks against the queue.
4. The MOVER2 and MSGUSR user IDs both need access to the dead-letter queue so that messages that cannot be put to the destination queue can be sent there.
5. Two user IDs are checked on all three checks performed because RESLEVEL is set to NONE.

The following profiles are required on queue manager QM2 for messages put to queue RQB on queue manager QM1 (for the LU 6.2 channel):

Table 19. Sample security profiles for queue manager QM2 using LU 6.2

Class	Profile	User ID	Access
MQADMIN	QSGA.ALTERNATE.USER.MSGUSR	MCALU62 MOVER1	UPDATE
MQADMIN	QSGA.CONTEXT.**	MCALU62 MOVER1	CONTROL
MQQUEUE	QSGA.LQB	MOVER1 MSGUSR	UPDATE

Table 19. Sample security profiles for queue manager QM2 using LU 6.2 (continued)			
Class	**Profile**	**User ID**	**Access**
MQQUEUE	QSGA.DLQ	MOVER1 MSGUSR	UPDATE

Notes:

1. The user ID passed in the MQMD of the message is used as the user ID for the MQPUT1 on queue manager QM2 because the receiver channel was defined with PUTAUT(CTX) and MCAUSER(MCALU62).
2. The MCA user ID is set to the value of the MCAUSER field of the receiver channel definition (MCALU62).
3. Because LU 6.2 supports security on the communications system for the channel, the user ID received from the network is used as the channel user ID (MOVER1).
4. Two user IDs are checked on all three checks performed because RESLEVEL is set to NONE.
5. MCALU62 and MOVER1 are used for the checks performed against the alternate user ID and Context profiles, and MSGUSR and MOVER1 are used for the checks against the queue profile.
6. The MOVER1 and MSGUSR user IDs both need access to the dead-letter queue so that messages that cannot be put to the destination queue can be sent there.

z/OS Server-to-server message channel interception example configurations

Server-to-server message channel interception requires configuration of channel definitions, as well as Advanced Message Security policies, to ensure that inbound and outbound messages can be correctly protected or unprotected. The configuration varies depending on whether the channel is inbound or outbound.

Inbound channel

The following example shows a typical configuration for an inbound channel of type receiver, and provides details of the AMS policy required to protect unprotected inbound messages:

Figure 14. Inbound configuration

The example shows:

- Queue manager QMA
- Channel TO.QMA
- Local queue DESTQ

Use the following code:

```
DEFINE CHANNEL(TO.QMA) CHLTYPE(RCVR) SSLCAUTH(REQUIRED) SSLCIPH(ANY_TLS12) TRPTYPE(TCP)
SPLPROT(ASPOLICY)

DEFINE QLOCAL(DESTQ) DESCR('AMS PROTECTED QUEUE')

setmqspl -m QMA -p DESTQ -e AES256 -r CN=TEST,O=ORG,C=US
```

Note: The policy described in the preceding text encrypts messages only; that is, AMS Confidentiality.

See setmqspl and the message security policy (CSQ0UTIL) for information on using **setmqspl** on z/OS.

Outbound channel

The following example shows a typical configuration for an outbound channel of type sender. The example provides details of the AMS policies required to protect messages put to the remote queue, and to unprotect and send messages got from the transmission queue:

Figure 15. Outbound configuration

The example shows a:

- Queue manager QMA
- Channel TO.BP
- Local transmission queue TO.BP.XMITQ
- Remote queue REMOTE.BPQ

use the following code:

```
DEFINE CHANNEL(TO.BP) CHLTYPE(SDR) SSLCAUTH(REQUIRED) SSLCIPH(ANY_TLS12) TRPTYPE(TCP)
SPLPROT(REMOVE) CONNAME('server(1414)') XMITQ(TO.BP.XMITQ)

DEFINE QLOCAL(TO.BP.XMITQ) DESCR('TRANSMISSION QUEUE FOR TO.BP') USAGE(XMITQ)

DEFINE QREMOTE(REMOTE.BPQ) DESCR('REMOTE QUEUE TO BP') RNAME(BP.LOCALQ) RQMANME(BPQM)
XMITQ(TO.BP.XMITQ)

setmqspl -m QMA -p TO.BP.XMITQ -e AES256 -r CN=TEST,O=ORG,C=US

setmqspl -m QMA -p REMOTE.BPQ -e AES256 -r CN=TEST,O=ORG,C=US
```

Note: The policy described in the preceding text encrypts messages only; that is, AMS Confidentiality.

Connessione di due gestori code utilizzando SSL/TLS

Le comunicazioni sicure che utilizzano i protocolli di sicurezza crittografici TLS implicano l'impostazione dei canali di comunicazione e la gestione dei certificati digitali che verranno utilizzati per l'autenticazione.

Per configurare l'installazione SSL/TLS è necessario definire i canali per utilizzare TLS. È inoltre necessario ottenere e gestire i certificati digitali. Su un sistema di test, è possibile utilizzare certificati autofirmati o certificati emessi da un'autorità di certificazione (CA) locale. Su un sistema di produzione, non utilizzare certificati autofirmati.

Per informazioni complete sulla creazione e la gestione dei certificati, consultare i seguenti argomenti:

- IBM i Utilizzo di SSL o TLS su IBM i
- ALW Utilizzo di SSL o TLS su sistemi AIX, Linux, and Windows
- z/OS Utilizzo di SSL o TLS su z/OS

Questa raccolta di argomenti introduce le attività coinvolte nella configurazione delle comunicazioni SSL/TLS e fornisce istruzioni dettagliate sul completamento di tali attività.

Potresti anche voler verificare l'autenticazione client SSL/TLS, che sono una parte facoltativa dei protocolli. Durante l'handshake SSL/TLS, il cliente SSL/TLS ottiene e convalida sempre un certificato digitale dal server. Con l'implementazione IBM MQ , il server SSL/TLS richiede sempre un certificato dal client.

Note:

1. In questo contesto, un client SSL / TLS fa riferimento alla connessione che inizia l'handshake.
2. z/OS Quando un gestore code z/OS opera nel ruolo di un client SSL/TLS, il gestore code invia solo un certificato.

Il client SSL/TLS invia un certificato solo se riesce a trovare un certificato con un'etichetta corrispondente. Per i dettagli, consultare Etichetta certificato digitale .

Il server SSL/TLS convalida sempre il certificato client se ne viene inviato uno. Se il client non invia un certificato, l'autenticazione ha esito negativo solo se la fine del canale che funge da server SSL/TLS è definita con il parametro **SSLCAUTH** impostato su REQUIRED oppure un parametro **SSLPEER** ha un valore impostato. Per ulteriori informazioni sulla connessione anonima di un gestore code, ossia quando il client SSL/TLS non invia un certificato, consultare “Connessione di due gestori code utilizzando l'autenticazione unidirezionale” a pagina 105.

Utilizzo di certificati autofirmati per l'autenticazione reciproca di due gestori code

Seguire queste istruzioni di esempio per implementare l'autenticazione reciproca tra due gestori code, utilizzando certificati TLS autofirmati.

Informazioni su questa attività

Scenario:

- Sono presenti due gestori code, QM1 e QM2, che devono comunicare in modo sicuro. È necessaria l'autenticazione reciproca tra QM1 e QM2.
- Si è deciso di verificare la propria comunicazione protetta utilizzando certificati autofirmati.

La configurazione risultante è simile alla seguente:

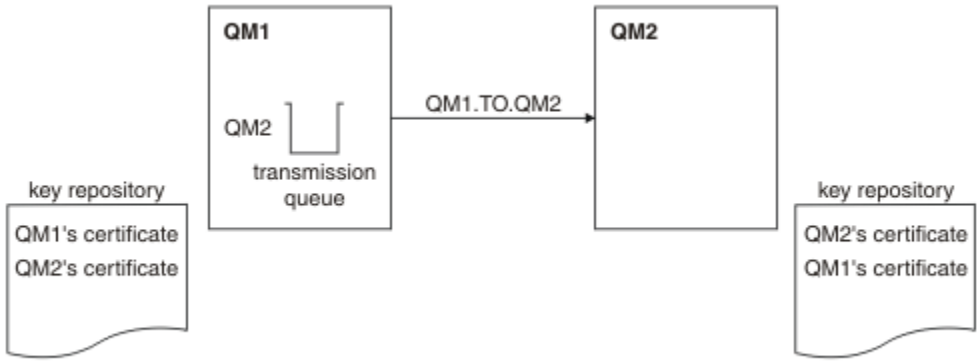


Figura 16. Configurazione risultante da questa attività

In Figura 16 a pagina 100, il repository delle chiavi per QM1 contiene il certificato per QM1 e il certificato pubblico da QM2. Il repository delle chiavi per QM2 contiene il certificato per QM2 e il certificato pubblico da QM1.

Procedura

1. Preparare il repository delle chiavi su ciascun gestore code, in base al sistema operativo:

- ALW Nei sistemi AIX, Linux, and Windows.
- z/OS Nei sistemi z/OS.

2. Creare un certificato autofirmato per ciascun gestore code:
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.
3. Estrarre una copia di ciascun certificato:
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.
4. Trasferire la parte pubblica del certificato QM1 al sistema QM2 e viceversa, utilizzando un programma di utilità come FTP z/OS, come descritto in Scambio di certificati autofirmati .
5. Aggiungere il certificato partner al repository delle chiavi per ciascun gestore code:
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.
6. In QM1, definire un canale mittente e la coda di trasmissione associata, immettendo comandi simili al seguente esempio:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA) DESCR('Sender channel using TLS from QM1 to QM2')

DEFINE QLOCAL(QM2) USAGE(XMITQ)
```

   Questo esempio utilizza CipherSpec TLS_RSA. Le CipherSpecs ad ogni estremità del canale devono essere uguali.
7. Su QM2, definire un canale ricevente immettendo un comando simile al seguente esempio:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS from QM1 to QM2')
```

   Il canale deve avere lo stesso nome del canale mittente definito nel passo “6” a pagina 101e utilizzare lo stesso CipherSpec.
8. Avviare il canale.

   z/OS Su z/OS, consultare Avvio del canale mittente.

Risultati

I repository e i canali chiave vengono creati come illustrato in Figura 16 a pagina 100

Operazioni successive

Verificare che l'attività sia stata completata correttamente utilizzando i comandi DISPLAY. Se l'attività ha avuto esito positivo, l'output risultante è simile a quello mostrato nei seguenti esempi.

Dal gestore code QM1, immettere il comando seguente:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

L'output risultante è simile al seguente esempio:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM1.TO.QM2)                     CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
```

```
   SSLCERTI("CN=QM2,OU=<Department>,O=<Organization>,ST=<State>,C=<Country>")

SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=<Department>,O=<Organization>,ST=<State>,C=
<Country>")
   STATUS(RUNNING)                          SUBSTATE(MQGET)
   XMITQ(QM2)
```

Dal gestore code QM2, immettere il seguente comando:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

L'output risultante è simile al seguente esempio:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM2.TO.QM1)                      CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                      CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=QM1,OU=<Department>,O=<Organization>,ST=<State>,C=<Country>")

SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=<Department>,O=<Organization>,ST=<State>,C=
<Country>")
   STATUS(RUNNING)                          SUBSTATE(RECEIVE)
   XMITQ( )
```

In ogni caso, il valore di SSLPEER deve corrispondere a quello del DN nel certificato partner creato nel passo “2” a pagina 101. Il nome degli emittenti corrisponde al nome peer perché il certificato è autofirmato.

SSLPEER è facoltativo. Se viene specificato, il valore deve essere impostato in modo che il DN nel certificato partner (creato nel passo “2” a pagina 101) sia consentito. Per ulteriori informazioni sull'utilizzo di SSLPE, consultare IBM MQ regole per i valori SSLPEER.

Utilizzo dei certificati firmati dalla CA per l'autenticazione reciproca di due gestori code

Seguire queste istruzioni di esempio per implementare l'autenticazione reciproca tra due gestori code, utilizzando i certificati TLS firmati dalla CA.

Informazioni su questa attività

Scenario:

- Sono presenti due gestori code denominati QM1 e QM2, che devono comunicare in modo sicuro. È necessaria l'autenticazione reciproca tra QM1 e QM2.
- In futuro si prevede di utilizzare questa rete in un ambiente di produzione e quindi si è deciso di utilizzare i certificati firmati dalla CA fin dall'inizio.

La configurazione risultante è simile alla seguente:

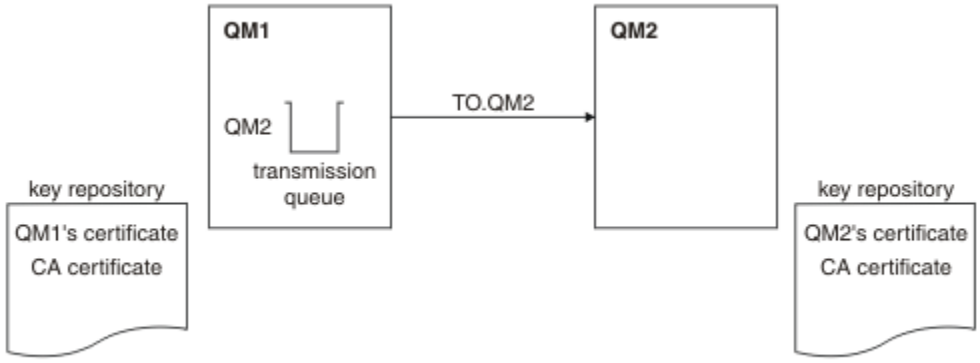


Figura 17. Configurazione risultante da questa attività

In Figura 17 a pagina 103, il repository delle chiavi per QM1 contiene il certificato QM1e il certificato CA. Il repository chiavi per QM2 contiene il certificato QM2e il certificato CA.

In questo esempio, sia il certificato di QM1che il certificato di QM2sono stati emessi dalla stessa CA. Se il certificato di QM1e il certificato di QM2sono stati emessi da diverse CA, i repository delle chiavi per QM1 e QM2 devono contenere entrambi i certificati CA.

Procedura

1. Preparare il repository delle chiavi su ciascun gestore code, in base al sistema operativo o ai sistemi utilizzati dall'azienda:
   - IBM i Sui sistemi IBM i .
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.
2. Richiedere un certificato firmato dalla CA per ciascun gestore code.
   È possibile utilizzare diverse CA per i due gestori code.
   - IBM i Sui sistemi IBM i .
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.
3. Aggiungere il certificato dell'autorità di certificazione al repository delle chiavi per ciascun gestore code:
   Se i gestori code utilizzano autorità di certificazione differenti, il certificato CA per ogni autorità di certificazione deve essere aggiunto a entrambi i repository delle chiavi.
   - IBM i Non eseguire questa operazione sui sistemi IBM i .
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.
4. Ricevere il certificato firmato dalla CA nel repository delle chiavi per ciascun gestore code:
   - IBM i Sui sistemi IBM i .
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.

5. In QM1, definire un canale mittente e la coda di trasmissione associata emettendo comandi simili al seguente esempio:

```
DEFINE CHANNEL(TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP)
CONNAME(QM2.MACH.COM) XMITQ(QM2) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
DESCR('Sender channel using TLS from QM1 to QM2')

DEFINE QLOCAL(QM2) USAGE(XMITQ)
```

   Questo esempio utilizza CipherSpec TLS_RSA_WITH_AES_128_CBC_SHA256. Le CipherSpecs ad ogni estremità del canale devono essere uguali.
6. Su QM2, definire un canale ricevente immettendo un comando simile al seguente:

```
DEFINE CHANNEL(TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) SSLCAUTH(REQUIRED)
DESCR('Receiver channel using TLS to QM2')
```

   Il canale deve avere lo stesso nome del canale mittente definito nel passo “5” a pagina 104e utilizzare lo stesso CipherSpec.
7. Avviare il canale:
   - IBM i Sui sistemi IBM i .
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.

Risultati

I repository e i canali chiave vengono creati come illustrato in Figura 17 a pagina 103.

Operazioni successive

Verificare che l'attività sia stata completata correttamente utilizzando i comandi DISPLAY. Se l'attività ha avuto esito positivo, l'output risultante è simile a quello mostrato nei seguenti esempi.

Dal gestore code QM1, immettere il comando seguente:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

L'output risultante è simile al seguente esempio:

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(SDR)
   CONNAME(192.0.0.2)                      CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=<Division> CA,OU=<Department>,O=<Organization>,ST=<State>,C=<Country>")

SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM2,OU=<Department>,O=<Organization>,ST=<State>,C=
<Country>")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

Dal gestore code QM2, immettere il seguente comando:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

L'output risultante è simile al seguente esempio:

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(RCVR)
   CONNAME(192.0.0.1)                      CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=<Division> CA,OU=<Department>,O=<Organization>,ST=<State>,C=<Country>")
```

```
SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=<Department>,O=<Organization>,ST=<State>,C=
<Country>")
   STATUS(RUNNING)                          SUBSTATE(RECEIVE)
   XMITQ( )
```

In ogni caso, il valore di SSLPEER deve corrispondere a quello del DN (Distinguished Name) nel certificato partner creato nel passo “2” a pagina 103. Il nome dell'emittente corrisponde al DN oggetto del certificato CA che ha firmato il certificato personale aggiunto nel passo “4” a pagina 103.

Connessione di due gestori code utilizzando l'autenticazione unidirezionale

Seguire queste istruzioni di esempio per modificare un sistema con autenticazione reciproca per consentire a un gestore code di connettersi utilizzando l'autenticazione unidirezionale a un altro; ossia, quando il client SSL/TLS non invia un certificato.

Informazioni su questa attività

Scenario:

- I due gestori code (QM1 e QM2) sono stati configurati come in “Utilizzo dei certificati firmati dalla CA per l'autenticazione reciproca di due gestori code” a pagina 102.
- Si desidera modificare QM1 in modo che si connetta utilizzando l'autenticazione unidirezionale a QM2.

La configurazione risultante è simile alla seguente:

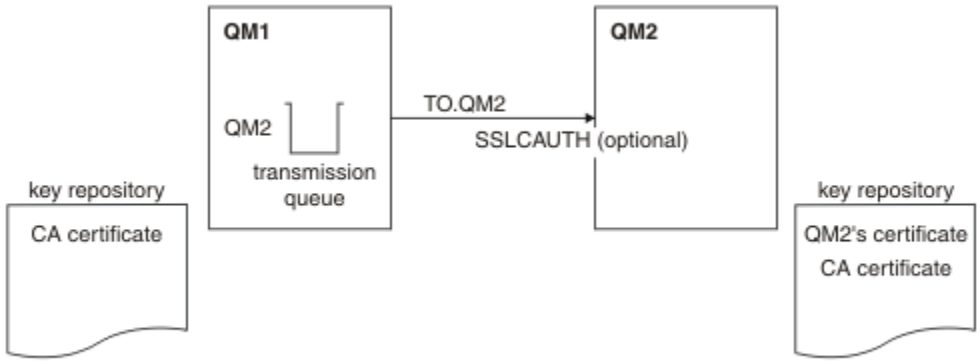


Figura 18. Gestori code che consentono l'autenticazione unidirezionale

Procedura

1. Rimuovere il certificato personale di QM1 dal relativo repository delle chiavi:
   - IBM i Rimozione di un certificato su sistemi IBM i
   - ALW Rimozione di un certificato su AIX, Linux, and Windows
   - z/OS Rimozione di un certificato su sistemi z/OS. Eseguire questa operazione due volte, per rimuovere sia il certificato personale per QMA che il certificato predefinito.

   Per i dettagli sulla modalità di etichettatura dei certificati, consultare Etichette dei certificati digitali.
2. Opzionale: Su QM1, se i canali SSL/TLS sono stati eseguiti in precedenza, aggiornare l'ambiente SSL/TLS , come descritto in Aggiornamento dell'ambiente TLS .
3. Consentire connessioni anonime sul ricevitore , come descritto in Consentire connessioni anonime su un canale ricevente .

   I repository chiave e i canali vengono modificati come illustrato in Figura 18 a pagina 105
4. Se il canale mittente non era in esecuzione, avviarlo.

Nota: Se il canale mittente era in esecuzione e si è immesso il comando REFRESH SECURITY TYPE (SSL) (nel passo 2), il canale viene riavviato automaticamente.

All'estremità del server del canale, la presenza del valore del parametro del nome peer sul pannello di stato del canale indica che è stato trasmesso un certificato client.

5. Verificare che l'attività sia stata completata correttamente immettendo alcuni comandi DISPLAY.

   Se l'attività ha avuto esito positivo, l'output risultante è simile a quello mostrato nei seguenti esempi:

   - Dal gestore code QM1 , immettere il comando seguente:

     ```
     DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
     ```

     L'output risultante sarà simile al seguente esempio:

     ```
     DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
          4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER
     AMQ8417: Display Channel Status details.
        CHANNEL(TO.QM2)                         CHLTYPE(SDR)
        CONNAME(192.0.0.1)                      CURRENT
        RQMNAME(QM2)
        SSLCERTI("CN=IBM MQ CA,OU=IBM MQ Devt,O=IBM,ST=Hampshire,C=UK")
        SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=IBM MQ
     Development,O=IBM,ST=Hampshire,C=UK")
        STATUS(RUNNING)                         SUBSTATE(MQGET)
        XMITQ(QM2)
     ```

   - Dal gestore code QM2 , immettere il seguente comando:

     ```
     DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
     ```

     L'output risultante sarà simile al seguente esempio:

     ```
     DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
          5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     AMQ8417: Display Channel Status details.
        CHANNEL(TO.QM2)                         CHLTYPE(RCVR)
        CONNAME(192.0.0.2)                      CURRENT
        RQMNAME(QMA)                            SSLCERTI( )
        SSLPEER( )                              STATUS(RUNNING)
        SUBSTATE(RECEIVE)                       XMITQ( )
     ```

     In QM2, il campo SSLPE è vuoto e indica che QM1 non ha inviato un certificato. In QM1, il valore di SSLPEER corrisponde a quello del DN nel certificato personale di QM2.

Connessione sicura di un client a un gestore code

Le comunicazioni sicure che utilizzano i protocolli di sicurezza crittografici TLS implicano l'impostazione dei canali di comunicazione e la gestione dei certificati digitali che verranno utilizzati per l'autenticazione.

Per configurare l'installazione SSL/TLS è necessario definire i canali per utilizzare TLS. È inoltre necessario ottenere e gestire i certificati digitali. Su un sistema di test, è possibile utilizzare certificati autofirmati o certificati emessi da un'autorità di certificazione (CA) locale. Su un sistema di produzione, non utilizzare certificati autofirmati.

Per informazioni complete sulla creazione e la gestione dei certificati, consultare i seguenti argomenti:

- IBM i Utilizzo di SSL o TLS su IBM i
- ALW Utilizzo di SSL o TLS su sistemi AIX, Linux, and Windows
- z/OS Utilizzo di SSL o TLS su z/OS

Questa raccolta di argomenti introduce le attività coinvolte nella configurazione delle comunicazioni SSL/TLS e fornisce istruzioni dettagliate sul completamento di tali attività.

Potresti anche voler verificare l'autenticazione client SSL/TLS, che sono una parte facoltativa dei protocolli. Durante l'handshake SSL/TLS, il cliente SSL/TLS ottiene e convalida sempre un certificato

digitale dal server. Con l'implementazione IBM MQ , il server SSL/TLS richiede sempre un certificato dal client.

IBM i ALW Su sistemi IBM i, AIX, Linux, and Windows , il client SSL/TLS invia un certificato solo se ne ha uno con etichetta nel formato IBM MQ corretto, che è `ibmwebspheremq` seguito dall'ID utente di collegamento in minuscolo o dal valore dell'attributo **CERTLABL** . Vedere Digital certificate labels.

Il server SSL/TLS convalida sempre il certificato client se ne viene inviato uno. Se il client non invia un certificato, l'autenticazione non riesce solo se la fine del canale che funge da server SSL/TLS è definita con il parametro **SSLCAUTH** impostato su `REQUIRED` o con un valore di parametro **SSLPEER** impostato. Per ulteriori informazioni sulla connessione anonima di un gestore code, consultare “Connessione anonima di un client a un gestore code” a pagina 111.

Concetti correlati

TLS CipherSpecs e CipherSuites in IBM MQ classes for Java

TLS CipherSpecs e CipherSuites in IBM MQ classes for JMS

Attività correlate

Utilizzo di certificati per il client .NET gestito

Utilizzo di certificati autofirmati per l'autenticazione reciproca di un client e di un gestore code

Segui queste istruzioni di esempio per implementare l'autenticazione reciproca tra un client e un gestore code, utilizzando certificati TLS autofirmati.

Informazioni su questa attività

IBM i DCM su IBM i non supporta i certificati autofirmati, quindi questa attività non è applicabile sui sistemi IBM i .

Scenario:

- Si dispone di un client C1e di un gestore code, QM1, che devono comunicare in modo sicuro. È necessaria l'autenticazione reciproca tra C1 e QM1.
- Si è deciso di verificare la comunicazione protetta utilizzando i certificati autofirmati.

La configurazione risultante è simile alla seguente:

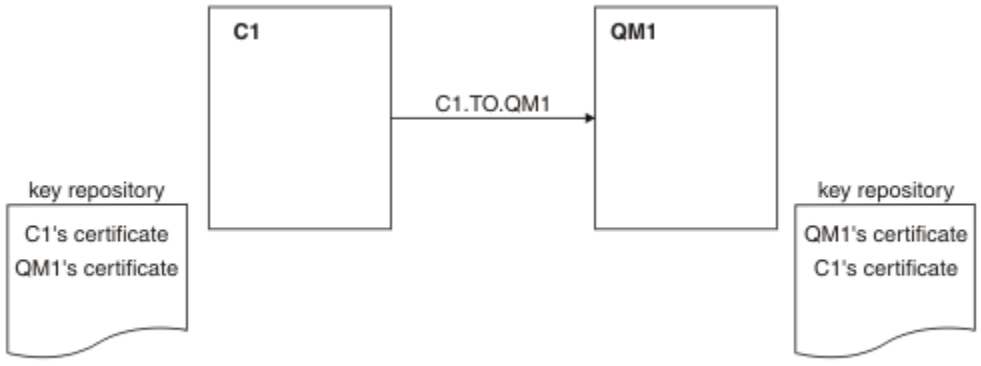


Figura 19. Configurazione risultante da questa attività

In Figura 19 a pagina 107, il repository delle chiavi per QM1 contiene il certificato per QM1 e il certificato pubblico da C1. Il repository delle chiavi per C1 contiene il certificato per C1 e il certificato pubblico da QM1.

Procedura

1. Preparare il repository chiavi sul client e sul gestore code, in base al sistema operativo:
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Su sistemi z/OS (solo gestore code).
2. Creare certificati autofirmati per il client e il gestore code:
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Su sistemi z/OS (solo gestore code).
3. Estrarre una copia di ciascun certificato:
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.
4. Trasferire la parte pubblica del certificato C1 al sistema QM1 e viceversa, utilizzando un programma di utilità come FTP.

   z/OS Per z/OS, consultare Scambio di certificati autofirmati.
5. Aggiungere il certificato partner al repository delle chiavi per client e gestore code:
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Nei sistemi z/OS.
6. Immettere il comando REFRESH SECURITY TYPE(SSL) sul gestore code.
7. Definire un canale di connessione client in uno dei seguenti modi:
   - Utilizzando la chiamata MQCONNX con la struttura MQSCO su C1, così come descritto in Creazione di un canale di connessione client su IBM MQ MQI client utilizzando MQCNO.
   - Utilizzando una tabella di definizione di canale client, come descritto in Creazione di definizioni di connessione server e di connessione client nel server.
8. In QM1, definire un canale di connessione server, immettendo un comando simile al seguente esempio:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS from C1 to QM1')
   ```

   Il canale deve avere lo stesso nome del canale di collegamento client definito nel passo 6 e utilizzare lo stesso CipherSpec.

Risultati

I repository e i canali chiave vengono creati come illustrato in Figura 19 a pagina 107.

Operazioni successive

Verificare che l'attività sia stata completata correttamente utilizzando i comandi **DISPLAY** . Se l'attività ha avuto esito positivo, l'output risultante è simile a quello mostrato nel seguente esempio.

Dal gestore code QM1, immettere il comando seguente:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

L'output risultante è simile al seguente esempio:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(192.0.0.1)                      CURRENT
```

```
   SSLCERTI("CN=QM1,OU=IBM MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=IBM MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                          SUBSTATE(RECEIVE)
```

È facoltativo impostare l'attributo di filtro **SSLPEER** delle definizioni di canale. Se la definizione di canale **SSLPEER** è impostata, il relativo valore deve corrispondere al DN soggetto nel certificato partner creato nel passo 2. Dopo una connessione riuscita, il campo **SSLPEER** nell'output **DISPLAY CHSTATUS** mostra l'oggetto DN del certificato del client remoto.

Utilizzo di certificati firmati CA per l'autenticazione reciproca di un client e di un gestore code

Segui queste istruzioni di esempio per implementare l'autenticazione reciproca tra un client e un gestore code utilizzando i certificati TLS firmati dalla CA.

Informazioni su questa attività

Scenario:

- Si dispone di un client C1e di un gestore code, QM1, che devono comunicare in modo sicuro. È necessaria l'autenticazione reciproca tra C1 e QM1.
- In futuro si prevede di utilizzare questa rete in un ambiente di produzione e quindi si è deciso di utilizzare i certificati firmati dalla CA fin dall'inizio.

La configurazione risultante è simile alla seguente:

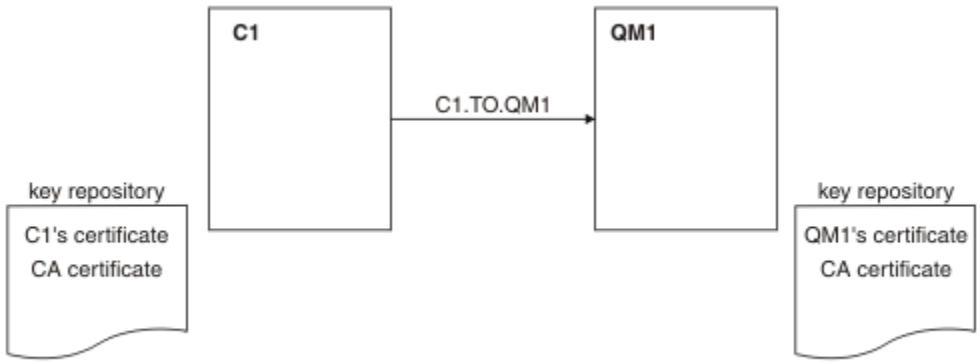


Figura 20. Configurazione risultante da questa attività

In Figura 20 a pagina 109, il repository delle chiavi per C1 contiene il certificato per C1 e il certificato CA. Il repository delle chiavi per QM1 contiene il certificato per QM1 e il certificato CA. In questo esempio, sia il certificato di C1che quello di QM1sono stati emessi dalla stessa CA. Se il certificato di C1e il certificato di QM1sono stati emessi da diverse CA, i repository delle chiavi per C1 e QM1 devono contenere entrambi i certificati CA.

Procedura

1. Preparare il repository chiavi sul client e sul gestore code, in base al sistema operativo:
   - IBM i Sui sistemi IBM i .
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Su sistemi z/OS (solo gestore code).
2. Richiedere un certificato firmato CA per il client e il gestore code.
   È possibile utilizzare diverse CA per il client e il gestore code.

- IBM i Sui sistemi IBM i .
- ALW Nei sistemi AIX, Linux, and Windows.
- z/OS Su sistemi z/OS (solo gestore code).

3. Aggiungere il certificato dell'autorità di certificazione al repository delle chiavi per client e gestore code.

   Se il client e il gestore code utilizzano autorità di certificazione differenti, il certificato CA per ogni autorità di certificazione deve essere aggiunto a entrambi i repository delle chiavi.

   - IBM i Non eseguire questa operazione sui sistemi IBM i .
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Su sistemi z/OS (solo gestore code).

4. Ricevere il certificato firmato dalla CA nel repository delle chiavi per client e gestore code:

   - IBM i Sui sistemi IBM i .
   - ALW Nei sistemi AIX, Linux, and Windows.
   - z/OS Su sistemi z/OS (solo gestore code).

5. Definire un canale di connessione client in uno dei seguenti modi:

   - Utilizzando la chiamata MQCONNX con la struttura MQSCO su C1, così come descritto in Creazione di un canale di connessione client su IBM MQ MQI client utilizzando MQCNO.
   - Utilizzando una tabella di definizione di canale client, come descritto in Creazione di definizioni di connessione server e di connessione client nel server.

6. In QM1, definire un canale di connessione server immettendo un comando simile al seguente esempio:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP)
   SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA) SSLCAUTH(REQUIRED)
   DESCR('Receiver channel using TLS from C1 to QM1')
   ```

   Il canale deve avere lo stesso nome del canale di collegamento client definito nel passo 6 e utilizzare lo stesso CipherSpec.

Risultati

I repository e i canali chiave vengono creati come illustrato in Figura 20 a pagina 109.

Operazioni successive

Verificare che l'attività sia stata completata correttamente utilizzando i comandi DISPLAY. Se l'attività ha avuto esito positivo, l'output risultante è simile a quello mostrato nel seguente esempio.

Dal gestore code QM1, immettere il comando seguente:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
```

L'output risultante è simile al seguente esempio:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(192.0.0.1)                      CURRENT
   SSLCERTI("CN=IBM MQ CA,OU=IBM MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=IBM MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

Il campo SSLPEER nell'output DISPLAY CHSTATUS mostra il DN oggetto del certificato client remoto creato nel passo 2. Il nome dell'emittente corrisponde al DN oggetto del certificato CA che ha firmato il certificato personale aggiunto nel Passo 4.

Connessione anonima di un client a un gestore code

Seguire queste istruzioni di esempio per modificare un sistema con autenticazione reciproca per consentire a un gestore code di connettersi in modo anonimo a un'altro.

Informazioni su questa attività

Scenario:

- Il gestore code e il client (QM1 e C1) sono stati impostati come in “Utilizzo di certificati firmati CA per l'autenticazione reciproca di un client e di un gestore code” a pagina 109.
- Si desidera modificare C1 in modo che si colleghi in modo anonimo a QM1.

La configurazione risultante è simile alla seguente:

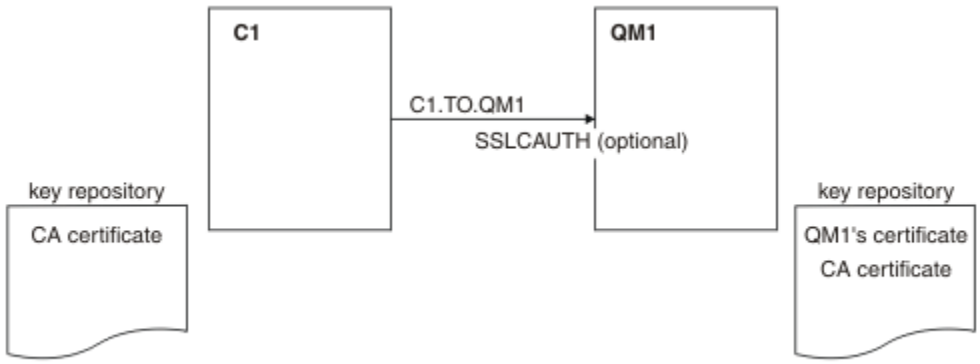


Figura 21. Client e gestore code che consentono la connessione anonima

Procedura

1. Rimuovere il certificato personale dal contenitore chiavi per C1, in base al sistema operativo:
   - IBM i Sistemi IBM i.
   - ALW Sistemi AIX, Linux, and Windows.

   L'etichetta del certificato è `ibmwebspheremq` seguita dall'ID utente di accesso in minuscolo o dal valore dell'attributo **CERTLABL** . Vedere Digital certificate labels.
2. Riavviare l'applicazione client o far sì che l'applicazione client chiuda e riapra tutte le connessioni SSL/TLS.
3. Consentire le connessioni anonime sul gestore code, immettendo il comando seguente:

```
ALTER CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) SSLCAUTH(OPTIONAL)
```

Risultati

I repository chiave e i canali vengono modificati come illustrato in Figura 21 a pagina 111

Operazioni successive

All'estremità del server del canale, la presenza del valore del parametro del nome peer sul pannello di stato del canale indica che è stato trasmesso un certificato client.

Verificare che l'attività sia stata completata correttamente immettendo alcuni comandi DISPLAY. Se l'attività ha avuto esito positivo, l'output risultante è simile a quello mostrato nel seguente esempio:

Dal gestore code QM1, immettere il comando seguente:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

L'output risultante sarà simile al seguente esempio:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(192.0.0.1)                      CURRENT
   SSLCERTI( )                             SSLPEER( )
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

I campi SSLCERTI e SSLPEER sono vuoti e indicano che C1 non ha inviato un certificato.

Windows Migrazione su Windows

Iniziando con un'installazione di IBM MQ 9.3 esistente, questo scenario guida l'utente attraverso le attività chiave richieste per aggiornare e migrare i dati in IBM MQ 9.4. Entrambe le versioni sono installate nello stesso ambiente Windows .

Windows Pianificazione della soluzione

Esaminare gli argomenti in questa sezione per comprendere cosa viene trattato in questo scenario, i motivi per i quali un'azienda potrebbe voler seguire lo scenario e una panoramica della soluzione proposta dallo scenario.

Attività correlate

Pianificazione dell'installazione

Windows Presupposti

Questo scenario fa diversi presupposti sul sistema che si sta utilizzando per impostare e gestire la configurazione IT di esempio. Questi presupposti includono il sistema operativo e la versione dei prodotti che si stanno utilizzando e se la sicurezza è configurata o meno per IBM MQ.

Questo scenario presuppone i seguenti punti:

- Si sta utilizzando un computer con un sistema operativo Windows per questo scenario, su cui si installerà sia la configurazione IBM MQ 9.3 iniziale che IBM MQ 9.4.

  Nota: Il clustering non è descritto in questo scenario. Vengono fornite istruzioni per l'installazione di una singola configurazione del server IBM MQ di esempio che è possibile utilizzare come punto di partenza per provare lo scenario nello stesso modo in cui è stato originariamente sviluppato.
- Si stanno utilizzando le seguenti versioni di IBM MQ:
  - Per la configurazione di esempio iniziale, si utilizza IBM MQ 9.3.
  - Per la configurazione di post - migrazione, si utilizza IBM MQ 9.4.
- Questo scenario non descrive la configurazione della sicurezza per IBM MQ. Se la sicurezza è configurata, è comunque possibile completare lo scenario.
- È possibile utilizzare il prompt dei comandi Windows e la GUI (graphical user interface) IBM MQ Explorerper completare le attività descritte in questo scenario.

Concetti correlati

Percorsi migrazione

Windows Panoramica di business

Una società desidera migrare la configurazione IT IBM MQ 9.3 esistente su un sistema Windows a IBM MQ 9.4.

L'azienda decide di migrare la propria soluzione di business a IBM MQ 9.4 per ottenere valore di business, tra cui:

- Utilizzo di funzionalità nuove e aggiornate disponibili in IBM MQ 9.4.
- Esplorazione del nuovo tipo di rilascio disponibile da IBM MQ 9.4; CDR (Continuous Delivery Release).
- Usufruendo dell'autorizzazione LDAP su piattaforme Windows .

Concetti correlati

Versioni e tipi di release IBM MQ

Informazioni correlate

Domande frequenti di IBM MQ per le release Long Term Support e Continuous Delivery

Windows Scelta di un percorso di migrazione

Quando si esegue la migrazione tra IBM MQ 9.3 e IBM MQ 9.4, è possibile utilizzare diversi percorsi di migrazione.

Questo argomento fornisce una panoramica dei seguenti percorsi di migrazione:

- Percorso a singolo stadio, noto anche come migrazione autonoma
- Percorso di migrazione affiancato
- Percorso di migrazione a più fasi

Nota: Questo scenario descrive solo i metodi di migrazione Single - stage e Side-by-side.

Considerare i vantaggi e le limitazioni di ciascun percorso per determinare quale si adatta meglio alle proprie esigenze:

Migrazione a singolo stadio

Nella migrazione a fase singola, l'installazione della versione più aggiornata del prodotto sostituisce una versione precedente nella stessa ubicazione di installazione.

Il vantaggio della migrazione a fase singola è che modifica la configurazione di un gestore code nella versione precedente il meno possibile. Le applicazioni esistenti passano automaticamente dal caricamento delle librerie dalla versione precedente al caricamento delle librerie della versione più recente. Utilizzando questo approccio, il sistema non sarà disponibile per l'intero processo.

Migrazione affiancata

Nella migrazione affiancata, si installa l'ultima versione di IBM MQ insieme ai gestori code che continuano ad essere associati alla versione precedente.

Quando si è pronti, migrare i gestori code e le applicazioni alla versione più recente.

Con questo approccio, poiché si disinstalla la versione precedente prima di avviare i gestori code, è possibile assegnare un'installazione della versione più recente come installazione primaria.

Per ulteriori informazioni, consultare Scelta di un'installazione primaria .

Migrazione a più fasi

Nella migrazione a più fasi, si installa la versione più recente del prodotto insieme ai gestori code in esecuzione che continuano ad essere associati con la versione precedente. È possibile creare gestori code ed eseguire nuove applicazioni utilizzando l'installazione della versione più recente. Quando si è pronti per avviare la migrazione di gestori code e applicazioni dalle versioni precedenti, è possibile farlo, uno per uno. Al termine della migrazione all'ultima versione, disinstallare la versione precedente e rendere l'installazione dell'ultima versione l'installazione primaria.

Con l'approccio a più fasi, finché non si disinstalla la versione precedente, è necessario configurare un ambiente per eseguire le applicazioni che si connettono a un gestore code all'ultima versione. È inoltre necessario fornire un percorso per eseguire comandi IBM MQ . Entrambe queste attività vengono eseguite con il comando **setmqenv** .

Concetti correlati

Panoramica dei concetti e metodi di migrazione

Attività correlate

Migrazione su AIX and Linux: singola fase

Migrazione su AIX and Linux: fianco a fianco

Migrazione su AIX and Linux: a più fasi

Riferimenti correlati

Elenco delle modifiche che influenzano la migrazione

Windows Soluzione tecnica

Questo scenario descrive due metodi di migrazione da una versione precedente di IBM MQ ad una versione successiva, dove entrambe le versioni vengono eseguite su un sistema operativo Windows e si trovano sullo stesso server.

Windows *Panoramica: configurazione IT iniziale*

Una società utilizza una configurazione IT esistente fornita da un IBM MQ 9.3 installato su un server con sistema operativo Windows . Questo scenario descrive la migrazione della configurazione IT iniziale in una configurazione IT equivalente fornita da IBM MQ 9.4 nello stesso server.

La configurazione IT iniziale include diversi componenti che un amministratore configura o utilizza, come mostrato in Figura 22 a pagina 115:

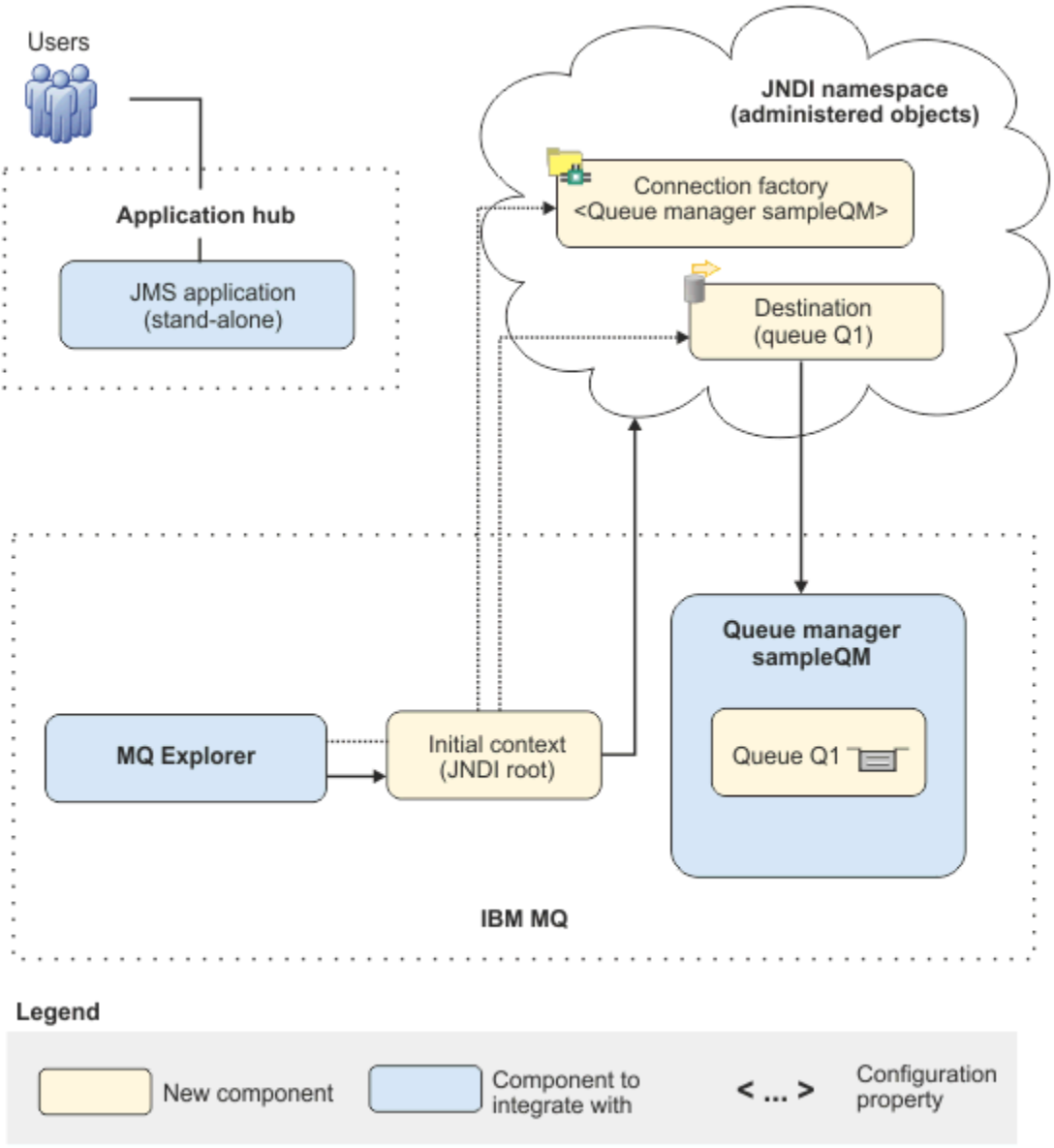


Figura 22. Configurazione IT iniziale

JMS applicazione

Un'applicazione autonoma con cui interagiscono gli utenti aziendali, ad esempio per registrare un ordine. L'applicazione utilizza Java Message Service (JMS) per la messaggistica asincrona.

- JMS è lo standard di messaggistica Java EE ampiamente supportato. Le applicazioni basate su JMSsono quindi portabili su molti prodotti di messaggistica.
- JMS fornisce un livello di astrazione dai dettagli del livello di messaggistica, semplificando il processo di sviluppo dell'applicazione.
- JMS fornisce la comunicazione asincrona, consentendo alle applicazioni di essere eseguite senza dover attendere una risposta, a differenza dei sistemi strettamente accoppiati come RPC (remote procedure call).
- Le applicazioni che utilizzano JMS non specifica direttamente i dettagli per accedere alle risorse. Invece, cercano e utilizzano oggetti JMS gestiti come una factory di connessione e una destinazione.

Per alcune situazioni, altri standard di messaggistica potrebbero essere più adatti di JMS. Ad esempio, IBM Message Service Clients for C, C++ e .NET, noto anche come XMS, sono API che

forniscono vantaggi simili a JMS per applicazioni nonJava . XMS è quindi più adatto se si utilizza la piattaforma .NET o si desidera integrare le applicazioni C++ esistenti con le applicazioni Java EE più recenti.

L'applicazione utilizza la messaggistica point - to - point per inviare i messaggi a una coda nell'infrastruttura ed elabora i messaggi di risposta, per fornire all'utente aziendale una risposta appropriata.

In questo modello di messaggistica, un'applicazione invia un messaggio a una coda e un'altra applicazione riceve il messaggio dalla coda e conferma la ricezione del messaggio. Questo modello è la forma più semplice di messaggistica perché coinvolge solo due endpoint. Questo modello è anche il più appropriato per l'applicazione di esempio di scenario: un singolo client richiede informazioni da un singolo server.

Nel modello di messaggistica alternativo, pubblicazione / sottoscrizione, un publisher pubblica un messaggio in un argomento del messaggio. I sottoscrittori sottoscrivono l'argomento per ricevere i messaggi. Il publisher e il sottoscrittore non dispongono di alcuna informazione reciproca e il messaggio viene ricevuto da zero o più destinatari.

Gestore code sampleQM
Il gestore code IBM MQ che fornisce l'infrastruttura di messaggistica iniziale. Ospita la coda utilizzata dall'applicazione JMS .

Q1 [Coda messaggi]
La coda IBM MQ a cui l'applicazione JMS invia messaggi.

Spazio nomi JNDI
Uno spazio dei nomi Java Naming Directory Interface JNDI viene utilizzato per contenere gli oggetti gestiti JMS , che le applicazioni possono utilizzare per connettersi a IBM MQ e per accedere alle destinazioni per inviare o ricevere messaggi.

JNDI fa parte di Java EEe fornisce un modo standard per le applicazioni di accedere ai vari tipi di servizi di denominazione e di directory, per il recupero dei componenti dell'applicazione. Ad esempio, è possibile utilizzare JNDI per accedere a un servizio di denominazione su un file system per richiamare l'ubicazione di un oggetto stampante o per accedere a un servizio di directory su un server LDAP per richiamare un oggetto utente che contiene informazioni su ID e password. JNDI migliora quindi la portabilità delle applicazioni basate su JMSe rende più semplice l'integrazione di tali applicazioni tra loro e nei sistemi esistenti. Per la messaggistica JMS , si utilizza JNDI per memorizzare gli oggetti che rappresentano la destinazione di un messaggio o la factory di connessione che crea la connessione tra la propria applicazione e la relativa destinazione di messaggistica.

Qualsiasi applicazione o processo con accesso allo spazio dei nomi JNDI può utilizzare gli stessi oggetti gestiti. Le proprietà degli oggetti amministrati possono essere modificate in JNDI, con tutte le applicazioni o i processi che possono beneficiare delle stesse modifiche.

Contesto iniziale
Un contesto iniziale definisce la root dello spazio dei nomi JNDI . Per utilizzare IBM MQ Explorer per creare e configurare gli oggetti gestiti, aggiungere prima un contesto iniziale che definisce la root dello spazio nomi JNDI . Allo stesso modo, un'applicazione JMS ottiene prima un contesto iniziale, prima di poter recuperare gli oggetti gestiti dallo spazio dei nomi JNDI .

Factory di connessione, myCF
Un oggetto factory di connessione JMS definisce una serie di proprietà di configurazione standard per connessioni. Un'applicazione utilizza un factory di connessione per creare una connessione a IBM MQ.

Destinazione, myQueue
Una destinazione JMS può essere un argomento o una coda. In questo scenario, la destinazione è una coda e identifica la coda IBM MQ a cui le applicazioni inviano messaggi o da cui un'applicazione riceve messaggi o entrambi. Un'applicazione ricerca la destinazione nello spazio nomi JNDI per creare una connessione alla coda IBM MQ .

Windows *Panoramica: la topologia logica fornita*

La società è stata migrata da IBM MQ 9.3 a IBM MQ 9.4.

La configurazione IT che segue la migrazione non viene modificata, come mostrato in Figura 23 a pagina 117. Il gestore code e l'applicazione di esempio vengono migrati e il business può beneficiare della nuova funzione nella versione più recente di IBM MQ.

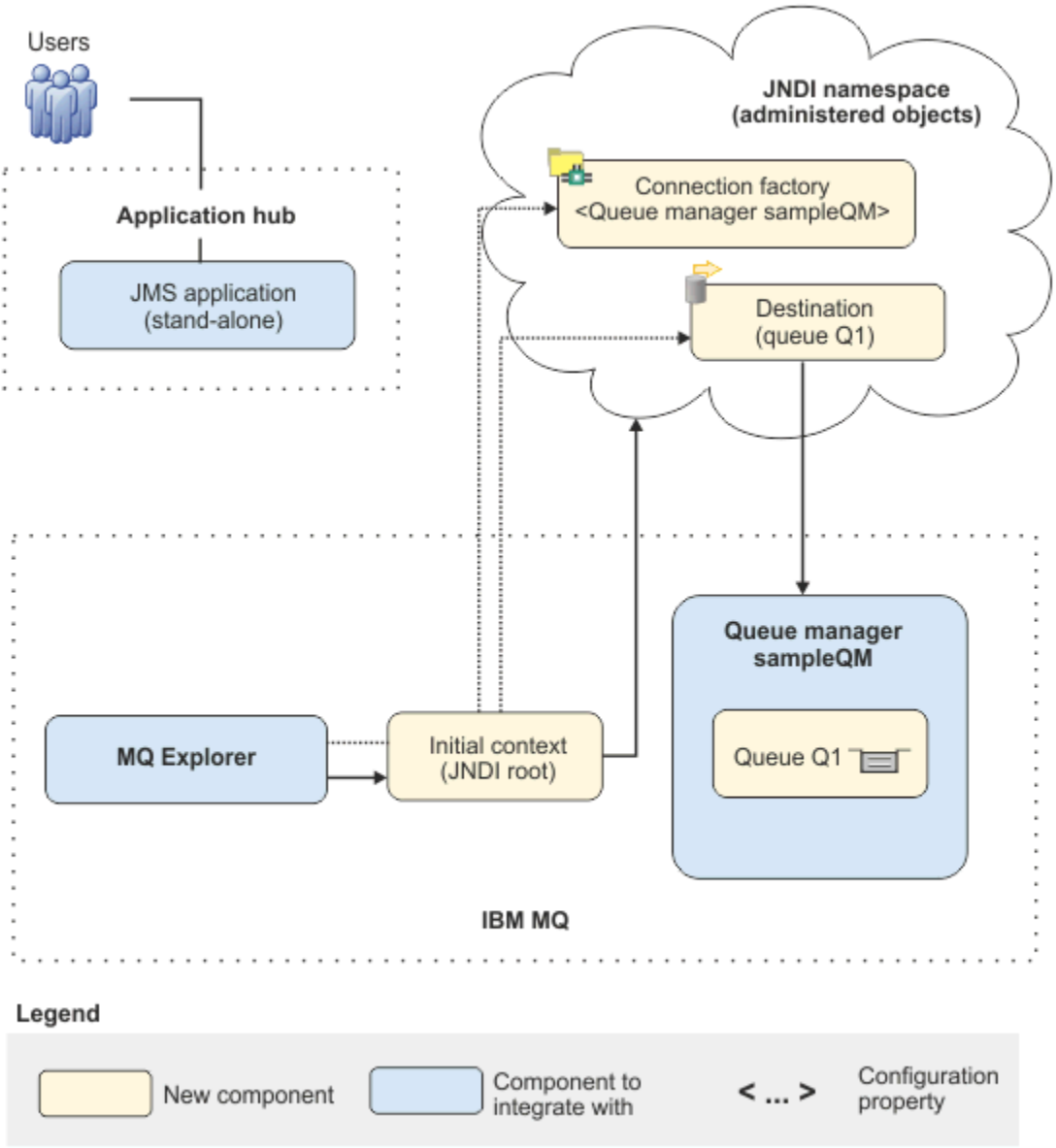


Figura 23. Configurazione IT fornita

Windows Implementazione della soluzione utilizzando la GUI (graphical user interface)

L'implementazione della soluzione in questo scenario comporta l'utilizzo della GUI (graphical user interface) per migrare da una release precedente di IBM MQ, in esecuzione su un sistema operativo Windows , a una release successiva, in esecuzione anche su un sistema operativo Windows , quindi verificare che i gestori code e le code siano stati migrati correttamente alla release successiva.

Prima di iniziare

Se si desidera provare lo scenario, seguire prima le istruzioni per impostare una copia dell'infrastruttura di messaggistica di esempio come descritto in “Creazione di una configurazione IT iniziale” a pagina 118. Questa configurazione di esempio si basa su IBM MQ 9.3.

Informazioni su questa attività

Il processo di migrazione descritto in questo scenario mostra la migrazione di un gestore code da IBM MQ 9.3 a IBM MQ 9.4.

Lo scenario include due opzioni per il metodo di migrazione. È possibile scegliere di provare una o l'altra di queste opzioni o entrambe.

Opzione 1: migrazione in una sola fase

Nella migrazione a fase singola, l'installazione della versione più recente del prodotto sostituisce una versione precedente nella stessa ubicazione di installazione.

Il vantaggio della migrazione a fase singola è che modifica la configurazione di un gestore code nella versione precedente il meno possibile. Le applicazioni esistenti passano automaticamente dal caricamento delle librerie dalla versione precedente al caricamento delle librerie della versione più recente. Utilizzando questo approccio, il sistema non sarà disponibile per l'intero processo.

Opzione 2: migrazione side - by - side

Nella migrazione affiancata, si installa la versione più recente di IBM MQ insieme a una versione precedente. I gestori code continuano ad essere associati alla versione precedente fino a quando non si è pronti a migrarli alla versione successiva.

Con l'approccio affiancato, poiché si disinstalla la versione precedente prima di avviare i gestori code migrati nella versione successiva, è possibile assegnare l'installazione della versione successiva come installazione primaria.

Procedura

1. Creare una configurazione IT iniziale di esempio da utilizzare come punto iniziale per lo scenario come descritto in “Creazione di una configurazione IT iniziale” a pagina 118.
2. Selezionare il metodo da utilizzare per migrare il prodotto, quindi seguire le istruzioni per l'opzione scelta:
   - “Opzione 1: migrazione in una sola fase” a pagina 128
   - “Opzione 2: migrazione side - by - side” a pagina 135

Attività correlate

Migrazione su AIX and Linux: singola fase

Migrazione su AIX and Linux: fianco a fianco

Migrazione di un gestore code da una versione precedente all'ultima versione su Windows

Scelta di un'installazione primaria

Windows Creazione di una configurazione IT iniziale

Questo scenario è stato sviluppato utilizzando una configurazione iniziale (IT) di esempio. Seguire le istruzioni per impostare questa configurazione di esempio per provare lo scenario nello stesso modo in cui è stato originariamente sviluppato.

Informazioni su questa attività

La configurazione IT iniziale per questo scenario, descritta in “Panoramica: configurazione IT iniziale” a pagina 114, include un contesto iniziale, aggiunto per IBM MQ Explorer per connettersi alla root dello spazio dei nomi JNDI. Lo spazio nomi JNDI comprende una factory di connessione, aggiunta per

l'applicazione JMS di esempio da utilizzare per la connessione a IBM MQe una destinazione, aggiunta per l'applicazione JMS di esempio per la connessione alla coda IBM MQ . Tale coda IBM MQ è stata aggiunta anche alla configurazione IT iniziale e viene utilizzata dall'applicazione JMS di esempio.

Procedura

1. Installare IBM MQ 9.3 e verificare l'installazione.
2. Configurare lo spazio dei nomi JNDI e gli oggetti gestiti.
3. Verificare la configurazione IT di esempio.

Windows *Installazione di IBM MQ 9.4 utilizzando il launchpad*

Utilizzare il launchpad di installazione e le procedure guidate per installare la versione di IBM MQ che si desidera impostare come configurazione IT iniziale da utilizzare come punto di partenza per questo scenario.

Prima di iniziare

Prima di avviare questa attività, completare i seguenti controlli:

- Quando si esegue l'installazione, è necessario disporre dell'autorità di amministratore locale.
- Assicurarsi che il nome della macchina non contenga spazi.
- Assicurarsi di disporre di spazio su disco sufficiente. Per ulteriori informazioni, consultare Disk space requriements on Multiplatforms.

Per questo scenario, non è necessario determinare se è necessario definire gli ID utente del dominio Windows per gli utenti IBM MQ , poiché questo requisito non rientra nell'ambito di questo scenario. Per ulteriori informazioni, consultare Creazione di un dominio Active Directory e DNS per IBM MQ .

Prima di installare IBM MQ, verificare che il sistema soddisfi i requisiti hardware e software. Per i dettagli più recenti sui requisiti hardware e software, consultare Requisiti di sistema per 'IBM MQ.

Informazioni su questa attività

Questa attivit ... descrive le operazioni di base per l'installazione di IBM MQ su un sistema operativo Windows .

I programmi di installazione contengono collegamenti a ulteriori informazioni. Il processo di installazione è composto dalle seguenti parti:

1. Avviare il programma di installazione.
2. Utilizzare il launchpad di installazione per verificare e installare i requisiti software, specificare le informazioni di rete e avviare la procedura guidata di installazione IBM MQ .
3. Utilizzare la procedura guidata di installazione di IBM MQ per installare il software e avviare Prepare IBM MQ Wizard.
4. Utilizza Prepare IBM MQ Wizard per avviare il servizio IBM MQ .

Procedura

1. Avviare il programma di installazione.

   In Esplora risorse di Windows , passare alla cartella temporanea in cui è stata scaricata l'immagine di installazione, quindi fare doppio clic su `setup.exe`.

   Il launchpad di installazione è avviato.
2. Utilizzando il launchpad, esaminare e, se necessario, modificare i requisiti software e la configurazione di rete.
   a) Fare clic sul pulsante **Requisiti software** per visualizzare la scheda **Requisiti software** .

b) Verificare che i requisiti software siano stati soddisfatti e che la voce per il requisito visualizzi un segno di spunta verde con le parole 0K . Apportare le correzioni indicate.

Nota: Per visualizzare ulteriori dettagli su qualsiasi requisito, fare clic sul pulsante più (+).

c) Fare clic sul pulsante **Configurazione di rete** per visualizzare la scheda **Configurazione di rete** .

d) Fare clic sul pulsante di opzione **No** .

Nota: Questo scenario presuppone che non sia necessario configurare un ID utente di dominio per IBM MQ. Per ulteriori informazioni relative alla configurazione degli utenti del dominio IBM MQ for Windows , fare clic sul pulsante **Ulteriori informazioni** .

e) Nella scheda **Installazione diIBM MQ** del Launchpad, selezionare la lingua di installazione e fare clic sul pulsante **Avvia IBM MQ Installer** per avviare la procedura guidata di installazione di IBM MQ .

L'utente ha completato la revisione IBM MQ dei requisiti di installazione, ha apportato le modifiche richieste e ha avviato la procedura guidata di installazione di IBM MQ .

3. Utilizzare la procedura guidata di installazione IBM MQ per installare il software e avviare Prepare IBM MQ Wizard.

a) Nella procedura guidata di installazione di IBM MQ , leggere l'accordo di licenza e selezionare la check box **Accetto i termini nell'accordo di licenza** , quindi fare clic su **Avanti**.

b) Fare clic su **Tipico**, quindi fare clic su **Avanti**.

c) Nella pagina **Pronto per l'installazione IBM MQ** , esaminare le informazioni di installazione e fare clic su **Installa**.

Nota: i seguenti dettagli:

- Nome installazione
- Cartella di livello superiore per Program Files
- Cartella di livello superiore per file di dati

Verranno installate le seguenti funzioni:

- IBM MQ Server
- IBM MQ: un'interfaccia grafica per la gestione e il monitoraggio delle risorse di IBM MQ
- Java™ e .NET Messaging e servizi Web
- IBM MQ Toolkit di sviluppo

Il processo di installazione inizia. A seconda del sistema, il processo di installazione può richiedere diversi minuti.

Alla fine del processo di installazione, la finestra IBM MQ Setup visualizza il messaggio `Installation Wizard Completed Successfully` .

d) Fare clic su **Fine**.

IBM MQ è stato installato correttamente Prepare IBM MQ Wizard viene avviato automaticamente, visualizzando la pagina **Benvenuti in Prepare IBM MQ Wizard** .

4. Utilizzare la procedura guidata Prepara MQ per avviare il servizio IBM MQ .

a) Nella pagina Benvenuti in Prepare IBM MQ Wizard , selezionare **Avanti**.

Prepare IBM MQ Wizard visualizza il messaggio `Status: Checking IBM MQ Configuration` e una barra di avanzamento. Una volta completato il processo, viene visualizzata la pagina Configurazione di rete IBM MQ .

b) Nella pagina Configurazione di rete IBM MQ di Prepare IBM MQ Wizard, selezionare **No**.

c) Fare clic su **Avanti**.

Prepare IBM MQ Wizard visualizza un messaggio `Status: starting the IBM MQ Service` e una barra di avanzamento. Una volta completato il processo, la procedura guidata visualizza la pagina Completamento di Prepare IBM MQ Wizard .

d) Selezionare **Avvia IBM MQ Explorer** e scegliere se avviare il Blocco note per visualizzare le note sulla release, quindi fare clic su **Fine**.

IBM MQ Explorer viene avviato.

È stato installato IBM MQed è stato avviato IBM MQ Explorer.

Risultati

IBM MQ è installato sul computer.

Operazioni successive

È possibile creare gli oggetti gestiti utilizzati in questo scenario come descritto in "Configurazione dello spazio nomi JNDI e degli oggetti gestiti" a pagina 121.

Concetti correlati

Requisiti hardware e software sui sistemi di Windows

Introduzione a IBM MQ

Attività correlate

Installazione di un server IBM MQ in Windows

Configurazione di un server IBM MQ

Windows *Configurazione dello spazio nomi JNDI e degli oggetti gestiti*

Definire un contesto iniziale per lo spazio nomi JNDI in IBM MQ Explorer, quindi, nello spazio nomi, definire gli oggetti gestiti che possono essere utilizzati dall'applicazione di esempio.

Informazioni su questa attività

In questa attività, verranno creati i seguenti oggetti in IBM MQ.

- Uno spazio nomi JNDI ubicato in un filesystem locale. Viene utilizzato un file system, poiché è il meccanismo JNDI più semplice per uno scenario di esempio.

  Lo spazio dei nomi JNDI può trovarsi su un file system, su un server LDAP (Lightweight Directory Access Protocol) o su un'altra implementazione JNDI. Se si desidera utilizzare uno spazio dei nomi JNDI su un server LDAP o un'altra implementazione JNDI, è necessario configurare lo spazio dei nomi JNDI e modificare l'applicazione di esempio per fare riferimento allo spazio dei nomi JNDI, come richiesto dall'implementazione.
- Oggetti gestiti nello spazio nomi JNDI. L'applicazione JMS può ricercare gli oggetti gestiti per connettersi a IBM MQ e accedere IBM MQ alle destinazioni con cui inviare o ricevere messaggi.

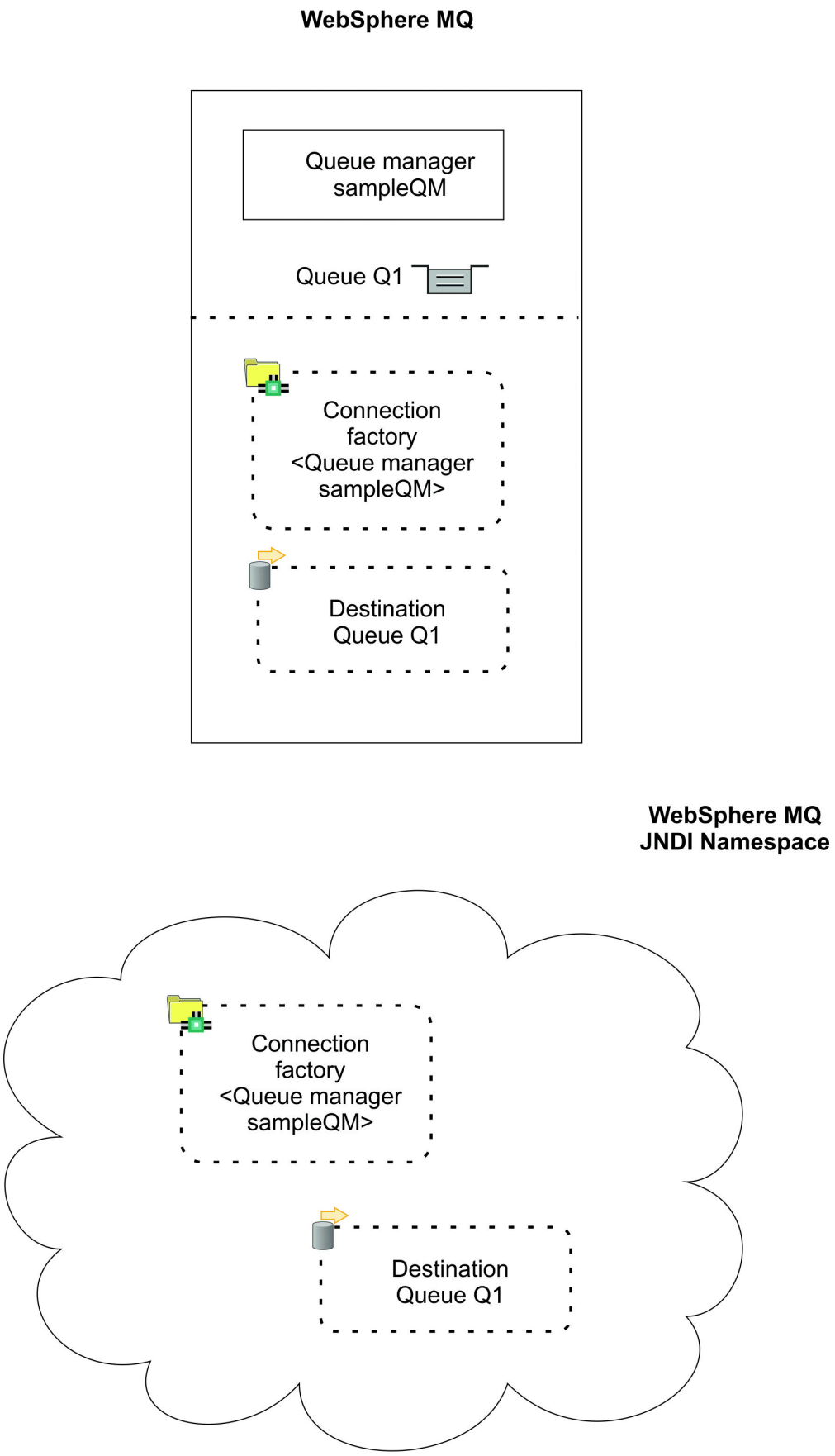


Figura 24. Oggetti creati in IBM MQ

Procedura

1. Avviare IBM MQ Explorer, se non è già avviato, facendo clic su **Start** > **Tutti i programmi** > **IBM MQ** > **IBM MQ Explorer**.

   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 .
2. Creare un gestore code da utilizzare per l'applicazione di esempio.
   a) Fare clic con il tasto destro del mouse su **Gestori code** e selezionare **Nuovo** > **Gestore code ...**.

      Viene avviata la procedura guidata Crea gestore code.
   b) Nel campo **Nome gestore code** , immettere `sampleQM`.

      È possibile scegliere un nome diverso per il gestore code, ma è necessario ricordarsi di utilizzarlo nei passi di configurazione successivi, invece di `sampleQM`.

      Nota: Il nome non deve contenere più di 48 caratteri, dalla seguente serie:

      - Caratteri maiuscoli o minuscoli (A-Z a - z)
      - Caratteri numerici (0-9)
      - Punto (.)
      - Barra (/)
      - Trattino basso (_)
      - Segno percentuale (%)

      I nomi rispettano la distinzione maiuscole/minuscole. Gli oggetti dello stesso tipo devono avere nomi differenti. Ad esempio, due code non possono avere lo stesso nome, ma possono avere un gestore code e una coda.
   c) Nel campo **Dead - letter queue** immettere `SYSTEM.DEAD.LETTER.QUEUE`.

      Questo campo è il nome della coda di messaggi non instradabili che viene creata automaticamente quando si crea il gestore code.

      Una coda di messaggi non recapitabili memorizza i messaggi che non possono essere consegnati alla destinazione corretta, ad esempio perché la coda è piena. Tutti i gestori code devono avere una coda di messaggi non instradabili associata.
   d) Lasciare vuoti gli altri campi e fare clic su **Fine**oppure, se il pulsante è disabilitato, fare clic su **Avanti**.

      Il pulsante **Fine** è disabilitato se il numero di porta è in conflitto con un gestore code esistente, ad esempio il gestore code creato come parte della configurazione predefinita. È necessario continuare con la procedura guidata per modificare il numero di porta predefinito.
   e) Se si è fatto clic su **Avanti**, continuare ad accettare i valori predefiniti e fare clic su **Avanti** su ogni pagina fino a quando non si arriva alla pagina finale della procedura guidata, quando il pulsante **Fine** diventa disponibile. Modificare il numero di porta specificato, ad esempio in 1415, e fare clic su **Fine**.

   IBM MQ visualizza una finestra di dialogo mentre il gestore code viene creato e avviato.
3. Aggiungere un contesto iniziale per lo *spazio dei nomi JNDI* quindi connettersi IBM MQ Explorer a tale contesto

   Prima di poter utilizzare IBM MQ Explorer per creare e configurare gli oggetti gestiti JMS , è necessario aggiungere un contesto iniziale per definire la root dello spazio nomi JNDI in cui sono memorizzati gli oggetti gestiti.

   Ogni volta che si desidera utilizzare IBM MQ Explorer per creare o gestire oggetti gestiti nello spazio nomi JNDI, è necessario connettere IBM MQ Explorer al contesto iniziale dello spazio nomi JNDI.

   a) Nel riquadro IBM MQ Explorer - **Navigator**, fare clic con il tasto destro del mouse su **JMS Oggetti amministrati**, quindi selezionare **Aggiungi contesto iniziale**.

      Questa azione visualizza la pagina " **Dettagli connessione** " .
   b) In " **Dove si trova lo spazio dei nomi JNDI** ", selezionare la check box **File system** .

c) Nel campo **Directory binding** , immettere `C:\JNDI-Directory`.

Questo valore corrisponde all'ubicazione dello spazio nomi JNDI specificata nell'applicazione JMS di esempio. Se è necessario specificare una directory JNDI differente, è necessario modificare l'applicazione in modo che corrisponda.

Se la directory non esiste sul sistema, la finestra visualizza il messaggio `Specified location does not exist or is not readable` . Fare clic su **Sfoglia ...** per aprire una finestra del file system, passare a `Local Disk (C:)`, quindi fare clic su **Crea nuova cartella** per creare la cartella `JNDI-Directory` . Fare clic su **OK**.

Fare clic su **Avanti**.

d) Nella pagina **Preferenze utente** , lasciare le impostazioni predefinite.

- **Nickname di contesto**: l'ubicazione dello spazio nomi JNDI verrà utilizzata come nickname per visualizzare il contesto iniziale in IBM MQ Explorer.
- **Connetti immediatamente al termine**: questa opzione connette IBM MQ Explorer al namespace JNDI una volta terminata la creazione del contesto iniziale, in modo che sia possibile creare immediatamente gli oggetti gestiti.
- **Riconnessione automatica al contesto all'avvio**: questa opzione non è selezionata, poiché di solito non è necessario IBM MQ Explorer riconnettersi automaticamente al contesto iniziale ogni volta che si chiude e si riapre IBM MQ Explorer.

Se si utilizza abitualmente IBM MQ Explorer per creare o gestire oggetti gestiti nello spazio dei nomi JNDI, è possibile selezionare la casella di spunta **Riconnetti automaticamente al contesto all'avvio** per consentire a IBM MQ Explorer di riconnettersi automaticamente al contesto iniziale ogni volta che viene avviato IBM MQ Explorer . Questa opzione consente di risparmiare la connessione manuale di IBM MQ Explorer al contesto iniziale.

Fare clic su **Fine** per creare e visualizzare il contesto iniziale.

4. Creare un oggetto gestito della factory di connessione.

Un oggetto gestito della produzione connessioni definisce una serie di proprietà di configurazione standard per le connessioni. Un'applicazione utilizza un factory di connessione per creare una connessione a IBM MQ.

a) Nel pannello IBM MQ Explorer - **Navigator** , espandere **JMS Oggetti gestiti**, quindi espandere il contesto iniziale, etichettato **file:/C: /JNDI-Directory/**.

b) Fare clic con il tastino destro su **Factory di connessione**, quindi selezionare **Nuovo** > **Factory di connessione ...**.

Questa azione visualizza la procedura guidata **Nuovo factory di connessione**

c) Nel campo Nome, immettere `myCF`

L'applicazione JMS di esempio contiene codice che ricerca una factory di connessione con il nome `myCF`. Se è necessario utilizzare un nome diverso, è necessario modificare l'applicazione in modo che corrisponda.

IBM MQ viene utilizzato per il provider di messaggistica, poiché l'applicazione di esempio utilizza la messaggistica point - to - point.

Fare clic su **Avanti**.

d) Lasciare il tipo di factory di connessione come **Factory di connessione**, poiché questa opzione è la più flessibile per l'utilizzo generale di JMS .

Un factory di connessione indipendente dal dominio consente alle applicazioni JMS di utilizzare sia la messaggistica point - to - point che la messaggistica di pubblicazione / sottoscrizione, soprattutto se si desidera che l'applicazione JMS esegua entrambi i tipi di messaggistica nella stessa transazione.

Se un'applicazione JMS è progettata per utilizzare solo la messaggistica point - to - point o solo la messaggistica di pubblicazione / sottoscrizione, è possibile selezionare il dominio di messaggistica specifico quando si crea la factory di connessione e viene creata una factory di connessione specifica del dominio (coda o argomento).

e) Lasciare il supporto per le transazioni XA come cancellato.

L'applicazione di esempio non utilizza transazioni conformi a XA.

IBM MQ JMS supporta le transazioni conformi a XA in modalità bind. Se si desidera che l'applicazione di esempio utilizzi transazioni conformi a XA, è necessario modificare l'applicazione di esempio.

Fare clic su **Avanti**.

f) Lasciare il trasporto come **Bind**.

L'applicazione JMS di esempio che utilizza la factory di connessione viene eseguita sullo stesso computer del gestore code, quindi può utilizzare il trasporto in modalità bind. Questa opzione significa che l'applicazione JMS si connette direttamente al gestore code e offre un vantaggio sulle prestazioni rispetto alla modalità client alternativa.

Fare clic su **Avanti**, quindi su **Avanti** .

g) Nella pagina **Modifica proprietà** , selezionare **Connessione** dal menu sulla sinistra, quindi nel riquadro **Connessione** selezionare sampleQM come **Gestore code di base**.

Il gestore code di base è il gestore code a cui si connetterà l'applicazione. Lasciare questo valore vuoto se si desidera che l'applicazione sia in grado di connettersi a più di un gestore code.

h) Fare clic su **Fine**.

IBM MQ visualizza una finestra di dialogo per mostrare che l'oggetto è stato creato correttamente. Fare clic su **OK** per chiudere la finestra di dialogo.

5. Creare un oggetto gestito di destinazione.

Un oggetto gestito di destinazione identifica la coda IBM MQ a cui le applicazioni inviano i messaggi o da cui un'applicazione riceve i messaggi o entrambi. Un'applicazione ricerca la destinazione nello spazio nomi JNDI per creare una connessione alla coda IBM MQ .

Nella messaggistica di pubblicazione / sottoscrizione, la destinazione identifica un argomento piuttosto che una coda.

a) Nel pannello IBM MQ Explorer - **Navigator** , espandere **JMS Oggetti gestiti**, quindi espandere il contesto iniziale, etichettato **file:/C: /JNDI-Directory/**.

b) Fare clic con il pulsante destro del mouse su **Destinazioni**, quindi selezionare **Nuovo** > **Destinazione ...**.

Viene visualizzata la procedura guidata **Nuova destinazione** .

c) Nel campo **Nome** , immettere `myQueue`.

Lasciare **Tipo** come **Coda**.

L'applicazione JMS di esempio contiene codice che ricerca una destinazione con il nome `myQueue`. L'applicazione JMS di esempio utilizza la messaggistica point-to-point, quindi richiede una destinazione di tipo coda. Le destinazioni di tipo argomento vengono utilizzate per la messaggistica di pubblicazione / sottoscrizione.

d) Selezionare la casella di controllo **Avviare la procedura guidata per creare una coda MQ corrispondente** .

L'oggetto di destinazione richiede una coda IBM MQ corrispondente ed è utile utilizzare IBM MQ Explorer per creare entrambi insieme. Quando si completa la procedura guidata **Nuova destinazione** , si apre la procedura guidata **Crea una coda MQ** , con molti dei dettagli di destinazione associati alla coda IBM MQ .

Fare clic su **Avanti**.

Fare nuovamente clic su **Avanti** .

e) Nella pagina " **Modifica proprietà** " , fare clic su **Seleziona ...** accanto a **Gestore code** Selezionare il gestore code sampleQM creato in precedenza e fare clic su **OK**.

f) Specificare `Q1` come nome della coda IBM MQ .

È possibile scegliere un nome diverso per la coda, ma è necessario ricordarsi di utilizzarlo nei passi di configurazione successivi, al posto di `Q1`.

Nota: Il nome non deve contenere più di 48 caratteri, dalla seguente serie:

- Caratteri maiuscoli o minuscoli (A-Z a - z)
- Caratteri numerici (0-9)
- Punto (.)
- Barra (/)
- Trattino basso (_)
- Segno percentuale (%)

I nomi rispettano la distinzione maiuscole/minuscole. Gli oggetti dello stesso tipo devono avere nomi differenti. Ad esempio, due code non possono avere lo stesso nome, ma possono avere un gestore code e una coda.

g) Fare clic su **Fine**.

Viene avviata la procedura guidata **Crea una coda MQ** .

Se la procedura guidata non viene avviata, è possibile che non sia stata selezionata la check box **Avvia procedura guidata per creare una coda MQ** corrispondente in un passo precedente. Nel riquadro IBM MQ Explorer **Navigator** , espandere il gestore code **sampleQM** , fare clic con il tasto destro del mouse su **Code**e selezionare **Nuovo** > **Coda locale ...**.

6. Creare una coda IBM MQ corrispondente.

L'oggetto gestito di destinazione creato precedentemente rappresenta una coda IBM MQ . Questa coda è dove vengono memorizzati i messaggi JMS .

a) Fare clic su **Avanti** per accettare il gestore code sampleQM specificato in precedenza.

b) Fare clic su **Avanti**.

c) Fare clic su **Fine** per creare la coda IBM MQ utilizzando le informazioni dall'oggetto gestito di destinazione creato in precedenza.

IBM MQ visualizza una finestra di dialogo con il messaggio che l'oggetto è stato creato correttamente.

La nuova coda è ora visibile nella sezione **Code** nel gestore code.

Risultati

A questo punto sono stati creati gli oggetti IBM MQ richiesti per utilizzare l'applicazione JMS di esempio.

Operazioni successive

Ora è possibile verificare di aver configurato correttamente IBM MQ per l'utilizzo con l'applicazione di esempio come descritto in “Verifica della configurazione IT di esempio” a pagina 126.

Windows *Verifica della configurazione IT di esempio*

Eseguire l'applicazione JMS autonoma di esempio per inviare e ricevere messaggi tramite IBM MQe verificare di aver configurato correttamente IBM MQ per l'utilizzo con l'applicazione di esempio.

Prima di iniziare

Scarica il pacchetto dell'applicazione di esempio. Fare clic sul seguente collegamento e salvare il file sul computer su cui si sta installando IBM MQ: sampleJMSApp.zip, quindi estrarre il contenuto. Il pacchetto contiene un file di esempio JMS application `.jar` e file batch per l'esecuzione dell'applicazione.

- Il file `sampleJMSApp.jar` di esempio e i file `.cmd` devono trovarsi nella stessa directory.
- I file `.cmd` utilizzano le variabili di ambiente per impostare il percorso classe per l'esecuzione dell'applicazione JMS . Quando si esegue l'applicazione JMS , se viene visualizzato un Java `java.lang.NoClassDefFoundError`, potrebbe essere necessario modificare la riga del percorso classi nel file di comandi.

Informazioni su questa attività

L'applicazione JMS comprende un client richiedente, che invia il messaggio iniziale, e un client risponditore, che riceve il messaggio e invia una risposta. I file batch forniti eseguono le seguenti azioni:

- `runresponder.cmd` apre una finestra del prompt dei comandi in cui il client responder viene avviato e attende un messaggio.
- `runrequester.cmd` apre una finestra di richiesta comandi separata in cui il client richiedente viene avviato, quindi invia un messaggio di richiesta e riceve una risposta.

Con due finestre di prompt dei comandi, è possibile visualizzare le azioni del richiedente e del responder separatamente e in modo più chiaro.

Procedura

1. Fare doppio clic sul file `runresponder.cmd` .

   Nella finestra del prompt dei comandi, etichettata **finestra Responder**, il client responder viene avviato e attende un messaggio.

   ```
   > Connection factory located in JNDI.> Destination located in JNDI.> Creating connection to
   QueueManager.> Created connection.
   > Waiting for message.
   ```

2. Fare doppio clic sul file `runrequester.cmd` .

   Nella **finestra del richiedente**, osservare i messaggi del richiedente. Nella **finestra Rispondi**, osservare i messaggi del risponditore aggiornati; il messaggio ricevuto (dal client richiedente) e il messaggio di risposta inviato.

Risultati

Nella finestra del prompt dei comandi, etichettata **Finestra del richiedente**, il client del richiedente mostra lo stato della connessione, il messaggio che ha inviato, quindi il messaggio di risposta che ha ricevuto dal client del risponditore:

```
> Connection factory located in JNDI.> Destination located in JNDI.> Creating connection to
QueueManager.> Connection created.
> Sending stock request for 'BakedBeans'> Sent Message
ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002b02
> Received Message ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002902 for 'B
akedBeans - 15 tins in stock'
> Closing connection to QueueManager.> Closed Connection.
-----------------------------------------------------
In this window, observe the messages sent through IBM MQ:
- The request message sent
- The reply message received
-----
When ready, press any key to close this window
Press any key to continue . . .
```

Nella **finestra Rispondi**, osservare i messaggi del risponditore aggiornati; il messaggio che ha ricevuto (dal client richiedente) e il messaggio di risposta che ha inviato:

```
> Connection factory located in JNDI.> Destination located in JNDI.> Creating connection to
QueueManager.> Created connection.
> Waiting for message.

> Received Message ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002b02 for 'B
akedBeans'
> Sending Reply Message 'BakedBeans - 15 tins in stock'> Sent Message
ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002902
> Closing connection to QueueManager.> Closed connection.
-----------------------------------------------------
In this window, observe the updated responder messages
- The request message received (from the requester)
- The reply message sent
-----
When ready, press any key to close this window
Press any key to continue . . .
```

I messaggi mostrati nelle due finestre dei comandi verificano che i client del richiedente e del responder dell'applicazione di esempio possano comunicare tra loro tramite IBM MQ.

Operazioni successive

È ora possibile avviare la migrazione dell'installazione di esempio di IBM MQ 9.3 a una release successiva di IBM MQ utilizzando una delle seguenti opzioni di migrazione:

- Per migrare utilizzando il metodo di migrazione a fase singola, seguire le istruzioni in “Opzione 1: migrazione in una sola fase” a pagina 128.
- Per eseguire la migrazione utilizzando il metodo di migrazione affiancato, seguire le istruzioni riportate in “Opzione 2: migrazione side - by - side” a pagina 135.

Opzione 1: migrazione in una sola fase

L'opzione 1 di questo scenario mostra come eseguire la migrazione da una versione precedente a una versione successiva di IBM MQ quando si utilizza il metodo di migrazione a fase singola. Con una migrazione a fase singola, l'installazione di una versione successiva di IBM MQ sostituisce una versione precedente nella stessa ubicazione di installazione.

Prima di iniziare

Il punto di partenza per questo scenario è la configurazione IT iniziale descritta in “Panoramica: configurazione IT iniziale” a pagina 114.

Prima di iniziare questa attività, attenersi alle istruzioni in “Creazione di una configurazione IT iniziale” a pagina 118 per impostare una configurazione IT iniziale.

Informazioni su questa attività

Con una migrazione a fase singola, è possibile scegliere di disinstallare la versione precedente di IBM MQ prima di installare la versione più recente o di installare la versione più recente senza prima disinstallare la versione precedente (ossia, eseguire la migrazione). In entrambi i casi, la release successiva viene installata nella stessa directory della release precedente. L'opzione 1 di questo scenario mostra una migrazione a singolo stadio in cui la versione precedente viene disinstallata prima di installare la versione più recente. I dati del gestore code non vengono rimossi durante il processo di disinstallazione, il che significa che i gestori code di esempio utilizzati in questo scenario vengono conservati e rilevati quando si installa la versione più recente di IBM MQ.

Procedura

1. Arrestare i gestori code in esecuzione nella versione precedente di IBM MQed eseguire il backup dei dati del gestore code.
2. Disinstallare la versione precedente di IBM MQ da cui si sta eseguendo la migrazione, senza rimuovere i dati del gestore code.
3. Installare IBM MQ 9.4 utilizzando il launchpad..
4. Utilizzare IBM MQ Explorer per verificare la nuova IBM MQ 9.4 installazione.

   Verificare che i gestori code siano stati migrati correttamente dalla release precedente e che sia possibile inserire e ricevere messaggi dalle code migrate.

Attività correlate

Migrazione su AIX and Linux: singola fase

Windows *Preparazione alla migrazione*

Prima di migrare a una versione più recente di IBM MQ, è necessario arrestare il gestore code ed eseguire il backup dei dati del gestore code.

Informazioni su questa attività

Se si esegue la migrazione da una versione precedente di IBM MQ senza prima eseguire il backup del sistema, non è possibile ripristinare la versione precedente, se si decide di non continuare con la migrazione. Il backup del sistema prima di installare la nuova versione consente di eseguire il backout dell'aggiornamento, se necessario. Se si esegue il backout di un aggiornamento, tuttavia, non è possibile ripristinare alcun lavoro, come le modifiche ai messaggi e agli oggetti, eseguite dalla versione più recente di IBM MQ.

Prima di eseguire il backup, arrestare il gestore code di cui si sta per eseguire il backup, che per questo scenario è sampleQM. Se si tenta di eseguire un backup di un gestore code in esecuzione, il backup potrebbe non essere congruente a causa di eventuali aggiornamenti in corso durante la copia dei file.

Procedura

1. Aprire IBM MQ Explorer.

   Fare clic su **Avvia** > **Tutte le applicazioni** > **IBM MQ** > **IBM MQ Explorer**.
2. Arrestare il gestore code sampleQM.
   a) Nella vista Navigator , fare clic con il tasto destro del mouse sul gestore code sampleQM.
   b) Fare clic su **Arresta**.

      Viene visualizzata la finestra **Termina gestore code** .
   c) Selezionare **Controllato**, quindi fare clic su **OK**.

      Selezionando l'opzione `Controllato` , il gestore code viene arrestato in modo controllato e ordinato. L'opzione **Immediata** , che forza l'arresto del gestore code, viene generalmente utilizzata solo se l'arresto controllato non viene completato correttamente.

   Il gestore code viene arrestato. In IBM MQ, l'icona accanto al gestore code sampleQM viene modificata in modo da includere una freccia rossa che punta verso il basso.
3. Chiudere IBM MQ Explorer.
4. Eseguire il backup dei dati del gestore code.

   Eseguire copie di tutti i seguenti dati, accertandosi di includere tutte le directory di backup. Alcune directory potrebbero essere vuote, ma sono necessarie tutte se è necessario ripristinare il backup in un secondo momento, quindi salvarle.

   - I dati del gestore code presenti in `C:\Programmi\ IBM \ MQ\Qmgrs`.
   - Le directory del file di log per i gestori code che si trovano in `C:\Programmi\ IBM \ MQ\log`, incluso il file di controllo log `amqhlctl.lfh`.
   - I file di configurazione presenti in `C:\Programmi\ IBM \ MQ\Config`.
   - IBM MQ 9.3 .ini e le voci di registro. Le informazioni sul gestore code sono memorizzate nel file .ini e possono essere utilizzate per ripristinare una versione precedente del prodotto.
5. Arrestare IBM MQ.
   a) Arresta il servizio IBM MQ.

      Fare clic con il tasto destro del mouse su **IBM MQ** nella barra delle applicazioni, quindi fare clic su **Arresta IBM MQ**.

      Viene visualizzata una finestra di dialogo con il seguente messaggio:

      ```
      La chiusura di IBM MQ terminerà tutti i gestori code in esecuzione e
      IBM MQ processi. Si è certi di voler proseguire? (AMQ4102)
      ```
   b) Fare clic su **Sì**, quindi attendere l'arresto di IBM MQ .
   c) Una volta arrestato IBM MQ , fare clic con il tasto destro del mouse sull'icona **IBM MQ** nella barra delle applicazioni, quindi fare clic su **Esci**.

Risultati

È stato arrestato il gestore code che si sta per migrare alla release successiva di IBM MQ ed è stato eseguito un backup dei dati del gestore code.

Operazioni successive

È ora possibile disinstallare IBM MQ come descritto in “Disinstallazione della versione precedente” a pagina 130.

Attività correlate

Backup dei dati del gestore code

Windows *Disinstallazione della versione precedente*

Disinstallare la versione precedente utilizzando il pannello di controllo. Per una migrazione a una singola fase su Windows, la disinstallazione della versione precedente del prodotto prima di installare la versione successiva è facoltativa.

Prima di iniziare

Prima di iniziare questa attività, è necessario arrestare i gestori code, chiudere IBM MQ Explorer e arrestare IBM MQ come descritto in “Preparazione alla migrazione” a pagina 128.

Informazioni su questa attività

In questa attività, disinstallare IBM MQ utilizzando il pannello di controllo Windows . I dati del gestore code non vengono rimossi come parte del processo di disinstallazione, il che significa che i gestori code di esempio utilizzati in questo scenario vengono conservati e possono essere rilevati quando si installa la versione più recente del prodotto.

Se è necessario disinstallare o meno la versione precedente del prodotto prima di installare la versione successiva dipende dal sistema operativo. Sui sistemi Windows , la disinstallazione è facoltativa ed è possibile, in alternativa, installare la versione più recente senza disinstallare quella precedente. Notare che in questo caso, alcune delle opzioni e dei messaggi visualizzati durante l'installazione sarebbero diversi da quelli visualizzati quando è stata disinstallata prima la versione precedente. Per ulteriori informazioni sulle piattaforme su cui è necessario disinstallare la versione precedente prima di installare la versione più recente, consultare Migrazione su AIX and Linux: fase singola.

Procedura

1. Aprire il Pannello di controllo Windows facendo clic su **Start> Pannello di controllo> Disinstalla un programma**.
2. Nella finestra **Programmi e funzioni** , individuare la voce per l'installazione che si desidera eliminare, ad esempio IBM WebSphere MQ (Installation1), e fare clic su **Disinstalla**.

   Il processo di disinstallazione inizia e viene eseguito fino al completamento. Una volta completato il processo, la versione precedente di IBM MQ viene rimossa dal computer e non viene più visualizzata nell'elenco dei programmi.

Risultati

La versione precedente di IBM MQ è stata rimossa dal computer. Tuttavia, i dati del gestore code non sono stati rimossi.

Operazioni successive

Ora è possibile installare la versione più recente di IBM MQ come descritto in “Installazione di IBM MQ 9.4 mediante il launchpad” a pagina 131.

Attività correlate

Disinstallare IBM MQ su sistemi Windows

Windows *Installazione di IBM MQ 9.4 mediante il launchpad*

Utilizzare il launchpad di installazione e le procedure guidate per installare la versione più recente di IBM MQ sullo stesso computer Windows su cui è stata installata la versione precedente.

Prima di iniziare

Prima di avviare questa attività, scaricare il file compresso che contiene l'immagine di installazione, quindi decomprimerlo in una directory temporanea.

Questa attività presuppone che sia stata precedentemente disinstallata la versione precedente di IBM MQ da cui si sta eseguendo la migrazione come descritto in "Disinstallazione della versione precedente" a pagina 130. Se si installa la versione più recente senza prima disinstallare la versione precedente, alcune delle opzioni e dei messaggi visualizzati durante il processo di installazione saranno diversi da quelli descritti in questa attività.

Prima di avviare questa attività, completare i seguenti controlli:

- Quando si esegue l'installazione, è necessario disporre dell'autorità di amministratore locale. Definire questa autorizzazione mediante le funzioni Windows .
- Assicurarsi che il nome della macchina non contenga spazi.
- Assicurarsi di disporre di spazio su disco sufficiente. Per ulteriori informazioni, consultare Disk space requriements on Multiplatforms.

Per questo scenario, non è necessario determinare se è necessario definire gli ID utente del dominio Windows per gli utenti IBM MQ , poiché questo requisito non rientra nell'ambito di questo scenario. Per ulteriori informazioni, consultare Creazione di un dominio Active Directory e DNS per IBM MQ .

Prima di installare IBM MQ, verificare che il sistema soddisfi i requisiti hardware e software. Per i dettagli più recenti sui requisiti hardware e software, consultare Requisiti di sistema per 'IBM MQ.

Informazioni su questa attività

Questa attività descrive i passi di base per l'installazione di IBM MQ su un sistema operativo Windows quando si esegue la migrazione da una versione precedente.

Nota: Le ubicazioni predefinite del programma e della directory dei dati sono le stesse per IBM MQ 9.0 e versioni successive. Pertanto, non è necessario modificare la specifica del programma e le directory di dati durante la migrazione da IBM MQ 9.0 a una versione successiva. Tuttavia, quando si migra da versioni precedenti a IBM MQ 9.0, ci sono delle differenze nelle posizioni predefinite che è necessario considerare. Per ulteriori informazioni, consultare Program and data directory locations on Windows.

I programmi di installazione contengono collegamenti a ulteriori informazioni, se richieste durante il processo di installazione. Il processo di installazione è composto dalle seguenti parti:

1. Utilizzare il Launchpad per controllare e installare i requisiti software, specificare le informazioni di rete e avviare la procedura guidata di installazione IBM MQ .
2. Utilizzare la procedura guidata di installazione IBM MQ per installare il software e avviare Prepare IBM MQ Wizard.
3. Utilizza Prepare IBM MQ Wizard per avviare il servizio IBM MQ .

Procedura

1. Avviare il programma di installazione.

   In Esplora risorse di Windows , passare alla cartella temporanea in cui è stata scaricata l'immagine di installazione, quindi fare doppio clic su `setup.exe`.

   Il launchpad di installazione è avviato.

2. Avviare il Launchpad, rivedere e, se necessario, modificare i requisiti software e la configurazione di rete.
   a) Passare alla directory del software IBM MQ e fare doppio clic su `Setup.exe` per avviare il Launchpad.
   b) Fare clic sul pulsante **Requisiti software** per visualizzare la scheda **Requisiti software** .
   c) Verificare che i requisiti software siano stati soddisfatti e che la voce per il requisito visualizzi un segno di spunta verde con le parole 0K . Apportare le correzioni indicate.

      Nota:

      Per i dettagli di un requisito, fare clic sulla casella di spunta per espandere una scheda di informazioni.
   d) Fare clic sul pulsante **Configurazione di rete** per visualizzare la scheda **Configurazione di rete** .
   e) Fare clic sul pulsante di opzione **No** .

      Nota: Questo scenario presuppone che non sia necessario configurare un ID utente di dominio per IBM MQ. Per ulteriori informazioni relative alla configurazione degli utenti del dominio IBM MQ for Windows , fare clic sul pulsante **Ulteriori informazioni** .
   f) Nella scheda **IBM MQ Installazione** del Launchpad, selezionare la lingua di installazione e fare clic su **Avvia IBM MQ Installer** per avviare la procedura guidata di installazione di IBM MQ .

   È stata completata l'impostazione di IBM MQ soddisfacendo o specificando i propri requisiti di installazione e si è avviata la procedura guidata di installazione di IBM MQ .
3. Utilizzare la procedura guidata di installazione IBM MQ per installare il software e avviare Prepare IBM MQ Wizard.
   a) Nella procedura guidata di installazione di IBM MQ , leggere l'accordo di licenza e fare clic sulla casella di spunta **Accetto i termini nell'accordo di licenza** , quindi fare clic su **Avanti**.
   b) Fare clic su **Tipico**, quindi fare clic su **Avanti**.
   c) Nella pagina **Pronto per l'installazione IBM MQ** , esaminare le informazioni di installazione, quindi fare clic su **Installa**.

      Le informazioni sull'installazione includono i seguenti dettagli:

      - Nome installazione
      - Cartella di livello superiore per Program Files
      - Cartella di livello superiore per File di dati

      Sono installate le seguenti funzionalità:

      - IBM MQ Server
      - IBM MQ: un'interfaccia grafica per la gestione e il monitoraggio delle risorse di IBM MQ
      - Java™ e .NET Messaging e servizi Web
      - IBM MQ Toolkit di sviluppo

      Il processo di installazione inizia. In base al sistema, il processo di installazione può richiedere diversi minuti.

      Alla fine del processo di installazione, la finestra IBM MQ Setup visualizza il messaggio `Installation Wizard Completed Successfully` .
   d) Fare clic su **Fine**.

   IBM MQ è stato installato correttamente Prepare IBM MQ Wizard viene avviato automaticamente, visualizzando la pagina **Benvenuti in Prepare IBM MQ Wizard** .
4. Utilizza Prepare IBM MQ Wizard per avviare il servizio IBM MQ .
   a) Nella pagina Benvenuti in Prepare IBM MQ Wizard , selezionare **Avanti**.

      Prepare IBM MQ Wizard visualizza il messaggio `Status: Checking IBM MQ Configuration` e una barra di avanzamento. Una volta completato il processo, viene visualizzata la pagina Configurazione di rete IBM MQ .

b) Nella pagina Configurazione di rete IBM MQ di Prepare IBM MQ Wizard, selezionare **No**.

c) Fare clic su **Avanti**.

Prepare IBM MQ Wizard visualizza un messaggio `Status: starting the IBM MQ Service` e una barra di avanzamento. Una volta completato il processo, la procedura guidata visualizza la pagina Completamento di Prepare IBM MQ Wizard .

d) Selezionare **Avvia IBM MQ Explorer** e scegliere se avviare il Blocco note per visualizzare le note sulla release, quindi fare clic sul pulsante **Fine** .

IBM MQ Explorer viene avviato.

Risultati

È stato installato IBM MQed è stato avviato IBM MQ Explorer.

Operazioni successive

Ora che è stata installata la versione più recente di IBM MQ, è possibile verificare che i gestori code di esempio siano stati migrati correttamente e che sia possibile inserire e richiamare messaggi dalle code migrate come descritto in “Verifica dell'installazione di IBM MQ 9.4” a pagina 133.

Concetti correlati

Dove trovare le immagini di installazione scaricabili

Attività correlate

Installazione di un server IBM MQ in Windows

Verifica dell'installazione di IBM MQ 9.4

Dopo aver installato IBM MQ 9.4, utilizzare IBM MQ Explorer per verificare che i gestori code e le code siano stati migrati correttamente dalla release precedente, quindi verificare che sia possibile utilizzare l'applicazione di esempio.

Informazioni su questa attività

Una volta verificato che il gestore code migrato, sampleQM, è visibile nella vista Navigator di IBM MQ Explorer, verificare che sia possibile inserire un messaggio e richiamare un messaggio dalla coda migrata, quindi verificare che sia ancora possibile eseguire l'applicazione di esempio.

Procedura

1. Se IBM MQ Explorer non è in esecuzione, avviarlo ora.

   Fare clic su **Start> Tutti i programmi> IBM MQ > IBM MQ Explorer**.
2. Verificare che i gestori code siano stati migrati correttamente alla versione più recente di IBM MQ:
   a) Nella vista Navigator, espandere la cartella **Gestori code**.
   b) Verificare che sia possibile visualizzare sampleQM del gestore code nella cartella **Gestori code** .
   c) Espandere il gestore code sampleQM, fare clic sulla cartella **Code** e verificare che sia possibile visualizzare la coda Q1 nella vista Contenuto.
3. Se il gestore code sampleQM non è già avviato, avviarlo ora.
   a) Nella vista Navigator , espandere il nodo dei gestori code.
   b) Fare clic con il tasto destro del mouse sul gestore code sampleQM, quindi fare clic su **Avvia**.
4. Verificare che sia possibile inserire un messaggio nella coda Q1.
   a) Nella vista Navigator, espandere la cartella **Gestori code**.
   b) Espandere il gestore code sampleQM, fare clic sulla cartella **Code** .
   c) Nella vista Contenuto, fare clic con il tasto destro del mouse sulla coda Q1, quindi fare clic su **Inserisci messaggio di prova**.

   Viene aperta la finestra **Inserisci messaggio di prova**.

d) Nel campo **Dati messaggio** , immettere del testo, ad esempio `Hello queue!`, quindi fare clic su **Inserisci messaggio**.

Il campo **Dati del messaggio** verrà cancellato e il messaggio verrà inserito sulla coda.

e) Fare clic su **Chiudi**.

Nella vista Contenuto, notare che il valore **Profondità coda corrente** della coda è ora 1. Se la colonna Profondità della coda corrente non è visibile, potrebbe essere necessario scorrere verso destra la vista Contenuto.

5. Verificare che sia possibile richiamare il messaggio dalla coda Q1.

a) Nella vista Navigator , espandere la cartella **Gestori code** ,

b) Espandere il gestore code sampleQM e fare clic sulla cartella **Code** .

c) Nella vista Contenuto, fare clic con il tasto destro del mouse sulla coda Q1, quindi selezionare **Sfoglia messaggi**.

Il browser dei messaggi viene aperto per mostrare l'elenco dei messaggi attualmente in coda.

d) Fare doppio clic sull'ultimo messaggio per aprire la finestra delle proprietà.

Nella pagina **Dati** della finestra delle proprietà, nel campo **Dati del messaggio** è riportato il contenuto del messaggio in formato leggibile.

6. Verificare che sia possibile eseguire l'applicazione di esempio.

a) Fare doppio clic sul file `runresponder.cmd` .

Nella finestra del prompt dei comandi, etichettata **finestra Responder**, il client responder viene avviato e attende un messaggio.

```
> Factory di connessione ubicato in JNDI.> Destinazione ubicata in JNDI.> Creazione della
connessione a QueueManager.> Connessione creata.
> In attesa di messaggio.
```

b) Fare doppio clic sul file `runrequester.cmd` .

Nella **finestra del richiedente**, osservare i messaggi del richiedente. Nella **finestra Rispondi**, osservare i messaggi del risponditore aggiornati; il messaggio ricevuto (dal client richiedente) e il messaggio di risposta inviato.

Nella finestra del prompt dei comandi, etichettata **Finestra del richiedente**, il client del richiedente mostra lo stato della connessione, il messaggio che ha inviato, quindi il messaggio di risposta che ha ricevuto dal client del risponditore:

```
> Factory di connessione ubicato in JNDI.> Destinazione presente in JNDI.> Creazione della
connessione a QueueManager.> Connessione creata.
> Invio richiesta stock per 'BakedBeans'> Messaggio inviato
ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002b02
> Messaggio ricevuto ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002902 per ' B
akedBeans - 15 contenitori in magazzino '
> Chiusura della connessione a QueueManager.> Connessione chiusa.
-------------------------------------------------------
In questa finestra, osservare i messaggi inviati tramite IBM MQ:
- Il messaggio di richiesta inviato
- Il messaggio di risposta ricevuto
-----
Quando si è pronti, premere un tasto qualsiasi per chiudere questa finestra
Premere qualsiasi tasto per continuare..
```

Nella **finestra Rispondi**, osservare i messaggi del risponditore aggiornati; il messaggio che ha ricevuto (dal client richiedente) e il messaggio di risposta che ha inviato:

```
> Factory di connessione ubicato in JNDI.> Destinazione ubicata in JNDI.> Creazione della
connessione a QueueManager.> Connessione creata.
> In attesa di messaggio.

> Ricevuto messaggio ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002b02 per ' B
akedBeans'
> Invio messaggio di risposta 'BakedBeans - 15 contenitori in magazzino'> Messaggio inviato
ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002902
> Chiusura connessione a QueueManager.> Connessione chiusa.
-------------------------------------------------------
In questa finestra, osservare i messaggi del responder aggiornati
- Il messaggio di richiesta ricevuto (dal richiedente)
- Il messaggio di risposta inviato
-----
```

```
Quando si è pronti, premere un tasto qualsiasi per chiudere questa finestra
Premere qualsiasi tasto per continuare..
```

I messaggi mostrati nelle due finestre dei comandi verificano che i client del richiedente e del responder dell'applicazione di esempio possano comunicare tra loro tramite IBM MQ.

Risultati

La migrazione alla versione più recente di IBM MQè stata eseguita correttamente.

Windows Opzione 2: migrazione side - by - side

L'opzione 2 di questo scenario mostra come eseguire la migrazione da una release precedente a una successiva di IBM MQ quando si utilizza il metodo di migrazione affiancato. Con una migrazione affiancata, si installa l'ultima versione di IBM MQ insieme alla versione precedente da cui si desidera eseguire la migrazione. I gestori code e le applicazioni continuano ad essere associate alla release precedente fino a quando non vengono migrate alla release successiva.

Prima di iniziare

Il punto di partenza per questo scenario è la configurazione IT iniziale descritta in “Panoramica: configurazione IT iniziale” a pagina 114.

Prima di iniziare questa attività, attenersi alle istruzioni in “Creazione di una configurazione IT iniziale” a pagina 118 per impostare una configurazione IT iniziale.

Informazioni su questa attività

Quando si segue il metodo di migrazione affiancato descritto in questo scenario, si installa la versione più recente insieme alla versione precedente in un'ubicazione alternativa. Poiché si disinstalla la versione precedente prima di avviare qualsiasi gestore code nella versione successiva, è possibile assegnare la propria installazione della versione successiva di IBM MQ come installazione primaria. Per ulteriori informazioni sull'installazione primaria, consultare Installazione primaria.

Procedura

1. Installare IBM MQ 9.4 utilizzando il launchpad e verificare l'installazione..
2. Arrestare i gestori code in esecuzione nella precedente versione di IBM MQ.
3. Disinstallare la versione precedente di IBM MQ.
4. Rendere IBM MQ 9.4 l'installazione primaria.
5. Opzionale: Associare i gestori code con IBM MQ 9.4
6. Utilizzare IBM MQ Explorer per verificare l'installazione di IBM MQ 9.4.

   Verificare che i gestori code siano stati migrati correttamente dalla release precedente e che sia possibile inserire e richiamare messaggi dalle code migrate.

Attività correlate

Migrazione su Windows: fianco a fianco

Windows *Installazione di IBM MQ 9.4 mediante il launchpad*

Utilizzare il launchpad di installazione e le procedure guidate per installare la versione più recente di IBM MQ insieme alla versione precedente su Windows.

Prima di iniziare

Prima di completare questa attività, completare i seguenti controlli:

- Quando si esegue l'installazione, è necessario disporre dell'autorità di amministratore locale. Definire questa autorizzazione mediante le funzioni Windows .

- Assicurarsi che il nome della macchina non contenga spazi.
- Assicurarsi di disporre di spazio su disco sufficiente, fino a 1005 MB, per installare completamente IBM MQ for Windows.
- Determinare se è necessario definire gli ID utente del dominio Windows per gli utenti IBM MQ .

Prima di installare IBM MQ, verificare che il sistema soddisfi i requisiti hardware e software. Per i dettagli più recenti sui requisiti hardware e software su tutte le piattaforme supportate, consultare Requisiti di sistema per 'IBM MQ.

Informazioni su questa attività

Questa attività descrive i passi di base per l'installazione di IBM MQ su Windows , se non è già installato sul sistema.

Questa attività presuppone che si utilizzino le ubicazioni predefinite del programma IBM MQ e dei file di dati.

Nota: Le ubicazioni predefinite del programma e della directory dei dati sono le stesse per IBM MQ 9.0 e versioni successive. Pertanto, non è necessario modificare la specifica del programma e le directory di dati durante la migrazione da IBM MQ 9.0 a una versione successiva. Tuttavia, quando si migra da versioni precedenti a IBM MQ 9.0, ci sono delle differenze nelle posizioni predefinite che è necessario considerare. Per ulteriori informazioni, consultare Program and data directory locations on Windows.

I programmi di installazione contengono collegamenti a ulteriori informazioni, se richieste durante il processo di installazione. Il processo di installazione è composto dalle seguenti parti:

1. Utilizzare il Launchpad per controllare e installare i requisiti software, specificare le informazioni di rete e avviare la procedura guidata di installazione IBM MQ .
2. Utilizzare la procedura guidata di installazione IBM MQ per installare il software e avviare Prepare IBM MQ Wizard.
3. Utilizza Prepare IBM MQ Wizard per avviare il servizio IBM MQ .

Procedura

1. Avviare il programma di installazione.

   In Esplora risorse di Windows , passare alla cartella temporanea in cui è stata scaricata l'immagine di installazione, quindi fare doppio clic su `setup.exe`.

   Il launchpad di installazione è avviato.
2. Utilizzando il launchpad, esaminare e, se necessario, modificare i requisiti software e la configurazione di rete.
   a) Fare clic sul pulsante **Requisiti software** per visualizzare la scheda **Requisiti software** .
   b) Verificare che i requisiti software siano stati soddisfatti e che la voce per il requisito visualizzi un segno di spunta verde con le parole 0K . Apportare le correzioni indicate.

      Nota: Per visualizzare ulteriori dettagli su qualsiasi requisito, fare clic sul pulsante più (+).
   c) Fare clic sul pulsante **Configurazione di rete** per visualizzare la scheda **Configurazione di rete** .
   d) Fare clic sul pulsante di opzione **No** .

      Nota: Questo scenario presuppone che non sia necessario configurare un ID utente di dominio per IBM MQ. Per ulteriori informazioni relative alla configurazione degli utenti del dominio IBM MQ for Windows , fare clic sul pulsante **Ulteriori informazioni** .
   e) Nella scheda **Installazione diIBM MQ** del Launchpad, selezionare la lingua di installazione e fare clic sul pulsante **Avvia IBM MQ Installer** per avviare la procedura guidata di installazione di IBM MQ .

   L'utente ha completato la revisione IBM MQ dei requisiti di installazione, ha apportato le modifiche richieste e ha avviato la procedura guidata di installazione di IBM MQ .

3. Utilizzare la procedura guidata di installazione IBM MQ per installare il software e avviare Prepare IBM MQ Wizard.

   La procedura guidata di installazione di IBM MQ controlla le installazioni esistenti e visualizza le opzioni di aggiornamento o installazione disponibili. Nel caso di questi scenari, ci sono due opzioni:

   - Installa senza modificare l'installazione esistente
   - Aggiornare l'installazione di 8.0.0.5 'Installazione 1'

   a) Selezionare **Installa lasciando inalterate le installazioni esistenti**e fare clic su **Avanti**.

   b) Leggere l'accordo di licenza e fare clic sulla casella di spunta **Accetto i termini nell'accordo di licenza** , quindi fare clic su **Avanti**.

   c) Fare clic su **Tipico**, quindi fare clic su **Avanti**.

   d) Nella pagina **Pronto per l'installazione IBM MQ** , esaminare le informazioni di installazione visualizzate e fare clic su **Installa**.

      Le informazioni sull'installazione includono i seguenti dettagli:

      - Nome installazione
      - Cartella di livello superiore per Program Files
      - Cartella di livello superiore per File di dati

      Sono installate le seguenti funzionalità:

      - IBM MQ Server
      - IBM MQ: un'interfaccia grafica per la gestione e il monitoraggio delle risorse di IBM MQ
      - Java™ e .NET Messaging e servizi Web
      - IBM MQ Toolkit di sviluppo

      Il processo di installazione inizia. In base al sistema, il processo di installazione può richiedere diversi minuti.

      Alla fine del processo di installazione, la finestra IBM MQ Setup visualizza il messaggio `Installation Wizard Completed Successfully` .

   e) Fare clic su **Fine**.

   IBM MQ è stato installato correttamente Prepare IBM MQ Wizard viene avviato automaticamente, visualizzando la pagina **Benvenuti in Prepare IBM MQ Wizard** .

4. Utilizza Prepare IBM MQ Wizard per avviare il servizio IBM MQ .

   a) Nella pagina Benvenuti in Prepare IBM MQ Wizard , selezionare **Avanti**.

      Prepare IBM MQ Wizard visualizza il messaggio `Status: Checking IBM MQ Configuration` e una barra di avanzamento. Una volta completato il processo, viene visualizzata la pagina Configurazione di rete IBM MQ .

   b) Nella pagina Configurazione di rete IBM MQ di Prepare IBM MQ Wizard, selezionare **No**.

   c) Fare clic su **Avanti**.

      Prepare IBM MQ Wizard visualizza un messaggio `Status: starting the IBM MQ Service` e una barra di avanzamento. Una volta completato il processo, la procedura guidata visualizza la pagina Completamento di Prepare IBM MQ Wizard .

   d) Selezionare **Avvia IBM MQ Explorer** e scegliere se avviare il Blocco note per visualizzare le note sulla release, quindi fare clic sul pulsante **Fine** .

      IBM MQ Explorer viene avviato.

Operazioni successive

È stata installata la versione più recente di IBM MQ insieme alla versione precedente, ma in una directory di installazione differente ed è stato avviato IBM MQ Explorer.

È ora possibile arrestare i gestori code in esecuzione nella versione precedente di IBM MQ , come descritto in “Arresto del gestore code” a pagina 138.

Windows *Arresto del gestore code*

Prima di migrare a una versione più recente di IBM MQ, è necessario arrestare il gestore code ed eseguire il backup dei dati del gestore code.

Informazioni su questa attività

Prima di eseguire il backup, arrestare il gestore code di cui si sta per eseguire il backup. Se si tenta di eseguire un backup di un gestore code in esecuzione, il backup potrebbe non essere congruente a causa di eventuali aggiornamenti in corso durante la copia dei file.

Procedura

1. Aprire IBM MQ Explorer.

   Fare clic su **Avvia** > **Tutte le applicazioni** > **IBM MQ** > **IBM MQ Explorer**.
2. Arrestare il gestore code sampleQM.
   a) Nella vista Navigator , fare clic con il tasto destro del mouse sul gestore code sampleQM.
   b) Fare clic su **Arresta**.

      Viene visualizzata la finestra **Termina gestore code** .
   c) Selezionare **Controllato**, quindi fare clic su **OK**.

      Selezionando l'opzione `Controllato` , il gestore code viene arrestato in modo controllato e ordinato. L'opzione **Immediata** , che forza l'arresto del gestore code, viene generalmente utilizzata solo se l'arresto controllato non viene completato correttamente.

   Il gestore code viene arrestato. In IBM MQ, l'icona accanto al gestore code sampleQM viene modificata in modo da includere una freccia rossa che punta verso il basso.
3. Chiudere IBM MQ Explorer.
4. Eseguire il backup dei dati del gestore code.

   Eseguire copie di tutti i seguenti dati, accertandosi di includere tutte le directory di backup. Alcune directory potrebbero essere vuote, ma sono necessarie tutte se è necessario ripristinare il backup in un secondo momento, quindi salvarle.

   - I dati del gestore code presenti in `C:\Programmi\ IBM \ MQ\Qmgrs`.
   - Le directory del file di log per i gestori code che si trovano in `C:\Programmi\ IBM \ MQ\log`, incluso il file di controllo log `amqhlctl.lfh`.
   - I file di configurazione presenti in `C:\Programmi\ IBM \ MQ\Config`.
   - IBM MQ 9.3 .ini e le voci di registro. Le informazioni sul gestore code sono memorizzate nel file .ini e possono essere utilizzate per ripristinare una versione precedente del prodotto.
5. Arrestare IBM MQ.
   a) Arresta il servizio IBM MQ.

      Fare clic con il tasto destro del mouse su **IBM MQ** nella barra delle applicazioni, quindi fare clic su **Arresta IBM MQ**.

      Viene visualizzata una finestra di dialogo con il seguente messaggio:

      ```
      La chiusura di IBM MQ terminerà tutti i gestori code in esecuzione e
      IBM MQ processi. Si è certi di voler proseguire? (AMQ4102)
      ```
   b) Fare clic su **Sì**, quindi attendere l'arresto di IBM MQ .
   c) Una volta arrestato IBM MQ , fare clic con il tasto destro del mouse sull'icona **IBM MQ** nella barra delle applicazioni, quindi fare clic su **Esci**.

Operazioni successive

Dopo aver arrestato i gestori code, è possibile associarli alla nuova installazione della versione più recente di IBM MQ come descritto in “Associazione dei gestori code a IBM MQ 9.4” a pagina 140.

Windows *Disinstallazione della versione precedente*

Disinstallare la versione precedente del prodotto utilizzando il pannello di controllo Windows .

Prima di iniziare

Prima di iniziare questa attività, è necessario arrestare i gestori code, chiudere IBM MQ Explorer e arrestare IBM MQ come descritto in “Arresto del gestore code” a pagina 138.

Informazioni su questa attività

In questa attività, disinstallare IBM MQ utilizzando il pannello di controllo Windows . I dati del gestore code non vengono rimossi come parte del processo di disinstallazione, il che significa che i gestori code di esempio utilizzati in questo scenario vengono conservati e possono essere rilevati quando si installa la versione più recente del prodotto.

Procedura

1. Aprire il Pannello di controllo Windows facendo clic su **Start> Pannello di controllo> Disinstalla un programma**.
2. Nella finestra **Programmi e funzioni** , individuare la voce per l'installazione che si desidera eliminare, ad esempio IBM WebSphere MQ (Installation1), e fare clic su **Disinstalla**.

   Il processo di disinstallazione inizia e viene eseguito fino al completamento. Una volta completato il processo, la versione precedente di IBM MQ viene rimossa dal computer e non viene più visualizzata nell'elenco dei programmi.

Risultati

La versione precedente del prodotto è stata rimossa dal computer. Tuttavia, i dati del gestore code non sono stati rimossi.

Operazioni successive

È ora possibile rendere la versione più recente diIBM MQ l'installazione primaria come descritto in “Rendere IBM MQ 9.4 l'installazione primaria” a pagina 139.

Attività correlate

Disinstallare IBM MQ su sistemi Windows

Windows *Rendere IBM MQ 9.4 l'installazione primaria*

Prima di avviare i gestori code nella nuova installazione della versione più recente di IBM MQ, è possibile, facoltativamente, rendere la versione più recente l'installazione primaria.

Informazioni su questa attività

Su sistemi che supportano più installazioni di IBM MQ, l'installazione primaria è quella a cui fanno riferimento le ubicazioni del sistema IBM MQ . Avere un'installazione primaria è facoltativo, ma conveniente.

Quando si segue il metodo di migrazione side - by - side descritto in questo scenario, poiché si disinstalla la versione precedente prima di avviare i gestori code nella versione successiva, è possibile assegnare l'installazione della versione successiva del prodotto come installazione primaria.

Per ulteriori informazioni sull'installazione primaria, consultare Installazione primaria.

Procedura

1. Verificare l'installazione primaria corrente immettendo il comando **dspmqinst** nel prompt dei comandi.

   Il prompt dei comandi visualizza i dettagli di tutte le installazioni correnti. L'installazione primaria corrente ha la seguente riga `Primary: Yes` .
2. Utilizzare il comando **setmqinst** per modificare l'installazione primaria corrente.

   Nel prompt dei comandi, immettere:

   ```
   setmqinst -x -n Installation_Name
   ```

   dove *Installation_Name>* è il nome dell'installazione primaria corrente.

   Se il comando ha esito positivo, il prompt dei comandi visualizza il messaggio `'Installation_Name' (Filepath) has been unset as the Primary Installation.`
3. Utilizzare il comando **setmqinst** per configurare la nuova installazione IBM MQ 9.4 come installazione primaria.

   Nel prompt dei comandi, immettere:

   ```
   setmqinst -i -n V9_Installation
   ```

   dove *V9_Installation* è il nome dell'installazione di IBM MQ 9.4 .

   Se il comando ha esito positivo, la richiesta comandi visualizza il messaggio `'V9_Installation' (Filepath) has been set as the primary installation. You must restart the operating system to complete the update.`

   Nota: Come indicato nel messaggio di esito positivo, è necessario riavviare il sistema operativo per completare l'aggiornamento.

Operazioni successive

Si è pronti ad associare i gestori code migrati alla versione più recente di IBM MQ come descritto in “Associazione dei gestori code a IBM MQ 9.4” a pagina 140.

Windows *Associazione dei gestori code a IBM MQ 9.4*

Utilizzare la procedura guidata Trasferisci gestori code per associare il gestore code sampleQM all'installazione della versione più recente di IBM MQ.

Prima di iniziare

Prima di iniziare questa attività, assicurarsi di aver arrestato il gestore code come descritto in “Arresto del gestore code” a pagina 138, altrimenti non sarà possibile completare il trasferimento.

Informazioni su questa attività

La funzione della procedura guidata Trasferisci gestori code di IBM MQ Explorer consente di trasferire uno o più gestori code da altre installazioni all'installazione corrente. La procedura guidata è equivalente al comando **setmqm**, ma evita di dover immettere i percorsi e i parametri richiesti. È possibile trasferire solo i gestori code arrestati; i gestori code in esecuzione vengono indicati per riferimento.

Una volta trasferito e avviato un gestore code su un'installazione per una versione successiva del prodotto, non è possibile migrare nuovamente a una versione precedente.

Procedura

1. Avviare IBM MQ Explorer.

   Fare clic su **Avvia** > **Tutte le applicazioni** > **IBM MQ** > **IBM MQ Explorer**.

2. Nella vista Navigator , fare clic con il tasto destro sul nodo dei gestori code e selezionare **Trasferisci gestori code**.
3. Fare clic con il pulsante destro del mouse, quindi selezionare il gestore code sampleQM, quindi fare clic su **Trasferisci**.

   Il comando **setmqm** viene richiamato con i gestori code selezionati. Se il trasferimento ha esito positivo, la struttura ad albero del navigator viene aggiornata in modo da includere i gestori code trasferiti. Se si verificano dei problemi, viene visualizzata una finestra con il messaggio di errore prodotto dal comando.
4. Avviare il gestore code sampleQM.
   a) Nella vista Navigator , espandere il nodo dei gestori code.
   b) Fare clic con il tastino destro del mouse sul gestore code, quindi selezionare **Avvia**.

Risultati

Il gestore code sampleQM è stato associato correttamente alla versione più recente di IBM MQ.

Operazioni successive

Verificare che il gestore code sampleQM sia stato migrato correttamente confermando che è possibile inserire un messaggio e richiamare un messaggio dalla coda come descritto in “Verifica dell'installazione di IBM MQ 9.4” a pagina 141.

Verifica dell'installazione di IBM MQ 9.4

Dopo aver installato la versione più recente di IBM MQ, utilizzare IBM MQ Explorer per verificare che i gestori code e le code siano stati migrati correttamente dalla release precedente, quindi verificare che sia possibile utilizzare l'applicazione di esempio.

Informazioni su questa attività

Una volta verificato che il gestore code migrato, sampleQM, è visibile nella vista Navigator di IBM MQ Explorer, verificare che sia possibile inserire un messaggio e richiamare un messaggio dalla coda migrata, quindi verificare che sia ancora possibile eseguire l'applicazione di esempio.

Procedura

1. Se IBM MQ Explorer non è in esecuzione, avviarlo ora.

   Fare clic su **Start> Tutti i programmi> IBM MQ > IBM MQ Explorer**.
2. Verificare che i gestori code siano stati migrati correttamente alla versione più recente di IBM MQ:
   a) Nella vista Navigator, espandere la cartella **Gestori code**.
   b) Verificare che sia possibile visualizzare sampleQM del gestore code nella cartella **Gestori code** .
   c) Espandere il gestore code sampleQM, fare clic sulla cartella **Code** e verificare che sia possibile visualizzare la coda Q1 nella vista Contenuto.
3. Se il gestore code sampleQM non è già avviato, avviarlo ora.
   a) Nella vista Navigator , espandere il nodo dei gestori code.
   b) Fare clic con il tasto destro del mouse sul gestore code sampleQM, quindi fare clic su **Avvia**.
4. Verificare che sia possibile inserire un messaggio nella coda Q1.
   a) Nella vista Navigator, espandere la cartella **Gestori code**.
   b) Espandere il gestore code sampleQM, fare clic sulla cartella **Code** .
   c) Nella vista Contenuto, fare clic con il tasto destro del mouse sulla coda Q1, quindi fare clic su **Inserisci messaggio di prova**.

      Viene aperta la finestra **Inserisci messaggio di prova**.

d) Nel campo **Dati messaggio** , immettere del testo, ad esempio `Hello queue!`, quindi fare clic su **Inserisci messaggio**.

Il campo **Dati del messaggio** verrà cancellato e il messaggio verrà inserito sulla coda.

e) Fare clic su **Chiudi**.

Nella vista Contenuto, notare che il valore **Profondità coda corrente** della coda è ora 1. Se la colonna Profondità della coda corrente non è visibile, potrebbe essere necessario scorrere verso destra la vista Contenuto.

5. Verificare che sia possibile richiamare il messaggio dalla coda Q1.

a) Nella vista Navigator , espandere la cartella **Gestori code** ,

b) Espandere il gestore code sampleQM e fare clic sulla cartella **Code** .

c) Nella vista Contenuto, fare clic con il tasto destro del mouse sulla coda Q1, quindi selezionare **Sfoglia messaggi**.

Il browser dei messaggi viene aperto per mostrare l'elenco dei messaggi attualmente in coda.

d) Fare doppio clic sull'ultimo messaggio per aprire la finestra delle proprietà.

Nella pagina **Dati** della finestra delle proprietà, nel campo **Dati del messaggio** è riportato il contenuto del messaggio in formato leggibile.

6. Verificare che sia possibile eseguire l'applicazione di esempio.

a) Fare doppio clic sul file `runresponder.cmd` .

Nella finestra del prompt dei comandi, etichettata **finestra Responder**, il client responder viene avviato e attende un messaggio.

```
> Factory di connessione ubicato in JNDI.> Destinazione ubicata in JNDI.> Creazione della
connessione a QueueManager.> Connessione creata.
> In attesa di messaggio.
```

b) Fare doppio clic sul file `runrequester.cmd` .

Nella **finestra del richiedente**, osservare i messaggi del richiedente. Nella **finestra Rispondi**, osservare i messaggi del risponditore aggiornati; il messaggio ricevuto (dal client richiedente) e il messaggio di risposta inviato.

Nella finestra del prompt dei comandi, etichettata **Finestra del richiedente**, il client del richiedente mostra lo stato della connessione, il messaggio che ha inviato, quindi il messaggio di risposta che ha ricevuto dal client del risponditore:

```
> Factory di connessione ubicato in JNDI.> Destinazione presente in JNDI.> Creazione della
connessione a QueueManager.> Connessione creata.
> Invio richiesta stock per 'BakedBeans'> Messaggio inviato
ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002b02
> Messaggio ricevuto ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002902 per ' B
akedBeans - 15 contenitori in magazzino '
> Chiusura della connessione a QueueManager.> Connessione chiusa.
-------------------------------------------------------
In questa finestra, osservare i messaggi inviati tramite IBM MQ:
- Il messaggio di richiesta inviato
- Il messaggio di risposta ricevuto
-----
Quando si è pronti, premere un tasto qualsiasi per chiudere questa finestra
Premere qualsiasi tasto per continuare..
```

Nella **finestra Rispondi**, osservare i messaggi del risponditore aggiornati; il messaggio che ha ricevuto (dal client richiedente) e il messaggio di risposta che ha inviato:

```
> Factory di connessione ubicato in JNDI.> Destinazione ubicata in JNDI.> Creazione della
connessione a QueueManager.> Connessione creata.
> In attesa di messaggio.

> Ricevuto messaggio ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002b02 per ' B
akedBeans'
> Invio messaggio di risposta 'BakedBeans - 15 contenitori in magazzino'> Messaggio inviato
ID=ID:414d5120514d5f4c33344c3238482020c3cd094d20002902
> Chiusura connessione a QueueManager.> Connessione chiusa.
-------------------------------------------------------
In questa finestra, osservare i messaggi del responder aggiornati
- Il messaggio di richiesta ricevuto (dal richiedente)
- Il messaggio di risposta inviato
-----
```

```
Quando si è pronti, premere un tasto qualsiasi per chiudere questa finestra
Premere qualsiasi tasto per continuare..
```

I messaggi mostrati nelle due finestre dei comandi verificano che i client del richiedente e del responder dell'applicazione di esempio possano comunicare tra loro tramite IBM MQ.

Risultati

La migrazione alla versione più recente di IBM MQè stata eseguita correttamente.

Operazioni successive

Per ulteriori informazioni sulla migrazione e l'aggiornamento, consultare Mantenimento e migrazione.

LTS Windows Installazione di una versione più recente di IBM MQ per coesistere con una versione precedente su Windows

Questo scenario mostra tutti i passi per l'installazione di una versione Long Term Support (LTS) di IBM MQ, mentre è coesistente ("side - by - side") con una versione precedente del prodotto. Inoltre, la procedura include l'installazione di un Fix Pack per la versione successiva. È necessario installare sempre l'ultimo livello di Fix Pack.

Panoramica di più installazioni

Una descrizione di più installazioni insieme all'hardware e al software utilizzati in questo scenario.

Informazioni su questa attività

Un aspetto importante di questa funzionalità di più installazioni di IBM MQ (più installazioni) nello stesso host è che questo tipo di installazione non richiede che i gestori code e le applicazioni della versione precedente del prodotto non debbano essere arrestati quando si eseguono attività con la versione successiva del prodotto.

Ciò significa che l'installazione della versione successiva del prodotto non influisce sull'esecuzione delle applicazioni sulla versione precedente del prodotto. Ciò è utile quando si tenta di eseguire una migrazione a più fasi dei gestori code sulla versione precedente del prodotto alla versione successiva.

Per questo scenario IBM MQ 8.0.0 viene utilizzato come versione precedente del prodotto e IBM MQ 9.1.0 viene utilizzato come versione successiva del prodotto.

Utilizzo di una versione Long Term Support di IBM MQ

Questo scenario utilizza una LTS versione di IBM MQ per la versione successiva del prodotto.

CD Se si utilizza una versione di Continuous Delivery (CD) di IBM MQ per la versione più recente del prodotto, è necessario disinstallare la versione di CD che si sta utilizzando, ad esempio, IBM MQ 9.1.1, prima di installare una versione successiva, ad esempio IBM MQ 9.1.5. Per ulteriori informazioni, vedi Migrazione da una release Continuous Delivery all'altra.

Hardware e software utilizzati per questo scenario

Sistema operativo

Windows 10
Nome host: `johndoe1.fyre.<yourdomainname>.com`

Gestori code

QM80
Creato con IBM MQ 8.0.0; per rimanere in IBM MQ 8.0.0

MMIG coda
Creato con IBM MQ 8.0.0; da migrare a IBM MQ 9.1.0

QM910
Creato con IBM MQ 9.1.0; per rimanere in IBM MQ 9.1.0

Installazione di una versione successiva di IBM MQ affiancata a una versione precedente.

Come installare IBM MQ 9.4 fianco a fianco alla versione esistente del prodotto sulla stessa macchina. L'installazione di IBM MQ 9.1 non verrà designata come installazione primaria.

Prima di iniziare

Verificare che IBM MQ 9.1 sia installato sul sistema. Utilizzare le seguenti istruzioni, Installazione del server IBM MQ su Windows, per installare il prodotto se IBM MQ 9.1 non è installato.

È necessario selezionare l'opzione *Personalizzato* in modo da poter selezionare esplicitamente il client. Per ulteriori informazioni, consultare Metodi di installazione per Windows .

Inoltre, è necessario richiamare il comando **setmqenv** con il parametro **-n** per impostare il nome dell'installazione su `Installation1`. È utile se si utilizza un file batch per richiamare il comando.

Informazioni su questa attività

Tutti i dati del gestore code vengono memorizzati in una struttura di directory comune. Anche se il codice eseguibile per ogni versione di IBM MQ è memorizzato in una diversa struttura di directory, i dati per tutti i gestori code, indipendentemente dalla versione, sono memorizzati in: `MQ_DATA_PATH=C:\ProgramData\IBM\MQ`.

Per installare IBM MQ 9.4:

Procedura

1. Accedere come amministratore.
   IBM MQ 9.4 verrà installato nella directory predefinita `C:\Program Files\IBM\MQ`.
2. Passare alla directory in cui si trova il file di download, ad esempio `C:\downloads\mq9300`.
3. Decomprimi il file scaricato.
   I file vengono estratti in una nuova sottodirectory denominata `MQServer`.
4. Passare alla nuova directory ed immettere il comando **setup.exe** per avviare il programma di installazione.
   a) Fare clic su *Requisiti software* per controllare che la propria azienda abbia installato il software richiesto.
      Per ulteriori informazioni, consultare Verifica dei requisiti su Windows . In questo scenario, il sistema ha i requisiti richiesti.
   b) Fare clic su *Configurazione di rete*.
      In questo scenario, la macchina non fa parte di un dominio, quindi non è necessario indicare un utente del dominio e la risposta alla domanda è `No`.
   c) Fare clic su *Installazione di IBM MQ*.
   d) Fare clic su *Avvia IBM MQ Installer*.
      Il programma di installazione rileva la presenza di altre installazioni sul sistema e visualizza il seguente messaggio:

      Aggiorna o installa
      Aggiornare l'installazione esistente o installare la nuova versione accanto ad essa

      Per questo scenario, lasciare intatte le altre installazioni, quindi selezionare la prima voce *Installa lasciando inalterate le installazioni esistenti*.
   e) Fare clic su **Avanti** e accettare la licenza.

f) Selezionare *Personalizzato* per l'opzione di installazione.

Per ulteriori informazioni, consultare Metodi di installazione per Windows .

g) Fare clic su **Avanti**.

Nel campo

Dettagli di installazione
Definire i dettagli dell'installazione

Viene visualizzato:

Nome installazione
Installation2

Cartella di installazione per i file di programma
`C:\ProgramFiles\IBM\MQ`

Viene visualizzato l'elenco delle funzionalità da installare. Notare che alcuni elementi:

- Non sono installati per impostazione predefinita
- È necessario selezionarli se si desidera installarli.

Per questo scenario, selezionare *Client MQI*e selezionare comunque questa opzione.

h) Fare clic su **Avanti**.

Nella schermata intitolata *Pronto per l'installazione IBM MQ* viene visualizzato il riepilogo del nome dell'installazione, l'ubicazione, i componenti da installare e così via.

i) Fare clic su **Installa** per continuare.

La copia dei file nella struttura della directory di installazione inizia. Una volta copiati i file, viene visualizzato il seguente dialogo: `The IBM MQ Installation Wizard has successfully installed IBM MQ`.

j) Fare clic su **Fine**.

Dopo l'installazione, viene visualizzata la seguente finestra di dialogo: `Welcome to the Prepare IBM MQ Wizard`.

Poiché questo scenario non utilizza un dominio Windows , accettare il valore predefinito **No**.

Accettare di avviare IBM MQ Explorere, a meno che non si disponga di un motivo specifico, è possibile accettare l'impostazione predefinita di *Avvia MQ Explorer con un nuovo spazio di lavoro*.

Risultati

È stata installata correttamente un'altra versione di IBM MQ for Windows insieme ad una versione esistente del prodotto.

Operazioni successive

È necessario eseguire il comando **setmqenv** per utilizzare i comandi su entrambe le versioni. Vedi “Utilizzo del comando setmqenv per l'esecuzione con entrambe le versioni di IBM MQ” a pagina 145 per i dettagli.

Utilizzo del comando `setmqenv` per l'esecuzione con entrambe le versioni di IBM MQ

Le attività di installazione sono complete ed è ora possibile verificare le directory contenenti il codice IBM MQ .

Prima di iniziare

Assicurarsi di aver installato correttamente il prodotto IBM MQ 8.0.0 , `Installation1`, in `C:\Program Files\IBM\WebSphere MQ\` e il prodotto IBM MQ 9.1 , `Installation2`, in `C:\Program Files\IBM\MQ`.

Informazioni su questa attività

Utilizzare il comando **dspmqinst** per visualizzare le informazioni di installazione delle versioni installate nel sistema senza dover esaminare le directory e il comando **dspmqver** per visualizzare le informazioni sulla versione.

Su sistemi Windows le informazioni vengono conservate nel Registro di sistema e le informazioni di configurazione dell'installazione vengono conservate nella chiave seguente: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebSphere MQ\Installation`.

Importante: Non è necessario modificare o fare riferimento direttamente a questa chiave.

Procedura

1. Visualizzare le informazioni di installazione utilizzando il comando **dspmqinst** .

```
InstName:      Installation1
InstDesc:
Identifier:    1
InstPath:      C:\Program Files\IBM\WebSphere MQ
Version:       8.0.0.9
Primary:       Yes
State:         Available
MSIProdCode:   {74F6B169-7CE6-4EFB-8A03-2AA7B2DBB57C}
MSIMedia:      8.0 Server
MSIInstanceId: 1

InstName:      Installation2
InstDesc:
Identifier:    2
InstPath:      C:\Program Files\IBM\MQ
Version:       9.1.0.0
Primary:       No
State:         Available
MSIProdCode:   {5D3ECA81-BF8D-4E80-B36C-CBB1D69BC110}
MSIMedia:      9.1 Server
MSIInstanceId: 1
```

   Nota: I relativi nomi di installazione (`InstName`) sono importanti.
2. Visualizzare la versione di IBM MQ utilizzando **dspmqver** per l'installazione predefinita (o primaria):

```
C:\> dspmqver
Name:        WebSphere MQ
Version:     8.0.0.9
Level:       p800-009-180321.1
BuildType:   IKAP - (Production)
Platform:    WebSphere MQ for Windows (x64 platform)
Mode:        64-bit
O/S:         Windows 10 Professional x64 Edition, Build 18363
InstName:    Installation1
InstDesc:
Primary:     Yes
InstPath:    C:\Program Files\IBM\WebSphere MQ
DataPath:    C:\ProgramData\IBM\MQ
MaxCmdLevel: 802
LicenseType: Production
```

   Dopo aver eseguito il comando si riceve il seguente messaggio: `Note there are a number (1) of other installations, use the '-i' parameter to display them`.
3. Immettere il comando `C:\> where dspmqver`e visualizzare le informazioni sull'installazione primaria:

```
C:\> where dspmqver
C:\Program Files\IBM\WebSphere MQ\bin64\dspmqver.exe
C:\Program Files\IBM\WebSphere MQ\bin\dspmqver.exe
```

4. Per visualizzare le informazioni relative al prodotto IBM MQ 9.1 , immettere il seguente comando, `C:\> setmqenv -n Installation2`.
5. Immettere nuovamente il comando `C:\> where dspmqver` e visualizzare le informazioni relative alla seconda installazione:

```
C:\> where dspmqver
C:\Program Files\IBM\MQ\bin64\dspmqver.exe
C:\Program Files\IBM\MQ\bin\dspmqver.exe
```

6. Immettere nuovamente il comando `C:\dspmqver` .

   Ora è possibile visualizzare:

```
C:\> dspmqver
Name:        IBM MQ
Version:     9.1.0.0
Level:       p910-L180705
BuildType:   IKAP - (Production)
Platform:    IBM MQ for Windows (x64 platform)
Mode:        64-bit
O/S:         Windows 10 Professional x64 Edition, Build 18363
InstName:    Installation2
InstDesc:
Primary:     No
InstPath:    C:\Program Files\IBM\MQ
DataPath:    C:\ProgramData\IBM\MQ
MaxCmdLevel: 910
LicenseType: Production
```

7. Immettere il comando `C:\ set MQ`e, dopo aver utilizzato **setmqenv** , visualizzare le informazioni relative alla seconda installazione.

```
C:\> set MQ
MQ_DATA_PATH=C:\ProgramData\IBM\MQ
MQ_ENV_MODE=64
MQ_FILE_PATH=C:\Program Files\IBM\MQ
MQ_INSTALLATION_NAME=Installation2
MQ_INSTALLATION_PATH=C:\Program Files\IBM\MQ
MQ_JAVA_DATA_PATH=C:\ProgramData\IBM\MQ
MQ_JAVA_INSTALL_PATH=C:\Program Files\IBM\MQ\java
MQ_JAVA_LIB_PATH=C:\Program Files\IBM\MQ\java\lib64
MQ_JRE_PATH=C:\Program Files\IBM\MQ\java\jre
```

   È possibile creare un file batch che eseguirà il comando **setmqenv** con la sintassi specificata. Accertarsi di disporre di questo file batch in una directory in PATH, ad esempio `C:\WinTools`.

   Ad esempio, è possibile creare il file batch `set-mq-910.bat` con il contenuto:

```
REM Setup the environment to run MQ 9.1
CALL "C:\Program Files\IBM\MQ\bin\setmqenv" -n Installation2
REM Adding Samples to the path
SET PATH=%PATH%;%MQ_FILE_PATH%\Tools\c\Samples\Bin;%MQ_FILE_PATH%\Tools\c\Samples\Bin64
;%MQ_FILE_PATH%\Tools\jms\samples;%MQ_JAVA_INSTALL_PATH%\bin\ dspmqver -f 2
```

   Note:

   a. È necessario utilizzare l'argomento "CALL" quando si richiama **setmqenv**. Senza questo argomento, l'elaborazione di **setmqenv** termina il batch e non consente l'esecuzione delle seguenti istruzioni. Ovvero, con l'argomento CALL, è possibile elaborare altre istruzioni nel file batch.

   b. Se si aggiunge una directory IBM MQ in PATH, ad esempio l'ubicazione per C-samples: PATH= ...;`C:\Program Files\IBM\MQ\tools\c\Samples\Bin`; ... questa directory verrà RIMOSSA da **setmqenv** alla successiva esecuzione del comando.

      Se si desidera essere in grado di eseguire C - samples, è necessaria l'ultima riga nel file batch precedente, per reinserire la directory degli esempi nel PATH.

      Notare anche che MQ_FILE_PATH viene utilizzato per utilizzare la struttura di directory appropriata per IBM MQ 9.1: `SET PATH=%PATH%;%MQ_FILE_PATH%\tools\c\Samples\Bin`.

Creazione di un gestore code

Come creare un gestore code, utilizzando il comando **crtmqm** . È possibile utilizzare IBM MQ Explorer per eseguire questa attività.

Prima di iniziare

Utilizzare il comando **dspmq** con i parametri **-o** *installation* e **-s** per mostrare il nome dell'installazione e lo stato dei gestori code correnti.

```
C:\> dspmq -o installation -s
QMNAME(QM80)                                  STATUS(Running) INSTNAME(Installation1)
  INSTPATH(C:\Program Files\IBM\WebSphere MQ) INSTVER(9.1.0.9)
QMNAME(QMMIG)                                 STATUS(Running) INSTNAME(Installation1)
  INSTPATH(C:\Program Files\IBM\WebSphere MQ) INSTVER(9.1.0.9)
```

Informazioni su questa attività

È necessario aprire un prompt dei comandi Windows e configurarsi come *Amministratore* per completare il seguente processo. Se si tenta di immettere il comando **crtmqm** senza utilizzare il prompt dei comandi, si riceve il messaggio AMQ7077: `Non si è autorizzati ad eseguire l'operazione richiesta`.

Procedura

1. Selezionare **Start** > **Windows System** > **Prompt dei comandi** > **Altro** > **Esegui come amministratore**
   Il titolo della finestra creata è *Amministratore: prompt dei comandi*.

   Nota: La versione di IBM MQ nel prompt dei comandi è IBM MQ 9.1.
2. Eseguire il comando **setmqenv** o il file batch che potrebbe essere stato creato, **set-mq-930**.
   Consultare “Utilizzo del comando setmqenv per l'esecuzione con entrambe le versioni di IBM MQ” a pagina 145 per i dettagli.
   In entrambi i casi, viene visualizzata la Versione 9.3.0.0
3. Immettere il seguente comando, `C:\> crtmqm -u SYSTEM.DEAD.LETTER.QUEUE QM930`
   Viene visualizzato il seguente output:

   ```
   IBM MQ queue manager created.
   Directory 'C:\ProgramData\IBM\MQ\qmgrs\QM930' created.
   The queue manager is associated with installation 'Installation2'.
   Creating or replacing default objects for queue manager 'QM930'.
   Default objects statistics : 87 created. 0 replaced. 0 failed.
   Completing setup.
   Setup completed.
   ```
4. Immettere il seguente comando per avviare il gestore code `C:\> strmqm QM930`
   Viene visualizzato il seguente output. Prendere nota delle righe che indicano l'installazione e la versione in cui è in esecuzione il gestore code:

   ```
   IBM MQ queue manager 'QM930' starting.
   The queue manager is associated with installation 'Installation2'.
   5 log records accessed on queue manager 'QM930' during the log replay phase.
   Log replay for queue manager 'QM930' complete.
   Transaction manager state recovered for queue manager 'QM910'.
   IBM MQ queue manager 'QM930' started using V9.3.0.0.
   ```
5. Immettere nuovamente il comando `C:\> dspmq -o installation -s` per visualizzare i gestori code installati:

   ```
   C:\> dspmq -o installation -s
   QMNAME(QM80)                                  STATUS(Running) INSTNAME(Installation1)
     INSTPATH(C:\Program Files\IBM\WebSphere MQ) INSTVER(9.1.0.9)
   QMNAME(QMMIG)                                 STATUS(Running) INSTNAME(Installation1)
     INSTPATH(C:\Program Files\IBM\WebSphere MQ) INSTVER(9.1.0.9)
   QMNAME(QM910)                                 STATUS(Running) INSTNAME(Installation2)
     INSTPATH(C:\Program Files\IBM\MQ) INSTVER(9.3.0.0)
   ++ Cannot use MQ 9.3.0 administrative commands to run an MQ 9.1 queue manager
   ```

   Importante: Non è possibile utilizzare i comandi di gestione su una versione di IBM MQ diversa da quella in uso.

Se si tenta di eseguire tale operazione, viene visualizzato il messaggio AMQ5691E: `Il gestore code < qmname> è associato a un'altra installazione (< installation name>).`

Migrazione di un gestore code a una versione successiva di IBM MQ

Dopo aver installato IBM MQ 9.4, ora si desidera migrare e aggiornare un gestore code IBM MQ 9.1 da utilizzare con IBM MQ 9.4.

Informazioni su questa attività

È necessario eseguire due passi principali:

1. Utilizzare il comando **setmqm** per associare il gestore code all'installazione desiderata, ossia la versione IBM MQ .
2. Utilizzare il comando **strmqm** nella versione desiderata, che aggiorna i dati del gestore code per la nuova versione.

Per questo scenario, il gestore code `QMMIG`, creato con IBM MQ 9.1, verrà utilizzato come illustrazione della procedura di migrazione.

Attenzione: Una volta che un gestore code è stato migrato ad una versione successiva di IBM MQ, non è più possibile utilizzarlo con la precedente versione di IBM MQ. Il processo di migrazione modifica una serie di definizioni di file e oggetti e non è possibile tornare indietro.

Procedura

1. Eseguire una copia di backup del gestore code utilizzando il comando **dmpmqcfg** .

   Per ulteriori informazioni, consultare Backup e ripristino dei dati del gestore code IBM MQ e Backup della configurazione del gestore code.

   a) Per specificare tutti gli attributi, inclusi quelli predefiniti, (eccetto **setmqaut**, che non è incluso nell'emissione, specificare il seguente comando:

   ```
   dmpmqcfg -m QMgr -a > QMgr.dmpmqcfg.out.all.mqsc
   ```

   b) Per catturare gli attributi nel formato **setmqaut** , immettere il seguente comando:

   ```
   dmpmqcfg -m QMgr -o setmqaut > QMgr.dmpmqcfg.setmqaut.bat
   ```

   Nota: Il file di output contenente i comandi **setmqaut** include il nome del gestore code in ciascun comando. Pertanto, se si desidera ripristinare i comandi in un gestore code differente, è necessario modificare il file e specificare il nome del gestore code desiderato.
2. Per ripristinare:

   a) Comandi per **runmqsc**, immettere:

   ```
   runmqsc Qmgr < QMgr.dmpmqcfg.out.mqsc
   ```

   o

   ```
   runmqsc Qmgr < QMgr.dmpmqcfg.out.all.mqsc
   ```

   b) I comandi **setmqaut** emettono:

   ```
   QMgr.dmpmqcfg.setmqaut.bat
   ```
3. Il gestore code da migrare si trova in IBM MQ 9.1, pertanto è necessario eseguire lo script che imposta l'ambiente di esecuzione su IBM MQ 9.4:

   ```
   C:\> set-mq-80
   ```

   a) Immettere il comando `C:\> dspmqver` per verificare la versione in cui il gestore code è in esecuzione su IBM MQ 9.1.

b) Immettere il comando `C:\> where dspmq` per controllare che il gestore code sia in esecuzione:

```
C:\Program Files\IBM\WebSphere MQ\bin64\dspmq.exe
C:\Program Files\IBM\WebSphere MQ\bin\dspmq.exe
```

c) Emettere il comando `C:\> dspmq -m QMMIG -o installation -s`

```
QMNAME(QMMIG)               STATUS(Running) INSTNAME(Installation1)
INSTPATH(C:\Program Files\IBM\WebSphere MQ) INSTVER(9.1.0.9)
```

d) Emettere il comando `C:\> runmqsc QMMIG`

```
display qmgr cmdlevel version
       1 : display qmgr cmdlevel
AMQ8408: Display Queue Manager details.
  QMNAME(QMMIG)                     CMDLEVEL(910)
  VERSION(09001009)
end
```

e notare che CMDLEVEL è all'indirizzo IBM MQ 9.1.

e) Arrestare il gestore code immettendo il comando `C:\ endmqm -i QMMIG`

Si ricevono i messaggi:

```
WebSphere MQ queue manager 'QMMIG' ending.
WebSphere MQ queue manager 'QMMIG' ended.
```

4. Modificare l'ambiente per eseguire i comandi IBM MQ 9.4 , emettendo il comando `C:\> set-mq-930` se è stato creato il file batch o utilizzando il comando **setmqenv** , quindi controllare la versione immettendo il comando **dspmqver** .
5. Visualizzare lo stato dei gestori code immettendo il comando `C:\> dspmq -o installation -s`.

Si riceve il seguente output:

```
QMNAME(QM91)                   STATUS(Running)INSTNAME(Installation1)
INSTPATH(C:\Program Files\IBM\WebSphere MQ) INSTVER(9.1.0.9)

QMNAME(QMMIG)                             STATUS(Ended immediately) INSTNAME(Installation1)
INSTPATH(C:\Program Files\IBM\WebSphere MQ) INSTVER(9.1.0.9)

QMNAME(QM910)                             STATUS(Running) INSTNAME(Installation2)
INSTPATH(C:\Program Files\IBM\MQ) INSTVER(9.3.0.0)
```

Attenzione: Il gestore code QMMIG è ancora associato a `Installation1` (IBM MQ 9.1) mentre `Installation2` è associato a IBM MQ 9.4.

Pertanto, è necessario dissociare il gestore code QMMIG da `Installation1` e associarlo a `Installation2`

6. Immettere il seguente comando per associare il gestore code QMMIG a `Installation2`

```
C:\> setmqm -m QMMIG -n Installation2
```

Viene ricevuto il seguente messaggio:

```
The setmqm command completed successfully.
```

che informa che QMMIG è ora associato a IBM MQ 9.4.

7. Avviare il gestore code QMMIG immettendo il comando `C:\> strmqm QMMIG`

Poiché questa è la prima volta che il comando IBM MQ 9.4 **strmqm** viene emesso su un gestore code che era stato precedentemente utilizzato con una versione precedente, viene eseguita una migrazione.

Viene visualizzato un output simile al seguente:

```
IBM MQ queue manager 'QMMIG' starting.
The queue manager is associated with installation 'Installation2'.
5 log records accessed on queue manager 'QMMIG' during the log replay phase.
Log replay for queue manager 'QMMIG' complete.
```

```
Transaction manager state recovered for queue manager 'QMMIG'.
Migrating objects for queue manager 'QMMIG'.
Default objects statistics : 5 created. 0 replaced. 0 failed.
IBM MQ queue manager 'QMMIG' started using V9.3.0.0.
```

8. Immettere il seguente comando, `C:\> runmqsc QMMIG` per visualizzare gli attributi del gestore code e prendere nota dei campi VERSION e CMDLEVEL:

```
display qmgr cmdlevel version
    1 : display qmgr cmdlevel version
AMQ8408I: Display Queue Manager details.
   QMNAME(QMMIG)                           CMDLEVEL(930)
   VERSION(09300000)
end
```

Risultati

È stata eseguita correttamente la migrazione di un gestore code a una versione successiva del prodotto.

Installazione di un fix pack su IBM MQ 9.4

Modalità di installazione di un fix pack su IBM MQ 9.4 installato su un sistema con installazioni a più versioni di IBM MQ.

Prima di iniziare

Assicurarsi di aver migrato il gestore code QMMIG a IBM MQ 9.4. Per ulteriori informazioni, consultare “Migrazione di un gestore code a una versione successiva di IBM MQ” a pagina 149.

Informazioni su questa attività

Per questo scenario, è presente un'altra versione installata (IBM MQ 9.1) e i gestori code in esecuzione con tale altra versione non verranno arrestati per dimostrare che è possibile continuare a utilizzare tali altre versioni, mentre si eseguono attività di manutenzione per IBM MQ 9.4.0.n.

Non viene selezionata alcuna opzione avanzata durante l'installazione dell'aggiornamento.

Procedura

1. Accedere come amministratore.
   a) Immettere il comando `C:\> set-mq-930` se è stato creato il file batch o utilizzare il comando **setmqenv** per accertarsi di essere su IBM MQ 9.4.0.n, dove n è `0` in questo scenario.
   b) Visualizzare lo stato dei gestori code immettendo il comando `C:\> dspmq -o installation -s`.
   Si riceve il seguente output:

```
QMNAME(QM80)                   STATUS(Running)INSTNAME(Installation1)
INSTPATH(C:\Program Files\IBM\MQ) INSTVER(9.1.0.0)

QMNAME(QMMIG)                            STATUS(Ended unexpectedly)
INSTNAME(Installation2)
INSTPATH(C:\Program Files\IBM\MQ) INSTVER(9.3.0.0)

QMNAME(QM910)                            STATUS(Ended immediately) INSTNAME(Installation2)
INSTPATH(C:\Program Files\IBM\MQ) INSTVER(9.3.0.0)
```

2. Arrestare i processi IBM MQ 9.4.0.
   Per ulteriori informazioni sull'arresto dei processi, consultare Applicazione e rimozione della manutenzione su Windows .
   Riepilogo:
   - Immettere il comando **endmqm immediate** per i gestori code QMMIG e QM930.

- Arrestare il servizio IBM MQ per l'installazione facendo clic con il tasto destro del mouse sull'icona IBM MQ nella barra delle attività, quindi fare clic su **Arresta IBM MQ**.

3. Individuare il fix pack. Questo scenario utilizza IBM MQ 9.4.0.5.

   Andare a Correzioni consigliate per IBM MQ per un elenco delle più recenti:

   - Continuous Delivery e l'elenco di correzioni per le release Continuous Delivery
   - Aggiornamento di sicurezza cumulativo per la release Long Term Support e l'elenco di correzioni per le release Long Term Support

   Nota: È necessario verificare che si stia utilizzando l'ultimo fix pack visitando e scaricando quello appropriato.

   a) Fare clic sulla scheda appropriata.

      Per questo scenario è *V9.3.0.5 LTS*

   b) Scaricare il software Windows da Fix Central o Passport Advantage. se è necessario scaricare l'intero prodotto,

      In questo scenario, inserire la serie di file nella seguente directory `C:\downloads\mq9305`; il nome file è `9.3.0-IBM-MQ-Win64-FP0005.zip`.

4. Estrarre i file dal file `.zip` ed eseguire il seguente comando, **`IBM-MQ-9.3.0-FP0005.exe`**.

   Viene visualizzata la finestra di dialogo *Installa ovunque* , contenente le seguenti informazioni `InstallAnywhere is preparing to install ...`

   È necessario aspettare fino al termine della preparazione, che può richiedere diversi minuti.

5. Fare clic su **OK** per continuare quando viene visualizzata la finestra *IBM MQ (file del fix pack 9.3.0.5)* .

   a) Quando viene visualizzata una sezione *Introduzione* , fare clic su **Avanti**.

   b) Quando viene visualizzata la sezione *Tipo di installazione* , selezionare l'opzione più adatta per l'azienda, probabilmente **Carica file e applica fix pack**e fare clic su **Avanti**.

   c) Quando viene visualizzata la sezione *Informazioni* , fare clic su **Avanti**.

   d) Quando viene visualizzata la sezione *Cartella di destinazione* , selezionare l'ubicazione predefinita `C:\Program Files\IBM\source\MQ 9.3.0.5`e fare clic su **Avanti**.

   e) Quando viene visualizzata la sezione *Opzioni avanzate* , fare clic su **Avanti**.

   f) Quando viene visualizzata la sezione *Riepilogo pre - installazione* , controllare le informazioni visualizzate e fare clic su **Installa**.

   g) Attendere il caricamento del codice.

      La sezione *Caricamento* presenta un indicatore di avanzamento e quando il processo è completo, viene selezionato *Caricamento completo* e viene visualizzata la sezione *Applica fix pack* .

   h) Fare clic su **Eseguito**.

      Poiché sul sistema è presente più di un'installazione, viene visualizzata una finestra di dialogo in cui è possibile selezionare l'installazione che si desidera aggiornare. In questo caso è `Installation2 (9.3.0.0)`.

   i) Fare clic su **OK**.

   j) Accettare il valore predefinito per *Cartella di backup* e fare clic su **Applica**.

      Vengono visualizzate più finestre di dialogo con indicatori di avanzamento ed è stato applicato il *Fix Pack 9.3.0.5 . Fare clic su Fine per terminare.*

   k) Fare clic su **Fine**.

Risultati

È stata correttamente aggiornata una versione di IBM MQ for Windows insieme ad una versione esistente del prodotto.

Managed File Transfer scenario

Un'introduzione alle topologie comuni di Managed File Transfer e uno scenario che illustra l'utilizzo della capacità Managed File Transfer mostrando come impostare il sistema e trasferire un messaggio di verifica.

- Topologie comuni
- Configurazione del server di base

Topologie comuni MFT

Questa sezione descrive le topologie Managed File Transfer comuni. Le frecce a doppia faccia in ogni diagramma rappresentano connessioni al gestore code.

Per ulteriori informazioni sulle opzioni di connessione del gestore code, consultare “Considerazioni sulla connettività” a pagina 156 .

Topologia di base con un gestore code

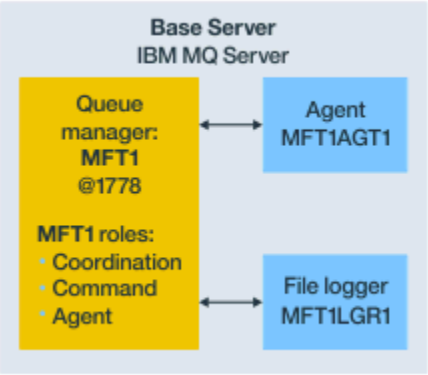


Figura 25. Topologia di base con un gestore code

Una topologia di base rappresenta una configurazione completa che include il gestore code di coordinamento. Il nome della configurazione è uguale al nome del gestore code di coordinazione. Se il nome del gestore code di coordinamento è MFT1, il nome della configurazione è MFT1.

La topologia di base è la prima configurazione Managed File Transfer completata. Una volta completata la configurazione di base, gli agent partner dei server remoti vengono aggiunti alla configurazione di base per scambiare i file.

La topologia di base non scambia file all'esterno del server della topologia di base. Tuttavia, la topologia di base consente di spostare i file in ubicazioni differenti nello stesso server e potrebbe essere utilizzata per scopi di sviluppo.

Topologia di base con un agent partner

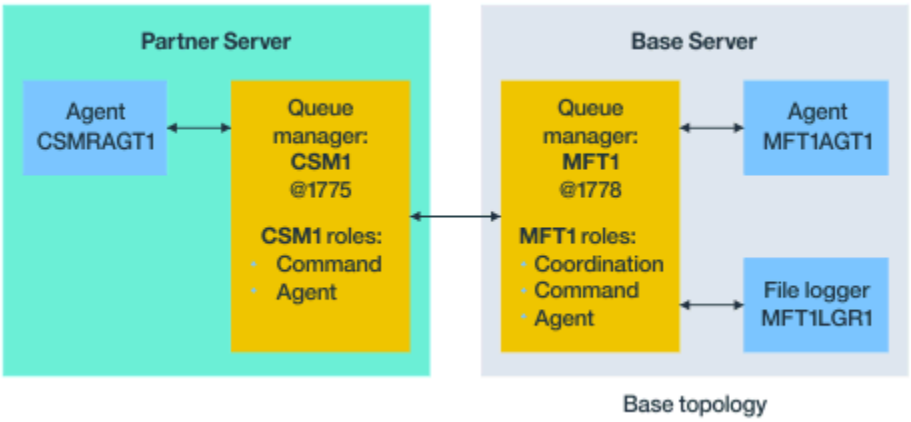


Figura 26. Topologia di base con un agent partner

Questa topologia può scambiare file tra i due agent. Gli agent partner aggiuntivi possono essere aggiunti in modo simile al primo agent aggiunto.

È possibile utilizzare un singolo gestore code per tutti e tre i ruoli del gestore code Managed File Transfer oppure è possibile utilizzare i gestori code dedicati per ruoli specifici.

Ad esempio, è possibile disporre di un gestore code dedicato al ruolo di gestore code di coordinamento e i ruoli comando e agent potrebbero condividere un secondo gestore code.

La connessione tra un gestore code dell'agent remoto in un server separato dalla configurazione di base e il gestore code di coordinamento della configurazione di base deve essere configurato come un client IBM MQ o un canale MQI.

La connessione al gestore code di coordinamento viene stabilita dal comando **fteSetupCoordination** . Se la connessione del gestore code di coordinamento non è configurata come un canale client IBM MQ , sul server partner, i comandi come **fteListAgents** non riescono quando vengono emessi dal server agent partner.

Topologia di base con gestore code di coordinazione separato e un agent partner

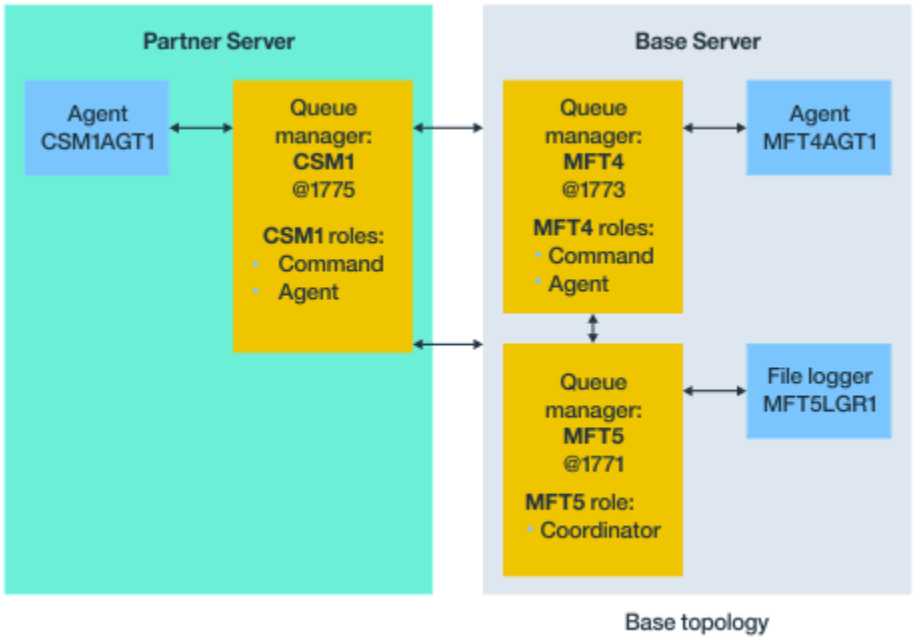


Figura 27. Topologia di base con gestore code di coordinazione separato e un agent partner

Nella topologia di base della figura 3, nel server di base, il gestore code MFT4 è condiviso per i ruoli comando e agent e il gestore code MFT5 è dedicato al ruolo gestore code di coordinazione.

La connettività deve esistere tra tutti i gestori code nella topologia, inclusi i gestori code nella topologia di base, MFT4 e MFT5.

Sul gestore code del server partner, il gestore code CSM1 ha il ruolo di gestore code di comandi e agent.

Questa topologia può scambiare file tra i due agent. Ogni agente partner deve connettersi a un gestore code, come mostrato nel diagramma. Gli agent partner aggiuntivi possono essere aggiunti in modo simile al modo in cui è stato aggiunto il primo agent partner.

Topologia di base con partner Managed File Transfer Agent

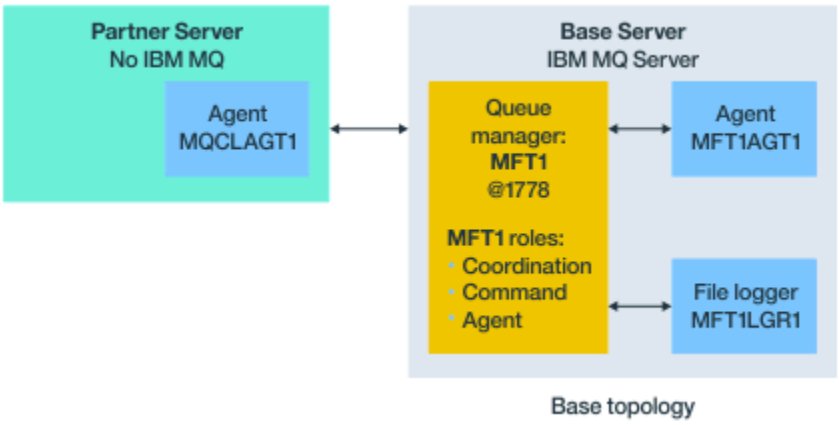


Figura 28. Topologia di base con partner Managed File Transfer Agent

Questa topologia può scambiare file tra i due agent.

Il server nell'agent partner, rappresentato come MQCLAGT1 nel diagramma, non presenta il server IBM MQ installato.

L'agent partner viene configurato utilizzando gli stessi comandi del server installato IBM MQ , con alcune eccezioni:

- La configurazione per questo agent partner deve utilizzare le connessioni client IBM MQ al gestore code di base o ai gestori code.
- Non è necessario eseguire le definizioni del ruolo del gestore code di coordinamento IBM MQ create dai comandi di configurazione nel server dell'agent partner. Le definizioni del gestore code di coordinamento esistono già nel server di base.

  Tuttavia, è necessario:

  – Copia le definizioni di oggetto dell'agent generate quando l'agent viene creato nel server partner
  – Trasferire il file di definizione sul server di configurazione di base e
  – Creare le definizioni nel gestore code identificato come gestore code agent nel server di base.

    In questo caso MFT1 sta servendo tutti e tre i ruoli e si creano gli oggetti per l'agent `MQCLAGT1` nel gestore code MFT1 .

  Come alternativa alla copia delle definizioni degli oggetti sul server di base, è possibile eseguire il comando **fteDefine** per l'agent MQCLAGT1 sul server di base in cui si trova il gestore code dell'agent. Utilizzare le definizioni generate dal comando **fteDefine** per creare le definizioni di agent richieste sul gestore code dell'agent.

  Ad esempio, nel diagramma visualizzato, copiare il file `MQCLAGT1_create.mqsc` dalla directory dell'agent nel server partner al server di configurazione di base e creare le definizioni dell'agent richieste nel gestore code MFT1 .

  La configurazione completata sul server dell'agent partner crea la directory di configurazione Managed File Transfer e i file delle proprietà richiesti.

Sul server partner è possibile installare Managed File Transfer Redistributable Client da Fix Central.

Nota: Il client ridistribuibile MQMFT differisce dal client ridistribuibile IBM MQ , in quanto è già compresso e non richiede l'uso del programma di utilità **genmqpkg** . Per ulteriori informazioni, consultare Client ridistribuibili.

Considerazioni sulla connettività

Nei diagrammi precedenti, ogni riga tra agent e gestori code rappresenta una connessione a un gestore code.

Questa connessione potrebbe essere:

- Una connessione locale
- Un collegamento o una connessione del canale di messaggi, oppure
- Una connessione MQI o client IBM MQ .

Il tipo di connessione selezionato nella configurazione dipende dai parametri specificati

- Quando si specifica il parametro del nome del gestore code senza altri parametri di connessione, si specifica una connessione di bind.

  Se il gestore code utilizzato è locale rispetto alla configurazione di Managed File Transfer , rappresenta anche una connessione locale, quando utilizzata nel server di configurazione di base.
- Se si specifica il parametro del nome del gestore code, insieme ai parametri dell'host, della porta e del nome canale corrispondenti, si specifica una connessione client IBM MQ .

Quando gli agent si trovano sullo stesso host del gestore code dell'agent, una specifica del tipo di bind, che risulta in una connessione locale, è più efficiente.

Configurazione del server di base

Come impostare il server di base con un gestore code di configurazione separato.

Prima di iniziare

Il seguente esempio presuppone che si disponga di:

- Consultare la sezione “Considerazioni sulla connettività” a pagina 156 e comprendere come influenzare il tipo di connessione ai gestori code nella configurazione.
- Un'infrastruttura IBM MQ funzionante. Per informazioni sull'impostazione dei gestori code, consultare Configurazione dei gestori code IBM MQ .
- Le attività di sicurezza IBM MQ sono state completate.

  Tutte le risorse di sistema, come l'accesso ai file, sono configurate con una sicurezza adeguata.

  Per la configurazione della sicurezza Managed File Transfer , fare riferimento a Protezione Managed File Transfer e Limitazione delle autorizzazioni utente sulle azioni dell'agente MFT.
- Tutte le connessioni IBM MQ vengono verificate dopo che IBM MQ è stato configurato utilizzando un programma di esempio per inviare e ricevere messaggi oppure utilizzando l'esempio **amqscnxc** per verificare le connessioni di tipo client IBM MQ .

  L'esempio **amqscnxc** si connette a un gestore code definendo la connessione del canale nel codice di esempio, simile al modo in cui Managed File Transfer si connette, quando utilizza una connessione di tipo client MQI o IBM MQ .
- Le istruzioni presuppongono che il server utilizzato per la configurazione di base abbia una versione di IBM MQ installata. Se si dispone di più installazioni IBM MQ nel server di base, è necessario prestare attenzione a utilizzare il percorso file corretto per la versione di IBM MQ che si desidera utilizzare.
- I gestori code utilizzati in queste istruzioni non richiedono l'autenticazione della connessione.

  Anche se potrebbe essere più semplice completare la prima configurazione senza l'autenticazione della connessione richiesta, se la propria azienda richiede l'utilizzo immediato dell'autenticazione della connessione, consultare MFT e IBM MQ autenticazione della connessione per istruzioni su come configurare un file di credenziali `MQMFTCredentials.xml`

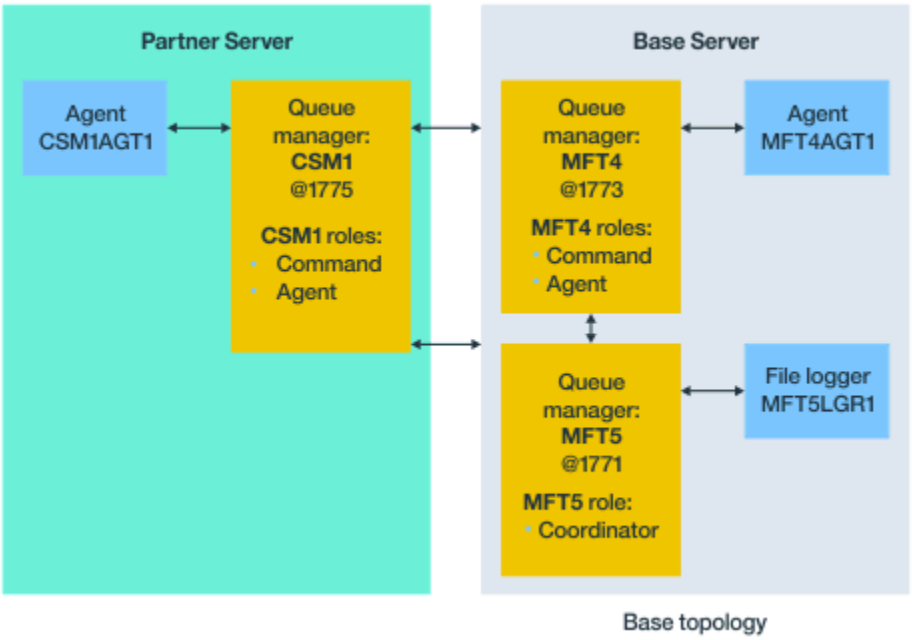


Figura 29. Topologia di base con gestore code di coordinazione separato e un agent partner

Informazioni su questa attività

I ruoli del gestore code per la configurazione di esempio sono:

- Server di base

  - Il gestore code MFT5 è il gestore code di coordinamento
  - Il gestore code MFT4 viene utilizzato come gestore code agent per l'agent MFT4AGT1e funge anche da gestore code comandi per la configurazione MFT5 sul server di base.
- Server partner
  - Il gestore code CSM1 funge da gestore code dell'agent per l'agent CSM1AGT1e da gestore code comandi per la configurazione MFT5 sul server partner.
  - Il Gestore code MFT5, sul server di base, è il gestore code di coordinamento.

Procedura

1. Configurazione del gestore code di coordinamento
2. Configurazione del gestore code comandi
3. Configurazione dell'agente
4. Impostazione del logger
5. Configurazione di un server partner

Operazioni successive

Configurare MQExplorer con MQMFT in modo da poter verificare la propria configurazione di esempio.

Configurazione del gestore code di coordinamento

Come configurare il gestore code di coordinamento per coordinare i trasferimenti file.

Prima di iniziare

Accertarsi di disporre di una connettività completa tra i gestori code configurati per questo scenario.

Informazioni su questa attività

Questa attività configura il gestore code di coordinamento MFT5e le istruzioni in questa sezione presuppongono che si stia utilizzando un'installazione di IBM MQ .

Se si dispone di più installazioni, è necessario impostare il percorso IBM MQ per la versione di IBM MQ richiesta, utilizzando il comando setmqenv , prima di avviare qualsiasi attività di configurazione.

Procedura

1. Accedere come amministratore Managed File Transfer .
2. Immettere il seguente comando per identificare il gestore code di coordinamento e impostare la struttura della directory di configurazione:

   ```
   fteSetupCoordination -coordinationQMgr MFT5
   ```

   Directory gestore code di coordinamento
   C:*data*\mqft\config\MFT5

   coordination.properties file
   C:*data*\mqft\config\MFT5\coordination.properties

   Il comando produce anche un file di comandi MQSC che è necessario eseguire sul gestore code di coordinamento C:*data*\mqft\config\MFT5\MFT5.mqsc:
3. Passare alla directory C:*data*\mqft\config\MFT5 .
4. Configurare il gestore code in modo che agisca come gestore code di coordinamento, eseguendo il comando riportato di seguito.

È necessario fornire il file di comandi MQSC, prodotto dal comando immesso nel Passo “2” a pagina 158:

```
runmqsc MFT5 < MFT5.mqsc > mft5.txt
```

5. Aprire il file dei risultati `mft5.txt` con l'editor preferito. e verificare che le definizioni siano state create correttamente.

Operazioni successive

Impostare il gestore code comandi.

Configurazione del gestore code comandi

Modalità di configurazione del gestore code comandi.

Prima di iniziare

Assicurarsi di aver configurato il gestore code di coordinamento. Per ulteriori informazioni, consultare “Configurazione del gestore code di coordinamento” a pagina 158.

Informazioni su questa attività

Questa attività identifica il gestore code comandi.

Procedura

Emetti il seguente comando:

```
fteSetupCommands -connectionQMgr MFT4
```

Si ottiene il seguente messaggio BFGCL0245I: il file `C:\data\mqft\config\MFT4\command.properties` è stato creato correttamente.

Il gestore code comandi non richiede definizioni IBM MQ extra. Dopo aver eseguito **fteSetupCommands**, il file `command.properties` viene creato nella directory di configurazione MFT5 .

Operazioni successive

Configurare l' agent.

Impostazione dell'agente

Come preparare un agent di trasferimento file MFT4AGT1, inclusi gli script MQSC che è necessario eseguire.

Prima di iniziare

È necessario impostare il gestore code comandi. Per ulteriori informazioni, consultare “Configurazione del gestore code comandi” a pagina 159.

Informazioni su questa attività

Questa attività prepara l'agent di trasferimento file Windows , MFT4AGT1.

Procedura

1. Emetti il seguente comando:

```
fteCreateAgent -agentName MFT4AGT1 -agentQMgr MFT4
```

Dopo aver creato l'agent con il comando **fteCreateAgent** , la directory agents e una sottodirectory per l'agent, MFT4AGT1, vengono aggiunte alla directory MFT5 .

Nella directory *data*\MFT5\agents\MFT4AGT1 è possibile trovare:

- agent.properties file
- File MFT4AGT1_create.mqsc , che contiene le definizioniIBM MQ richieste dall'agent.

2. Passare alla directory *data*\MFT5\agents\MFT4AGT1 e creare le definizioni del gestore code dell'agent richieste immettendo il seguente comando:

```
runmqsc MFT4 < MFT4AGT1_create.mqsc > mft4.txt
```

3. Aprire il file dei risultati mft4.txt con l'editor preferito e verificare che le definizioni siano state create correttamente.
4. Avviare l'agent immettendo il seguente comando: **fteStartAgent** MFT4AGT1.
5. Visualizzare l'agent immettendo il seguente comando: **fteListAgents**.

   L'output dovrebbe essere simile al seguente:

```
5655-MFT, 5724-H72 Copyright IBM Corp. 2008, 2025.  ALL RIGHTS RESERVED
BFGPR0127W: No credentials file has been specified to connect to IBM MQ.
Therefore, the assumption is that IBM MQ authentication has been disabled.
Agent Name:     Queue Manager Name:     Status:
MFT4AGT1        MFT4                    READY
```

   Nota: se non è stata abilitata l'autenticazione della connessione nell'ambiente Managed File Transfer , è possibile ignorare il messaggio BFGPR0127W .

   Se si immette il comando **ftelistAgents** e si riceve il seguente messaggio, BFGCL0014W: Non esiste alcun agent che corrisponde ai criteri di selezione correnti., vedere Cosa fare se l'agent MFT non viene elencato dal comando **fteListAgents**.

Operazioni successive

Imposta il logger.

Impostazione del programma di registrazione

È necessario un file o un programma di registrazione database per conservare la cronologia e le informazioni di verifica relative all'attività di trasferimento per la configurazione. In questo esempio si crea un programma di registrazione file.

Prima di iniziare

È necessario aver impostato:

- Gestore code di configurazione
- Gestore code comandi
- Agente

Procedura

1. Emetti il seguente comando:

```
fteCreateLogger -loggerQMgr MFT5 -loggerType FILE
-fileLoggerMode CIRCULAR -fileSize 5MB -fileCount 3 MFT5lgr1
```

   Una volta eseguito il comando **fteCreateLogger** , la directory *data*\mqft\config\MFT5\loggers viene creata con una sottodirectory MFT5LGR1 .

La sottodirectory MFT5LGR1 contiene il file `logger.properties` . Nella directory è presente anche un file denominato `MFT5LGR1_create.mqsc` con le definizioni IBM MQ richieste dal programma di registrazione.

2. Passare alla directory *data*`\mqft\config\MFT5\loggers\MFT5LGR1`.
3. Eseguire il file di comandi MQSC associato.

   ```
   runmqsc MFT5 < MFT5_create.mqsc
   ```

   per creare le definizioni richieste dal programma di registrazione.

   a) Esaminare i risultati delle definizioni dell'oggetto per verificare che gli oggetti richiesti siano stati creati correttamente.
4. Avviare il programma di registrazione immettendo il comando **fteStartLogger** `MFT5LGR1`.
5. Esaminare il contenuto del file `output0.log` in *data*`\mqft\logs\MFT5\loggers\MFT5LGR1\logs`.

   Dopo alcune informazioni sul programma di registrazione, l'ultima istruzione dovrebbe contenere il messaggio: BFGDB0023I: `Il programma di registrazione ha completato le attività di avvio ed è ora in esecuzione`.

   Di tanto in tanto, le informazioni di log potrebbero non essere scritte in `output0.log` al primo avvio del programma di registrazione. Se il file `output0.log` è vuoto, riavviare il programma di registrazione immettendo **fteStopLogger** MFT5LGR1 e premendo il tasto **Invio** .

   Riavviare il programma di registrazione immettendo **fteStartLogger** MFTULGR1 e premendo il tasto **Invio** . Il file `output0.log` ora visualizza i dati.

   Lo stesso comportamento si estende alla versione agent del file `output0.log` la prima volta che un agent viene avviato.

   Arrestare e avviare l'agente utilizzando comandi **fteStopAgent** e **fteStartAgent** . Vengono quindi visualizzati i dati di log scritti nel file `output0.log` dell'agente.

Risultati

È stato configurato il server di base, che include il gestore code di coordinamento per questa configurazione.

Operazioni successive

Ora si esegue un lavoro simile per il server partner, che contiene un agent remoto.

Configurazione di un server partner

Come configurare un server partner, quando il server di base dispone di un gestore code di coordinamento separato

Prima di iniziare

Assicurarsi di aver completato tutte le attività per configurare un server base, che include un gestore code di configurazione.

Informazioni su questa attività

Gli stessi presupposti relativi a IBM MQ e alla configurazione della sicurezza, nonché il percorso IBM MQ si applicano anche al server partner.

Iniziare impostando la directory di configurazione MFT5 e identificando il gestore code di coordinamento utilizzando il comando **fteSetupCoordination** .

Procedura

1. Creare la directory di configurazione del server partner immettendo il seguente comando:

```
fteSetupCoordination -coordinationQMgr MFT5
-coordinationQMgrHost 177.16.20.15 -coordinationQMgrPort 1771
-coordinationQMgrChannel MQMFT.MFT5.SVRCONN
```

   Note:

   a. Quando il gestore code di coordinamento si trovano su un server diverso dal server partner, la connessione al gestore code di coordinamento del server di base deve essere definito come connessione client.

      Se non si definisce la connessione del gestore code di coordinamento come una connessione client IBM MQ sul server partner, qualsiasi comando Managed File Transfer , che si connette al gestore code di coordinamento, avrà esito negativo.

      Un esempio di un comando che si connette al gestore code di coordinamento è **fteListAgents**.

   b. Non è necessario creare le definizioni IBM MQ poiché le definizioni richieste dal gestore code di coordinamento sono state completate quando è stato configurato il server di base.

2. Identificare il gestore code dei comandi immettendo il seguente comando:

```
fteSetupCommands -connectionQMgr CSM1
```

   Il gestore code dei comandi non richiede alcuna definizione IBM MQ extran.

3. Identificare il gestore code dell'agent partner e creare il gestore code dell'agent partner immettendo il seguente comando:

```
fteCreateAgent -agentName CSM1AGT1 -agentQMgr CSM1
```

4. Passare alla directory CSM1AGT1 .
5. Creare le definizioni IBM MQ richieste dall'agent, emettendo il seguente comando:

```
runmqsc CSM1 < CSM1AGT1_create.mqsc > csm1.txt
```

   a) Aprire il file `csm1.txt` con l'editor preferito per verificare che tutte le definizioni richieste dell'agente siano state create correttamente.

6. Avviare l'agent immettendo il seguente comando:

```
fteStartAgent CSM1AGT1
```

7. Visualizzare l'agent immettendo **fteListAgents**

   L'output dovrebbe essere simile al seguente:

```
C:\>fteListAgents
5655-MFT, 5724-H72 Copyright IBM Corp. 2008, 2025.  ALL RIGHTS RESERVED
BFGPR0127W: No credentials file has been specified to connect to IBM MQ. Therefo
re, the assumption is that IBM MQ authentication has been disabled.
Agent Name:     Queue Manager Name:     Status:
CSM1AGT1        CSM1                    READY
MFT4AGT1        MFT4                    READY
```

   Nota: se non è stata abilitata l'autenticazione della connessione nell'ambiente Managed File Transfer , è possibile ignorare il messaggio BFGPR0127W .

   Se si immette il comando **ftelistAgents** e si riceve il seguente messaggio, BFGCL0014W: Non `esiste alcun agent che corrisponde ai criteri di selezione correnti.`, vedere Cosa fare se l'agent MFT non viene elencato dal comando **fteListAgents**.

   Se lo stato di uno degli agent è UNREACHABLE, consultare Cosa fare se un agent viene visualizzato come in uno stato SCONOSCIUTO.

Configurazione di IBM MQ Explorer con MFT

Questa attività consente di collegare IBM MQ Explorer alla configurazione Managed File Transfer .

Procedura

1. Avviare IBM MQ Explorer.
2. Nel pannello di sinistra Navigator , scorrere verso il basso ed espandere la cartella: `Managed File Transfer`.

   Viene visualizzata la voce per il gestore code di coordinamento: MFT5
3. Fare clic con il tasto destro del mouse su MFT5 e selezionare **Connetti**.
   a) Selezionare `Agents` nel menu a discesa che viene visualizzato e verificare che entrambi gli agenti, MFT4AGT1 e CSMAGT1, siano nello stato `Ready` .

Operazioni successive

Verificare la configurazione di esempio con IBM MQ Explorer.

Utilizzo di IBM MQ Explorer per verificare un trasferimento file

Questa attività fornisce un esempio di come utilizzare IBM IBM MQ Explorer con Managed File Transfer, per verificare un trasferimento file, dopo aver impostato IBM MQ Explorer come descritto nell'argomento precedente.

Prima di iniziare

Verificare di disporre di un sistema funzionante, che gli agenti siano READY e che IBM MQ Explorer funzioni. Per ulteriori informazioni, consultare “Configurazione di IBM MQ Explorer con MFT” a pagina 163 .

Informazioni su questa attività

Determinare il file da utilizzare per verificare il trasferimento e una directory in cui copiarlo. Per questo esempio, si presume che venga utilizzato il file `test-file.txt` fuori dalla directory `C:\temp\mft` .

```
C:\temp\mft> dir *
Date stamp 61 test-file.txt
1 File(s) 61 bytes
```

Procedura

1. Avviare IBM MQ Explorer in Windows
2. Nel pannello di sinistra Navigator , espandere la cartella: `Managed File Transfer`.

   Viene visualizzata la voce per il gestore code di coordinamento: MFT5
3. Fare clic con il tasto destro del mouse su MFT5 e selezionare **Connetti**.
4. Una volta connessi, fare clic con il pulsante destro del mouse su MFT5 e selezionare **Nuovo trasferimento**
   a) Utilizzare il menu a discesa per selezionare MFT4AGT1 per l'agent di origine e CSMAGT1 per l'agent di destinazione.
   b) Fare clic su **Avanti**.
   c) Fare clic su **Aggiungi** nella finestra successiva.

      Viene visualizzata una finestra di dialogo. Il lato sinistro è per `Source` e il lato destro per `Destination`.
5. Nel pannello `Source` :
   a) Selezionare **Trasferimento testo** poiché il file è testo.

b) Selezionare **Sfoglia** per individuare il file.

In questo caso, il file è `C:\temp\mft\test-file.txt`.

Attenzione: Non selezionare **OK** per completare il pannello `Destination` .

6. Nel pannello `Destination` :
   a) Immettere il nome che si sta fornendo al file nella destinazione, ad esempio `test-file.txt`.

   L'utilizzo dei percorsi relativi è supportato. La parte superiore del percorso completo è la directory home dell'ID utente che avvia l'agent di destinazione.

   b) Selezionare `Overwrite files if present` se si richiede questa opzione.

   c) Fare clic su **OK**.

   Il file selezionato viene visualizzato nel pannello **Nuovi trasferimenti** .
7. Se il menu di configurazione MFT5 è chiuso e mostra +MFT5, espandere il menu facendo clic sul segno **+** .
8. Resta alla configurazione MFT selezionata.

   Successivamente, si verifica lo stato del trasferimento effettuando la seguente procedura.
9. Fare clic su **Log trasferimenti** nel gestore code di coordinamento MFT5.
10. Esaminare lo stato in `Managed File Transfer - Current Transfer progress panel`, immediatamente sotto il pannello superiore **Log di trasferimento** e attendere il completamento del trasferimento.

    Se il trasferimento viene visualizzato correttamente e con uno sfondo verde, è stato completato correttamente il test della propria configurazione.

    Se il trasferimento non è riuscito con uno sfondo rosso, si è verificato un errore.

    Nella maggior parte dei casi, è possibile utilizzare la barra di scorrimento sotto il pannello superiore **Log di trasferimento** e visualizzare un riepilogo dei motivi dell'errore.

    a) Se non è possibile determinare il motivo per cui il trasferimento non è riuscito, fare doppio clic sulla voce per il trasferimento nel pannello **Log trasferimenti** superiore.

    b) Selezionare XML nel riquadro sinistro del pannello a comparsa visualizzato.

    c) Scorrere le informazioni per determinare la causa dell'errore.

    d) Effettuare le correzioni necessarie e testare nuovamente il trasferimento.

Introduzione aIBM MQ Internet Pass-Thru

Questi scenari mostrano come impostare alcune semplici configurazioni IBM MQ Internet Pass-Thru (MQIPT). È inoltre possibile utilizzare queste attività per verificare che il prodotto sia stato installato correttamente.

Prima di iniziare

Prima di iniziare a utilizzare questi scenari, assicurarsi che i seguenti prerequisiti siano stati completati:

- Si ha familiarità con la definizione di gestori code, code e canali su IBM MQ.
- Sono già stati installati un client e un server IBM MQ .
- MQIPT viene installato in una directory denominata `C:\mqipt` sui sistemi Windows . (Gli esempi sono scritti per i sistemi Windows , ma verranno eseguiti su qualsiasi piattaforma supportata.) Per ulteriori informazioni sull'installazione di MQIPT, consultare Installazione di MQIPT.
- Il client, il server e ciascuna istanza di MQIPT sono installati su computer separati.
- Si ha familiarità con l'inserimento di messaggi in una coda utilizzando il comando **amqsputc** .
- Si ha familiarità con il richiamo dei messaggi da una coda utilizzando il comando **amqsgetc** .
- Si ha familiarità con l'impostazione delle autorità client in IBM MQ.

Informazioni su questa attività

Una volta completati i prerequisiti, completare i seguenti passi iniziali per impostare il sistema pronto per la gestione degli scenari.

Procedura

1. Nel server IBM MQ , completare le attività riportate di seguito:
   - Definire un gestore code denominato `MQIPT.QM1`.
   - Definire un canale di connessione server denominato `MQIPT.CONN.CHANNEL`.
   - Definire una coda locale denominata `MQIPT.LOCAL.QUEUE`.
   - Avviare un listener TCP/IP per `MQIPT.QM1` sulla porta 1414. Se la porta 1414 è già utilizzata da un'altra applicazione, scegliere un indirizzo di porta libero e sostituirlo nei seguenti esempi.
   - Verificare che l'autenticazione della connessione e dell'autenticazione del canale sia configurata per consentire le connessioni client dalla macchina client con l'ID utente. Se l'autenticazione della connessione è impostata per richiedere alle applicazioni di fornire credenziali di autenticazione per le connessioni client, sarà necessario impostare una delle seguenti variabili di ambiente prima di eseguire i comandi **amqsputc** e **amqsgetc** :

     ID UTENTE MQSAMP
     Impostare l'ID utente da utilizzare per l'autenticazione della connessione, se si desidera utilizzare un ID utente e una password per l'autenticazione con il gestore code.

     V 9.4.0 Linux AIX **MQSAMP_TOKEN**
     Impostare su un valore non vuoto se si desidera utilizzare un token di autenticazione per l'autenticazione con il gestore code.
2. Verificare l'instradamento dal client IBM MQ al gestore code inserendo un messaggio nella coda locale del gestore code, utilizzando il comando **amqsputc** e richiamandolo, utilizzando il comando **amqsgetc** .

   Per preparare gli scenari in questa sezione, creare e modificare il file `mqipt.conf` nel modo seguente:

   a. Copiare il file `mqiptSample.conf` , che è possibile trovare nella directory secondaria `samples` della directory di installazione MQIPT , in `mqipt.conf` nella directory home MQIPT scelta. I seguenti scenari utilizzano `C:\mqiptHome` come directory home MQIPT .

   b. Creare due directory insieme a `mqipt.conf` denominate `errors` e `logs`. Impostare le autorizzazioni file su queste directory in modo che siano scrivibili dall'ID utente che eseguirà MQIPT.

   c. Eliminare tutti gli instradamenti dal file `mqipt.conf` .

   d. Nella sezione `[global]` rimanente, verificare che **`ClientAccess`** esista e che sia impostata su `true`.

Operazioni successive

Dopo aver impostato il proprio sistema, si è pronti per avviare i seguenti scenari:

- “Verifica del corretto funzionamento di MQIPT” a pagina 166
- “Richiedi un certificato firmato CA per MQIPT” a pagina 168
- “Creazione di certificati di verifica” a pagina 167
- “Autenticazione di un server TLS” a pagina 171
- “Autenticazione di un client TLS” a pagina 173
- “Configurazione del tunneling HTTP” a pagina 179
- “Configurazione del controllo accessi” a pagina 181
- “Configurazione di un proxy SOCKS” a pagina 183

- “Configurazione di un client SOCKS” a pagina 185
- “Configurazione del supporto cluster MQIPT” a pagina 187
- “Assegnazione dei numeri di porta” a pagina 190
- “Richiamo di CRL utilizzando un server LDAP” a pagina 191
- “Esecuzione di MQIPT in modalità proxy TLS” a pagina 194
- “Esecuzione di MQIPT in modalità proxy TLS con un gestore sicurezza” a pagina 195
- “Utilizzo di un'uscita di sicurezza” a pagina 198
- “Instradamento delle richieste di connessione client ai server del gestore code IBM MQ utilizzando le uscite di sicurezza” a pagina 200
- “Instradamento dinamico delle richieste di connessione client” a pagina 203
- “Utilizzo di un'uscita certificato per autenticare un server TLS” a pagina 206

Verifica del corretto funzionamento di MQIPT

Utilizzare questa semplice configurazione per assicurarsi che MQIPT sia installato correttamente.

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.

Informazioni su questa attività

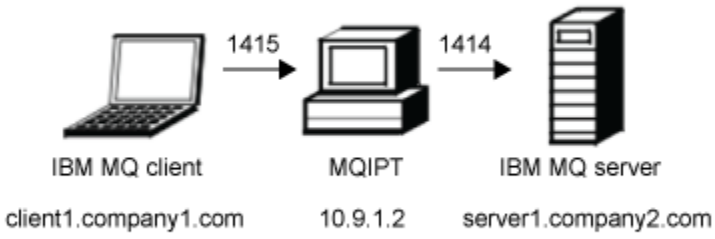


Figura 30. Diagramma di rete del test di verifica dell'installazione

Questo diagramma mostra la connessione dal client IBM MQ (denominato client1.company1.com sulla porta 1415) tramite MQIPT al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per verificare che MQIPT stia funzionando correttamente, completare la seguente procedura:

1. Definire un instradamento MQIPT .

   Nel computer MQIPT , modificare `mqipt.conf` e aggiungere una definizione di instradamento:

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   ```

2. Avviare MQIPT.

   Aprire un prompt dei comandi e immettere il comando seguente:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
   ```

dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to:
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocol
MQCPI078 Route 1415 ready for connection requests
```

3. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:
   a) Impostare la variabile di ambiente **MQSERVER** :

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

   b) Inserisci un messaggio:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
   Hello world
   ```

   Premere il tasto Invio due volte dopo aver immesso la stringa del messaggio.
   c) Ottieni il seguente messaggio:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
   ```

   Viene restituito il messaggio "Hello world".
4. Per arrestare IBM MQ, immettere il seguente comando:

```
mqiptAdmin -stop -n ipt1
```

Creazione di certificati di verifica

Un certificato autofirmato può essere utilizzato da un instradamento MQIPT per identificarsi con un peer remoto.

I certificati autofirmati possono essere utili negli scenari di test in cui è necessario garantire la connettività TLS senza pagare un'autorità di certificazione (CA) per un certificato. Tuttavia, non utilizzare certificati autofirmati negli ambienti di produzione. Se è necessario richiedere un certificato da utilizzare in un ambiente di produzione, consultare “Richiedi un certificato firmato CA per MQIPT” a pagina 168.

Prima di iniziare

Prima di avviare questa attività, completare i passi elencati in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.

Informazioni su questa attività

V 9.4.0 V 9.4.0 Utilizzare il comando **mqiptKeytool** per creare il certificato. Specificare il nome del keystore che contiene il certificato nella proprietà di instradamento **SSLServerKeyRing** o **SSLClientKeyRing** MQIPT , a seconda che il certificato sia utilizzato da connessioni in entrata o in uscita.

Procedura

Immettere il seguente comando per creare un certificato personale autofirmato per scopi di test in un keystore PKCS #12 :

```
mqiptKeytool -genkeypair -keystore keystore_name -storetype pkcs12 -storepass password
             -alias label -dname DN_identity
             -keyalg key_algorithm -keysize key_size -sigalg signature_algorithm
```

dove:

-keystore *nome_keystore*
Specifica il nome del keystore. Ad esempio, `mqiptKeys.p12`. Il keystore viene creato se non esiste.

-storepass *password*
Specifica la password del keystore.

-alias *etichetta*
Specifica l'etichetta del certificato.

-dname *identità_DN*
Specifica il DN (Distinguished Name) X.500 per il certificato racchiuso tra virgolette. Ad esempio, `"CN=Test Certificate, OU=Sales, O=Example, C=US"`.

-keyalg *algoritmo_chiave*
Specifica l'algoritmo utilizzato per creare la coppia di chiavi. Ad esempio, RSA.

-keysize *dimensione_chiave*
Specifica la dimensione della chiave. Ad esempio, 2048.

-sigalg *algoritmo_firma*
Specifica l'algoritmo utilizzato per firmare il certificato. Ad esempio, SHA256WithRSA.

Se si utilizzano i valori di esempio, questo comando crea un certificato digitale con una chiave pubblica RSA a 2048 bit e una firma digitale che utilizza RSA con l'algoritmo hash SHA-256 .

Scegli un algoritmo di crittografia della chiave pubblica appropriato, la dimensione della chiave e l'algoritmo di firma digitale per le esigenze di protezione della tua azienda. Per ulteriori informazioni, consultare Considerazioni sui certificati digitali per MQIPT.

Operazioni successive

Immettere il seguente comando per crittografare la password del keystore:

```
mqiptPW
```

Immettere la password del keystore da codificare quando richiesto. Impostare il valore della proprietà appropriata nel file di configurazione **mqipt.conf** sulla password codificata emessa dal comando **mqiptPW** . A seconda che il certificato venga utilizzato da connessioni in entrata o in uscita, impostare il valore della proprietà **SSLServerKeyRingPW** o **SSLClientKeyRingPW** o la parola d'ordine codificata. Per ulteriori informazioni sulla codifica delle password del keystore, consultare Codifica delle password memorizzate.

Richiedi un certificato firmato CA per MQIPT

Richiedere un certificato firmato da una CA (Certificate Authority) attendibile per consentire a MQIPT per utilizzare TLS.

Prima di iniziare

Prima di avviare questa attività, completare i passi elencati in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.

V 9.4.0 V 9.4.0 Questa attività presuppone che si richieda un nuovo certificato da una CA utilizzando il comando **mqiptKeytool** e che il certificato personale venga restituito in un file. Un certificato è sufficiente per abilitare l'autenticazione server per le connessioni TLS effettuate a MQIPT . Se si richiede l'autenticazione client per le connessioni TLS effettuate da MQIPT per la destinazione dell'instradamento, richiedere un secondo certificato completando due volte i passi in questa attività per creare due keystore.

Informazioni su questa attività

V 9.4.0 V 9.4.0 Utilizzare il comando **mqiptKeytool** per creare la richiesta del certificato e ricevere il certificato firmato nel keystore. Specificare il nome del keystore che contiene il certificato nella proprietà di instradamento **SSLServerKeyRing** o **SSLClientKeyRing** MQIPT , a seconda se il certificato viene utilizzato da connessioni in entrata o in uscita.

Procedura

1. Immettere il seguente comando per creare una coppia di chiavi e un certificato associato in un keystore PKCS #12 :

```
mqiptKeytool -genkeypair -keystore keystore_name -storetype pkcs12 -storepass password
             -alias label -dname DN_identity
             -keyalg key_algorithm -keysize key_size -sigalg signature_algorithm
```

   dove:

   -keystore *nome_keystore*
   Specifica il nome del keystore. Ad esempio, `mqiptKeys.p12`. Il keystore viene creato se non esiste.

   -storepass *password*
   Specifica la password del keystore.

   -alias *etichetta*
   Specifica l'etichetta del certificato.

   -dname *identità_DN*
   Specifica il DN (Distinguished Name) X.500 per il certificato racchiuso tra virgolette. Ad esempio, `"CN=Test Certificate, OU=Sales, O=Example, C=US"`.

   -keyalg *algoritmo_chiave*
   Specifica l'algoritmo utilizzato per creare la coppia di chiavi. Ad esempio, RSA.

   -keysize *dimensione_chiave*
   Specifica la dimensione della chiave. Ad esempio, 2048.

   -sigalg *algoritmo_firma*
   Specifica l'algoritmo utilizzato per firmare il certificato. Ad esempio, `SHA256WithRSA`.

   Se si utilizzano i valori di esempio, questo comando crea un certificato digitale con una chiave pubblica RSA a 2048 bit e una firma digitale che utilizza RSA con l'algoritmo hash SHA-256 .

   Scegli un algoritmo di crittografia della chiave pubblica appropriato, la dimensione della chiave e l'algoritmo di firma digitale per le esigenze di protezione della tua azienda. Per ulteriori informazioni, consultare Considerazioni sui certificati digitali per MQIPT.

2. Immettere il seguente comando per creare una richiesta di firma certificato:

```
mqiptKeytool -certreq -keystore keystore_name -storetype pkcs12 -storepass password
             -alias label -file certreq_filename
```

   dove:

   -keystore *nome_keystore*
   Specifica il nome del keystore. Ad esempio, `mqiptKeys.p12`. Il keystore viene creato se non esiste.

   -storepass *password*
   Specifica la password del keystore.

   -alias *etichetta*
   Specifica l'etichetta del certificato.

   -file *nomefile_certreq*
   Specifica il nome file per la richiesta di certificato.

   Invia il file di richieste di certificati che il comando crea alla tua CA da firmare.

3. Quando si riceve il certificato firmato dalla CA, immettere il seguente comando per aggiungere il certificato al keystore:

```
mqiptKeytool -importcert -keystore keystore_name -storetype pkcs12 -storepass password
             -file cert_filename
```

dove:

-keystore *nome_keystore*
Specifica il nome del keystore. Ad esempio, `mqiptKeys.p12`. Il keystore viene creato se non esiste.

-storepass *password*
Specifica la password del keystore.

-file *nomefile_cert*
Specifica il nome del file che contiene il certificato firmato.

4. Accertarsi che il certificato CA della CA che ha firmato il certificato personale sia presente nel keystore della CA. È possibile scegliere se aggiungere il certificato CA allo stesso keystore del certificato personale oppure a un keystore separato utilizzato solo per i certificati CA.

Per utilizzare un keystore CA separato, è possibile utilizzare il keystore CA di esempio denominato `sslCAdefault.pfx` fornito con MQIPToppure creare un nuovo keystore PKCS #12 . Aggiungere il certificato CA pubblico della CA che ha firmato il certificato personale al keystore della CA, a meno che non sia già presente nel keystore di esempio.

Il certificato CA pubblico potrebbe essere restituito con il tuo certificato personale. Se il certificato CA pubblico non viene restituito con il certificato, è necessario richiedere il certificato CA dalla stessa CA che ha fornito il certificato personale e quindi aggiungerlo al keystore.

Immettere il seguente comando per aggiungere il certificato CA al keystore CA:

```
mqiptKeytool -importcert -keystore keystore_name -storetype pkcs12 -storepass password
             -file cert_filename -alias label
```

dove:

-keystore *nome_keystore*
Specifica il nome del keystore CA. Il keystore viene creato se non esiste.

-storepass *password*
Specifica la password del keystore CA.

-file *nomefile_cert*
Specifica il nome del file che contiene il certificato CA.

-alias *etichetta*
Specifica l'etichetta da fornire al certificato CA

Operazioni successive

Immettere il seguente comando per crittografare la password del keystore:

```
mqiptPW
```

Immettere la password del keystore da codificare quando richiesto. Impostare il valore della proprietà appropriata nel file di configurazione **`mqipt.conf`** sulla password codificata emessa dal comando **`mqiptPW`** . A seconda che il certificato venga utilizzato da connessioni in entrata o in uscita, impostare il valore della proprietà **`SSLServerKeyRingPW`** o **`SSLClientKeyRingPW`** o la parola d'ordine codificata. Per ulteriori informazioni sulla codifica delle password del keystore, consultare Codifica delle password memorizzate.

Per utilizzare questi nuovi keystore per l'autenticazione del server, collocare i keystore in una directory denominata `ssl` nella directory home MQIPT e impostare le seguenti proprietà di instradamento:

```
SSLClientCAKeyRing=C:\\mqiptHome\\ssl\\sslCAdefault.pfx
SSLClientCAKeyRingPW=encrypted_password
SSLServerKeyRing=C:\\mqiptHome\\ssl\\myServer.pfx
```

```
SSLServerKeyRingPW=encrypted_password
SSLServerCAKeyRing=C:\\mqiptHome\\ssl\\sslCAdefault.pfx
SSLServerCAKeyRingPW=encrypted_password
```

Per ulteriori informazioni sulla configurazione di MQIPT per l'utilizzo di TLS, consultare “Autenticazione di un server TLS” a pagina 171.

Autenticazione di un server TLS

In questo scenario, è possibile verificare una connessione TLS utilizzando il certificato di verifica nel file keyring di esempio (`sslSample.pfx`), fornito con MQIPT nella directory secondaria `samples/ssl` della directory di installazione MQIPT .

Prima di iniziare

Prima di iniziare a utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164e di aver letto l'argomento Supporto SSL/TLS in MQIPT.

Informazioni su questa attività

La connessione viene effettuata tra un client di IBM MQ e un server IBM MQ tramite due istanze di MQIPT. La connessione tra MQIPT 1 e MQIPT 2 utilizza TLS, con MQIPT 1 che agisce come client TLS e MQIPT 2 che agisce come server TLS.

Durante l'handshake TLS, il server invia il proprio certificato di test al client e il client utilizza la copia del certificato con l'indicatore trust - as - peer impostato per autenticare il server. Viene utilizzato CipherSuite SSL_RSA_WITH_AES_256_CBC_SHA256 . il file di configurazione `mqipt.conf` in questo scenario si basa sul file di configurazione creato nello scenario “Verifica del corretto funzionamento di MQIPT” a pagina 166 . Per i dettagli su come creare un certificato di test da utilizzare in questo esempio, consultare “Creazione di certificati di verifica” a pagina 167.

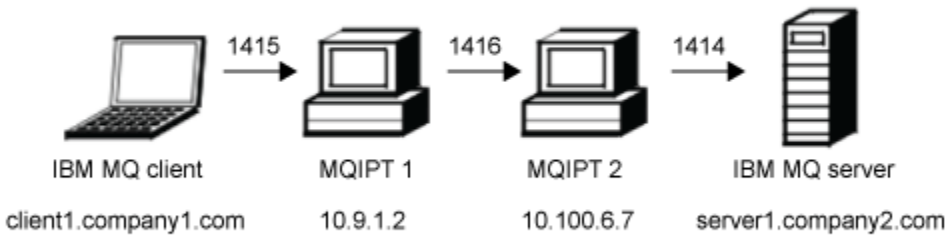


Figura 31. Diagramma di rete del server SSL/TLS

Questo diagramma mostra la connessione dal client IBM MQ (denominato client1.company1.com sulla porta 1415) tramite due istanze di MQIPT al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per autenticare un server TLS, completare la seguente procedura:

1. Sul sistema MQIPT 1:
   a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

```
[route]
ListenerPort=1415
Destination=10.100.6.7
```

```
DestinationPort=1416
SSLClient=true
SSLClientKeyRing=C:\\mqipt\\samples\\ssl\\sslSample.pfx
SSLClientKeyRingPW=<mqiptPW>1!PCaB1HWrFMOp43ngjwgArg==!6N/vsbqru7iqMhFN+wozxQ==
SSLClientCipherSuites=SSL_RSA_WITH_AES_256_CBC_SHA256
```

b) Aprire un prompt dei comandi e avviare MQIPT:

```
C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
```

dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 is starting and will forward messages to :
MQCPI034 ....10.100.6.7(1416)
MQCPI035 ....using MQ protocol
MQCPI036 ....SSL Client side enabled with properties :
MQCPI139 ......secure socket protocols <NULL>
MQCPI031 ......cipher suites SSL_RSA_WITH_AES_256_CBC_SHA256
MQCPI032 ......key ring file C:\\mqipt\\samples\\ssl\\sslSample.pfx
MQCPI047 ......CA key ring file <NULL>
MQCPI071 ......site certificate uses
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI038 ......peer certificate uses
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI078 Route 1415 ready for connection requests
```

2. Sul sistema MQIPT 2:

a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

```
[route]
ListenerPort=1416
Destination=Server1.company2.com
DestinationPort=1414
SSLServer=true
SSLServerKeyRing=C:\\mqipt\\samples\\ssl\\sslSample.pfx
SSLServerKeyRingPW=<mqiptPW>1!PCaB1HWrFMOp43ngjwgArg==!6N/vsbqru7iqMhFN+wozxQ==
SSLServerCipherSuites=SSL_RSA_WITH_AES_256_CBC_SHA256
```

b) Aprire un prompt dei comandi e avviare MQIPT:

```
C:
cd \mqipt\bin
mqipt .. -n ipt2
```

dove `..` indica che il file di configurazione MQIPT , `mqipt.conf`, si trova nella directory principale e `ipt2` è il nome da fornire all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt2
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1416 is starting and will forward messages to :
MQCPI034 ....Server1.company2.com(1414)
MQCPI035 ....using MQ protocol
MQCPI037 ....SSL Server side enabled with properties :
MQCPI139 ......secure socket protocols <NULL>
MQCPI031 ......cipher suites SSL_RSA_WITH_AES_256_CBC_SHA256
MQCPI032 ......key ring file C:\\mqipt\\samples\\ssl\\sslSample.pfx
MQCPI047 ......CA key ring file <NULL>
MQCPI071 ......site certificate uses
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI038 ......peer certificate uses
```

```
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI033 ......client authentication set to false
MQCPI078 Route 1416 ready for connection requests
```

3. Da un prompt dei comandi sul client IBM MQ , immettere i seguenti comandi:
   a) Impostare la variabile di ambiente **MQSERVER** :

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```

   b) Inserisci un messaggio:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world
```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.
   c) Ottieni il seguente messaggio:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
```

   Viene restituito il messaggio "Hello world".

Autenticazione di un client TLS

In questo scenario, è possibile verificare una connessione TLS utilizzando il certificato di test di esempio per eseguire l'autenticazione server e client.

Prima di iniziare

Prima di iniziare a utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164e di aver letto l'argomento Supporto SSL/TLS in MQIPT.

Informazioni su questa attività

La connessione viene effettuata tra un client di IBM MQ e un server IBM MQ tramite due istanze di MQIPT. La connessione tra MQIPT 1 e MQIPT 2 utilizza TLS, con MQIPT 1 che agisce come client TLS e MQIPT 2 che agisce come server TLS.

Durante l'handshake TLS, il server invia il certificato di test al client. Il client utilizza la propria copia del certificato, con l'indicatore trust - as - peer, per autenticare il server. Il client invia quindi il certificato di test al server. Il server utilizza la copia del certificato, con l'indicatore trust - as - peer, per autenticare il client. Viene utilizzato CipherSuite SSL_RSA_WITH_AES_256_CBC_SHA256 . il file di configurazione `mqipt.conf` in questo scenario si basa sul file di configurazione creato nello scenario “Verifica del corretto funzionamento di MQIPT” a pagina 166 .

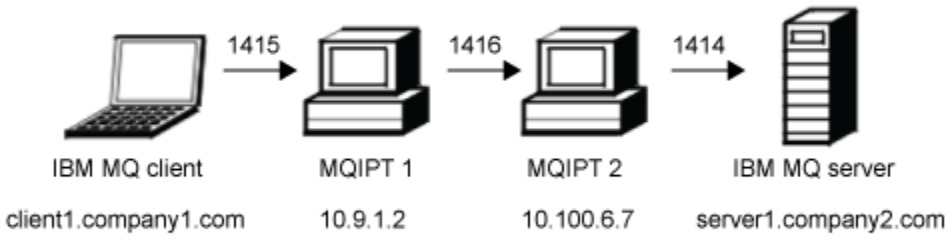


Figura 32. Diagramma di rete del client SSL/TLS

Questo diagramma mostra la connessione dal client IBM MQ (denominato client1.company1.com sulla porta 1415) tramite due istanze di MQIPT al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per autenticare un client TLS, completare la seguente procedura:

1. Sul sistema MQIPT 1:

   a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

   ```
   [route]
   ListenerPort=1415
   Destination=10.100.6.7
   DestinationPort=1416
   SSLClient=true
   SSLClientKeyRing=C:\\mqipt\\samples\\ssl\\sslSample.pfx
   SSLClientKeyRingPW=<mqiptPW>1!PCaB1HWrFMOp43ngjwgArg==!6N/vsbqru7iqMhFN+wozxQ==
   SSLClientCipherSuites=SSL_RSA_WITH_AES_256_CBC_SHA256
   ```

   b) Aprire un prompt dei comandi e avviare MQIPT:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
   ```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

   I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

   ```
   5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
   MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
   MQCPI004 Reading configuration information from mqipt.conf
   MQCPI152 MQIPT name is ipt1
   MQCPI021 Password checking has been enabled on the command port
   MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
   MQCPI006 Route 1415 is starting and will forward messages to :
   MQCPI034 ....10.100.6.7(1416)
   MQCPI035 ....using MQ protocol
   MQCPI036 ....SSL Client side enabled with properties :
   MQCPI139 ......secure socket protocols <NULL>
   MQCPI031 ......cipher suites SSL_RSA_WITH_AES_256_CBC_SHA256
   MQCPI032 ......key ring file C:\\mqipt\\samples\\ssl\\sslSample.pfx
   MQCPI047 ......CA key ring file <NULL>
   MQCPI071 ......site certificate uses
   UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
   MQCPI038 ......peer certificate uses
   UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
   MQCPI078 Route 1415 ready for connection requests
   ```

2. Sul sistema MQIPT 2:

   a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

   ```
   [route]
   ListenerPort=1416
   Destination=Server1.company2.com
   DestinationPort=1414
   SSLServer=true
   SSLServerAskClientAuth=true
   SSLServerKeyRing=C:\\mqipt\\samples\\ssl\\sslSample.pfx
   SSLServerKeyRingPW=<mqiptPW>1!PCaB1HWrFMOp43ngjwgArg==!6N/vsbqru7iqMhFN+wozxQ==
   SSLServerCipherSuites=SSL_RSA_WITH_AES_256_CBC_SHA256
   ```

   b) Aprire un prompt dei comandi e avviare MQIPT:

   ```
   C:
   cd \mqipt\bin
   mqipt .. -n ipt2
   ```

   dove `..` indica che il file di configurazione MQIPT , `mqipt.conf`, si trova nella directory principale e `ipt2` è il nome da fornire all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt2
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1416 is starting and will forward messages to :
MQCPI034 ....Server1.company2.com(1414)
MQCPI035 ....using MQ protocol
MQCPI037 ....SSL Server side enabled with properties :
MQCPI139 ......secure socket protocols <NULL>
MQCPI031 ......cipher suites SSL_RSA_WITH_AES_256_CBC_SHA256
MQCPI032 ......key ring file C:\\mqipt\\samples\\ssl\\sslSample.pfx
MQCPI047 ......CA key ring file <NULL>
MQCPI071 ......site certificate uses
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI038 ......peer certificate uses
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI033 ......client authentication set to true
MQCPI078 Route 1416 ready for connection requests
```

3. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:
   a) Impostare la variabile di ambiente **MQSERVER** :

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

   b) Inserisci un messaggio:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
   Hello world
   ```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.

   c) Ottieni il seguente messaggio:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
   ```

   Viene restituito il messaggio "Hello world".

Autenticazione di client e server TLS

È possibile eseguire MQIPT come server e client TLS per terminare la sessione TLS in entrata e inoltrare i dati alla destinazione utilizzando una connessione TLS separata.

Prima di iniziare

- Completare i passaggi elencati in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.
- Leggere l'argomento Supporto SSL/TLS in MQIPT.

Nota: Questo scenario utilizza certificati autofirmati per comodità. Non utilizzare alcun certificato autofirmato negli ambienti di produzione. Invece, ottenere i certificati firmati da una CA (Certificate Authority) attendibile.

Informazioni su questa attività

La connessione viene effettuata tra un client di IBM MQ e un server IBM MQ tramite una singola istanza di MQIPT. Le connessioni tra il client IBM MQ e MQIPTe tra MQIPT e il server IBM MQ , utilizzano entrambe TLS. Pertanto, l'instradamento MQIPT è sia un server TLS che un client TLS.

Durante l'handshake TLS fra il client e MQIPT, il client e MQIPT inviano i loro certificati l'un l'altro per autenticare la connessione. Quando viene stabilita la connessione tra client e MQIPT , MQIPT stabilisce una connessione TLS separata al server IBM MQ . MQIPT e il server IBM MQ inviano i certificati l'uno all'altro per autenticare la connessione.

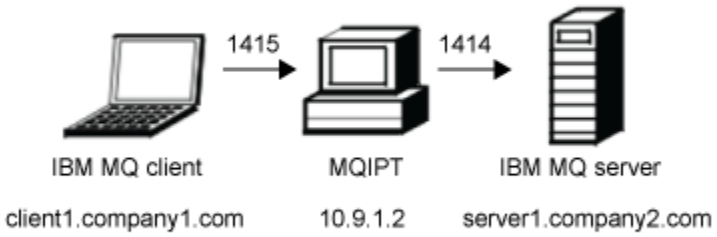


Figura 33. Diagramma di rete server e client SSL/TLS

Questo diagramma mostra la connessione dal client IBM MQ (denominato client1.company1.com) tramite una singola istanza di MQIPT al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per configurare una rotta MQIPT sia come server TLS che come client TLS, completa la seguente procedura:

1. Sul sistema in cui viene eseguito il client, completare la seguente procedura per configurare il client IBM MQ per utilizzare una connessione TLS.
   a) Creare un archivio chiavi per il client.

      Immettere il seguente comando per creare un nuovo repository chiavi denominato `clientkey.kdb` nella directory `C:\ProgramData\IBM\MQ` :

      ```
      runmqakm -keydb -create -db C:\ProgramData\IBM\MQ\clientkey.kdb -pw password -stash
      ```

      dove *password* è la password del repository delle chiavi.

      Per ulteriori informazioni, vedi Impostazione di un repository delle chiavi su AIX, Linux, and Windows.

   b) Creare un certificato personale per il client, nel repository delle chiavi client creato nel passo “1.a” a pagina 176.

      Immettere il comando riportato di seguito per creare un nuovo certificato autofirmato con etichetta `clientcert` per il client:

      ```
      runmqakm -cert -create -db C:\ProgramData\IBM\MQ\clientkey.kdb -stashed
               -label clientcert -dn CN=Client
      ```

      Per ulteriori informazioni, consultare Creazione di un certificato personale autofirmato su AIX, Linux, and Windows.

   c) Estrarre il certificato dal contenitore chiavi client.

      Immettere il comando seguente per estrarre il certificato client:

      ```
      runmqakm -cert -extract -db C:\ProgramData\IBM\MQ\clientkey.kdb -stashed -label clientcert
               -target C:\ProgramData\IBM\MQ\client.crt -format ascii
      ```

      Per ulteriori informazioni, vedi Estrazione della parte pubblica di un certificato autofirmato da un repository delle chiavi su AIX, Linux, and Windows.

   d) Copiare il file del certificato estratto sul sistema su cui è in esecuzione MQIPT .
2. Sul sistema su cui è in esecuzione il server IBM MQ , completare la seguente procedura per configurare il gestore code in modo da utilizzare una connessione TLS.
   a) Creare un repository delle chiavi per il gestore code.

Immettere il seguente comando per creare un repository delle chiavi denominato key.kdb per il gestore code.

```
runmqakm -keydb -create -db C:\ProgramData\IBM\MQ\qmgrs\MQIPT!QM1\ssl\key.kdb -pw
password -stash
```

dove *password* è la password del repository delle chiavi.

Assicurarsi che all'utente mqm sia concesso l'accesso in lettura al file stash `C:\ProgramData\IBM\MQ\qmgrs\MQIPT!QM1\ssl\key.sth` creato dal comando per memorizzare la password del repository delle chiavi codificata.

Per ulteriori informazioni, vedi Impostazione di un repository delle chiavi su AIX, Linux, and Windows.

b) Creare un certificato personale per il gestore code, nel repository delle chiavi del gestore code creato al passo "2.a" a pagina 176.

Immettere il comando riportato di seguito per creare un nuovo certificato autofirmato con etichetta `ibmwebspheremqmqipt.qm1` per il gestore code:

```
runmqakm -cert -create -db C:\ProgramData\IBM\MQ\qmgrs\MQIPT!QM1\ssl\key.kdb -stashed
         -label ibmwebspheremqmqipt.qm1 -dn CN=MQIPT.QM1
```

Per ulteriori informazioni, consultare Creazione di un certificato personale autofirmato su AIX, Linux, and Windows.

c) Estrarre il certificato dal repository delle chiavi del gestore code.

Immettere il seguente comando per estrarre il certificato gestore code:

```
runmqakm -cert -extract -db C:\ProgramData\IBM\MQ\qmgrs\MQIPT!QM1\ssl\key.kdb -stashed
-label ibmwebspheremqmqipt.qm1
         -target C:\ProgramData\IBM\MQ\qmgrs\MQIPT!QM1\ssl\mqipt.qm1.crt -format ascii
```

Per ulteriori informazioni, vedi Estrazione della parte pubblica di un certificato autofirmato da un repository delle chiavi su AIX, Linux, and Windows.

d) Copiare il file del certificato estratto sul sistema su cui è in esecuzione MQIPT .

e) Immettere il seguente comando MQSC per modificare l'MQIPT MQIPT.CONN.CHANNEL per utilizzare TLS:

```
ALTER CHANNEL(MQIPT.CONN.CHANNEL) CHLTYPE(SVRCONN) TRPTYPE(TCP)
SSLCIPH(ANY_TLS12_OR_HIGHER)
```

3. Sul sistema su cui viene eseguito MQIPT , completa la seguente procedura per configurare la rotta MQIPT per utilizzare TLS.

a) Creare un certificato personale per MQIPT in un repository delle chiavi PKCS #12 .

V 9.4.0 V 9.4.0 Immettere il seguente comando per creare un nuovo certificato autofirmato con l'etichetta `mqiptcert`:

```
mqiptKeytool -genkeypair -keystore C:\mqiptHome\ssl\mqipt.p12 -storetype pkcs12
-storepass password
           -alias mqiptcert -dname "CN=MQIPT Test Certificate"
           -keyalg RSA -keysize 2048 -sigalg SHA256WithRSA
```

dove *password* è la password del repository delle chiavi.

b) Immettere il seguente comando per aggiungere il certificato client e il certificato gestore code al repository delle chiavi MQIPT :

V 9.4.0 V 9.4.0

```
mqiptKeytool -importcert -keystore C:\mqiptHome\ssl\mqipt.p12 -storetype pkcs12
-storepass password -file client.crt
mqiptKeytool -importcert -keystore C:\mqiptHome\ssl\mqipt.p12 -storetype pkcs12
-storepass password -file mqipt.qm1.crt
```

dove *password* è la password del repository delle chiavi, *client.crt* è il file del certificato client creato nel passo “1.c” a pagina 176e *mqipt.qm1.crt* è il certificato del gestore code creato nel passo “2.c” a pagina 177.

c) Estrarre il certificato MQIPT dal repository delle chiavi.

V 9.4.0 V 9.4.0 Immettere il seguente comando per estrarre il certificato di MQIPT :

```
mqiptKeytool -exportcert -keystore C:\mqiptHome\ssl\mqipt.p12 -storetype pkcs12
-storepass password
           -alias mqiptcert -file C:\mqiptHome\ssl\mqipt.crt -rfc
```

dove *password* è la password del repository delle chiavi.

d) Copiare il file del certificato estratto sia sul sistema su cui viene eseguito il client che sul sistema su cui viene eseguito il server IBM MQ .

e) Immettere il seguente comando per codificare la password del repository delle chiavi MQIPT :

```
mqiptPW
```

Quando richiesto, immettere la password del repository delle chiavi specificata al momento della creazione del repository delle chiavi nel passo “3.a” a pagina 177.

f) Modificare il file `mqipt.conf` e aggiungere la seguente definizione di instradamento:

```
[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414
SSLServer=true
SSLServerKeyRing=C:\\mqiptHome\\ssl\\mqipt.p12
SSLServerKeyRingPW=encrypted_password
SSLClient=true
SSLClientKeyRing=C:\\mqiptHome\\ssl\\mqipt.p12
SSLClientKeyRingPW=encrypted_password
```

dove *encrypted_password* è la password del repository delle chiavi codificata creata eseguendo il comando **mqiptPW** nel passo “3.e” a pagina 178.

4. Aggiungere il certificato MQIPT al repository delle chiavi del client e al repository delle chiavi del gestore code.

a) Sul sistema in cui viene eseguito il client, immettere il seguente comando per aggiungere il certificato MQIPT al repository delle chiavi client:

```
runmqakm -cert -add -db C:\ProgramData\IBM\MQ\clientkey.kdb -stashed
         -label mqiptcert -file mqipt.crt -format ascii
```

dove *mqipt.crt* è il file del certificato MQIPT creato nel passo “3.c” a pagina 178.

b) Sul sistema su cui viene eseguito il server IBM MQ , immettere il seguente comando per aggiungere il certificato MQIPT al repository delle chiavi del gestore code:

```
runmqakm -cert -add -db C:\ProgramData\IBM\MQ\qmgrs\MQIPT!QM1\ssl\key.kdb -stashed
         -label mqiptcert -file mqipt.crt -format ascii
```

dove *mqipt.crt* è il file del certificato MQIPT creato nel passo “3.c” a pagina 178.

Per ulteriori informazioni, vedi Aggiunta di un certificato CA (o la parte pubblica di un certificato autofirmato) in un repository delle chiavi, sui sistemi AIX, Linux, and Windows.

5. Sul sistema su cui è in esecuzione MQIPT , aprire un prompt dei comandi e immettere i seguenti comandi per avviare MQIPT:

```
C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
```

dove `C:\mqiptHome` indica il percorso del file di configurazione MQIPT , `mqipt.conf`, e `ipt1` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 is starting and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocol
MQCPI036 ....SSL Client side enabled with properties :
MQCPI139 ......secure socket protocols <NULL>
MQCPI031 ......cipher suites <NULL>
MQCPI032 ......key ring file C:\\mqiptHome\\ssl\\mqipt.p12
MQCPI047 ......CA key ring file <NULL>
MQCPI071 ......site certificate uses
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI038 ......peer certificate uses
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI037 ....SSL Server side enabled with properties :
MQCPI139 ......secure socket protocols <NULL>
MQCPI031 ......cipher suites <NULL>
MQCPI032 ......key ring file C:\\mqiptHome\\ssl\\mqipt.p12
MQCPI047 ......CA key ring file <NULL>
MQCPI071 ......site certificate uses
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI038 ......peer certificate uses
UID=*,CN=*,T=*,OU=*,DC=*,O=*,STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI033 ......client authentication set to false
MQCPI078 Route 1415 ready for connection requests
```

6. Da un prompt dei comandi sul sistema client IBM MQ , immettere il seguente comando per eseguire il programma di esempio TLS:

```
AMQSSSLC -m MQIPT.QM1 -c MQIPT.CONN.CHANNEL -x 10.9.1.2(1415)
         -k "C:\ProgramData\IBM\MQ\clientkey" -l clientcert -s ANY_TLS12_OR_HIGHER
```

Il seguente messaggio indica che l'applicazione si è connessa correttamente al gestore code:

```
Connection established to queue manager MQIPT.QM1
```

Configurazione del tunneling HTTP

In questo scenario, è possibile verificare una connessione semplice tra due istanze di MQIPT su HTTP.

Prima di iniziare

Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.

Nota: V 9.4.0 V 9.4.0 Da IBM MQ 9.4.0, gli instradamenti di MQIPT non accettano connessioni HTTP per impostazione predefinita. Le rotte devono essere configurate per accettare le connessioni HTTP utilizzando la proprietà **`AllowedProtocols`** .

Informazioni su questa attività

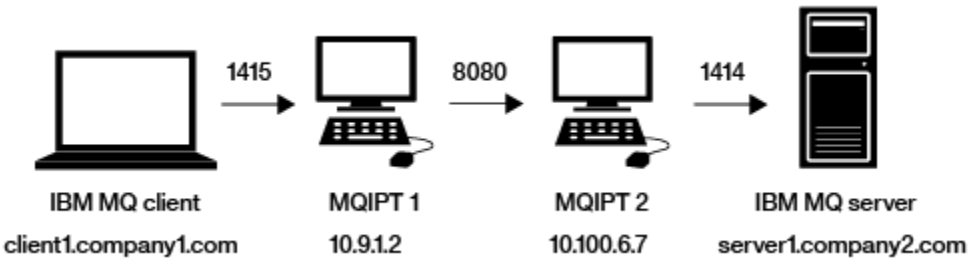


Figura 34. Diagramma di rete del tunneling HTTP

Questo diagramma mostra la connessione dal client IBM MQ (denominato client1.company1.com sulla porta 1415) attraverso due istanze di MQIPT, eseguendo il tunnelling della connessione su HTTP e infine al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per configurare il tunneling HTTP tra due istanze di MQIPT, completare la seguente procedura:

1. Sul sistema MQIPT 1:

   a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

   ```
   [route]
   ListenerPort=1415
   Destination=10.100.6.7
   DestinationPort=8080
   HTTP=true
   HTTPServer=10.100.6.7
   HTTPServerPort=8080
   ```

   b) Aprire un prompt dei comandi e avviare MQIPT:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
   ```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

   I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

   ```
   5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
   MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
   MQCPI004 Reading configuration information from mqipt.conf
   MQCPI152 MQIPT name is ipt1
   MQCPI021 Password checking has been enabled on the command port
   MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
   MQCPI006 Route 1415 is starting and will forward messages to :
   MQCPI034 ....10.100.6.7(8080)
   MQCPI035 ....using HTTP
   MQCPI066 ....and HTTP server at 10.100.6.7(8080)
   MQCPI078 Route 1415 ready for connection requests
   ```

2. Sul sistema MQIPT 2:

   a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

   ```
   [route]
   ListenerPort=8080
   Destination=Server1.company2.com
   DestinationPort=1414
   AllowedProtocols=http
   ```

   b) Aprire un prompt dei comandi e avviare MQIPT:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt2
   ```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt2` è il nome da assegnare all'istanza di MQIPT.

   I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

   ```
   5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
   MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
   MQCPI004 Reading configuration information from mqipt.conf
   MQCPI152 MQIPT name is ipt2
   MQCPI021 Password checking has been enabled on the command port
   MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
   MQCPI006 Route 8080 is starting and will forward messages to :
   MQCPI034 ....Server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI158 ....connection protocols accepted: HTTP
   MQCPI078 Route 8080 ready for connection requests
   ```

3. Da un prompt dei comandi sul client IBM MQ , immettere i seguenti comandi:

a) Impostare la variabile di ambiente **MQSERVER** :

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```

b) Inserisci un messaggio:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world
```

Premere Invio due volte dopo aver immesso la stringa del messaggio.

c) Ottieni il seguente messaggio:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
```

Viene restituito il messaggio "Hello world".

Configurazione del controllo accessi

In questo scenario, è possibile configurare MQIPT in modo che accetti solo connessioni da client specifici utilizzando Java security manager per aggiungere controlli di sicurezza sulla porta del listener MQIPT .

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.

Informazioni su questa attività

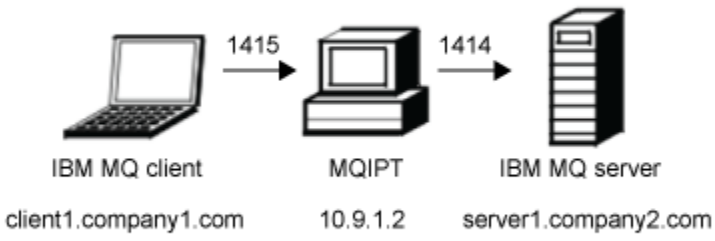


Figura 35. Diagramma della rete di controllo accessi

Questo diagramma mostra la connessione dal client IBM MQ (denominato client1.company1.com sulla porta 1415) tramite MQIPT al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per configurare il controllo accessi, completare la seguente procedura:

1. Impostare MQIPT:
   a) Copiare la politica Java security manager di esempio nella directory home di MQIPT immettendo il seguente comando da un prompt dei comandi:

```
copy C:\mqipt\samples\mqiptSample.policy C:\mqiptHome\mqipt.policy
```

   b) Avviare il programma di utilità Policy Tool utilizzando il seguente comando:

```
C:\mqipt\java\jre\bin\policytool
```

   c) Fare clic su **File** > **Apri** , quindi selezionare `C:\mqiptHome\mqipt.policy`..

d) Fare clic su **Modifica voce politica** quindi modificare CodeBase da:

```
file:/C:/Program Files/IBM/IBM MQ Internet Pass-Thru/lib/com.ibm.mq.ipt.jar
```

A:

```
file:/C:/mqipt/lib/com.ibm.mq.ipt.jar
```

e) Modificare le autorizzazioni file per le directory `IBM MQ Internet Pass-Thru`, `errors` e `logs` da:

```
C:\Program Files\IBM\IBM MQ Internet Pass-Thru
```

A:

```
C:\mqiptHome
```

f) Modificare le altre autorizzazioni file da:

```
C:\Program Files\IBM\IBM MQ Internet Pass-Thru
```

A:

```
C:\mqipt
```

g) Fare clic su **Aggiungi autorizzazione**

Completare i campi come di seguito indicato:

Autorizzazione: `java.net.SocketPermission`
Destinazione:: `client1.company1.com:1024-`
Azioni: `accetta, ascolta, risolvi`

h) Fare clic su **File> Salva** per salvare le modifiche al file della politica.

i) Modificare `mqipt.conf`.

i) Aggiungere le seguenti proprietà alla sezione `[global]` :

```
SecurityManager=true
SecurityManagerPolicy=C:\mqiptHome\mqipt.policy
```

ii) Aggiungere la seguente definizione di instradamento:

```
[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414
```

2. Avviare MQIPT:

Aprire un prompt dei comandi e immettere quanto segue:

```
C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
```

dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI055 Setting the java.security.policy to C:\mqiptHome\mqipt.policy
MQCPI053 Starting the Java Security Manager
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
```

```
MQCPI035 ....using MQ protocol
MQCPI078 Route 1415 ready for connection requests
```

3. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:
   a) Impostare la variabile di ambiente **MQSERVER** :

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

   b) Inserisci un messaggio:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
   Hello world
   ```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.
   c) Ottieni il seguente messaggio:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
   ```

   Viene restituito il messaggio "Hello world".

Configurazione di un proxy SOCKS

In questo scenario, è possibile fare in modo che MQIPT agisca come un proxy SOCKS.

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.
- Abilitare SOCKS sull'intero computer IBM MQ o solo sulle applicazioni client IBM MQ **amqsputc** e **amqsgetc**.
- Configurare il client SOCKS nel modo seguente:
  1. Utilizzare MQIPT come proxy SOCKS.
  2. Abilitare il supporto SOCKS 5.
  3. Disabilitare l'autenticazione utente.
  4. Limitare le connessioni all'indirizzo di rete MQIPT .

Informazioni su questa attività

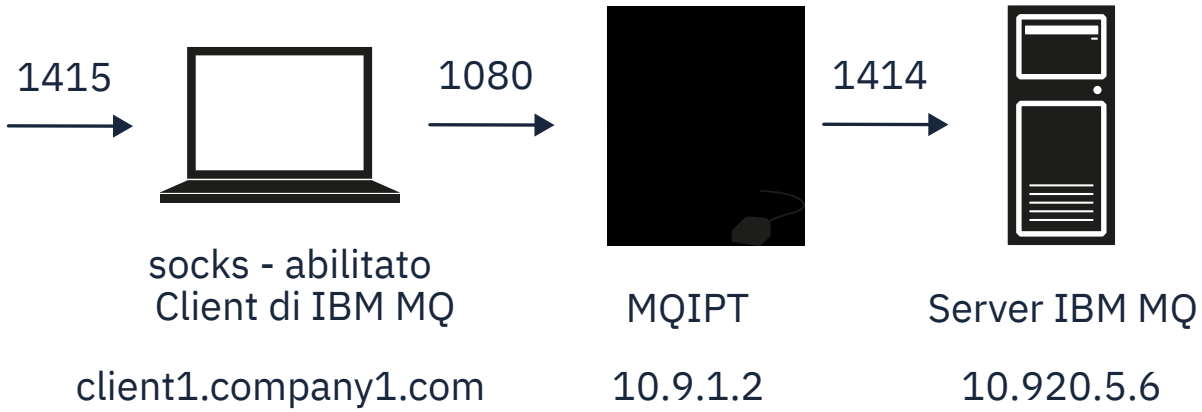


Figura 36. Diagramma di rete proxy SOCKS

Questo diagramma mostra il flusso di connessione dal client IBM MQ (denominato client1.company1.com sulla porta 1415) tramite MQIPT al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per configurare un proxy SOCKS, completare la seguente procedura:

1. Configurare e avviare MQIPT:
   a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

   ```
   [route]
   ListenerPort=1080
   Destination=server1.company2.com
   DestinationPort=1414
   SocksServer=true
   ```

   I valori delle proprietà di instradamento **Destination** e **DestinationPort** vengono ignorati poiché la destinazione reale viene ottenuta dal client IBM MQ durante il processo di handshake SOCKS.

   b) Aprire un prompt dei comandi e avviare MQIPT:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
   ```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

   I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

   ```
   5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
   MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
   MQCPI004 Reading configuration information from mqipt.conf
   MQCPI152 MQIPT name is ipt1
   MQCPI021 Password checking has been enabled on the command port
   MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
   MQCPI006 Route 1080 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocol
   MQCPI052 ....SOCKS server side enabled
   MQCPI078 Route 1080 ready for connection requests
   ```

2. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:
   a) Impostare la variabile di ambiente **MQSERVER** :

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.20.5.6(1414)
   ```

   b) Inserisci un messaggio:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
   Hello world
   ```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.

   c) Ottieni il seguente messaggio:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
   ```

   Viene restituito il messaggio "Hello world".

Configurazione di un client SOCKS

In questo scenario, è possibile eseguire MQIPT come se fosse abilitato a SOCKS, utilizzando un proxy SOCKS esistente.

È simile allo scenario “Configurazione di un proxy SOCKS” a pagina 183, ad eccezione del fatto che MQIPT effettua una connessione abilitata a SOCKS invece del client IBM MQ .

Prima di iniziare

Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164

Informazioni su questa attività

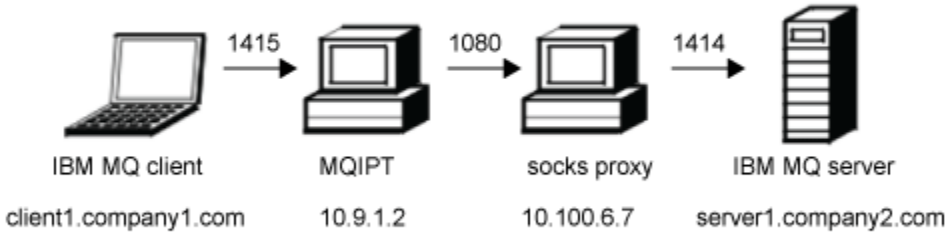


Figura 37. Diagramma di rete del client SOCKS

Questo diagramma mostra la connessione di rete dal client IBM MQ (denominato client1.company1.com sulla porta 1415) tramite MQIPT, quindi tramite il proxy SOCKS (sulla porta 1080) al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per configurare un client SOCKS, completare la seguente procedura:

1. Configura MQIPT.

   Nel computer MQIPT , modificare `mqipt.conf` e aggiungere una definizione di instradamento:

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   SocksClient=true
   SocksProxyHost=10.9.6.7
   SocksProxyPort=1080
   ```

2. Avviare MQIPT.

   Aprire un prompt dei comandi e immettere:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
   ```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

   I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

   ```
   5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
   MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
   MQCPI004 Reading configuration information from mqipt.conf
   MQCPI152 MQIPT name is ipt1
   MQCPI021 Password checking has been enabled on the command port
   MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocol
   MQCPI039 ....and SOCKS proxy at 10.9.6.7(1080)
   MQCPI078 Route 1415 ready for connection requests
   ```

3. Da un prompt dei comandi sul client IBM MQ , immettere i seguenti comandi:

   a) Impostare la variabile di ambiente **MQSERVER** :

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```

b) Inserisci un messaggio:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world
```

Premere Invio due volte dopo aver immesso la stringa del messaggio.

c) Ottieni il seguente messaggio:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
```

Viene restituito il messaggio "Hello world".

Configurazione del supporto cluster MQIPT

In questo scenario, è possibile impostare un ambiente cluster.

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.
- Sul server IBM MQ LONDON:
  - È stato definito un gestore code denominato LONDRA.
  - Definito un canale di connessione server denominato MQIPT.CONN.CHANNEL.
  - Avviato un listener TCP/IP per LONDRA sulla porta 1414.
  - SOCKS - abilita il gestore code.
- Sul server IBM MQ NEWYORK:
  - Definito un gestore code denominato NEWYORK.
  - Definito un canale di connessione server denominato MQIPT.CONN.CHANNEL.
  - Avviato un listener TCP/IP per NEWYORK sulla porta 1414.
  - SOCKS - abilita il gestore code.

Nota: Per SOCKS - abilitare un gestore code, abilitare l'intero computer o solo l'applicazione server IBM MQ . Configurare il client SOCKS nel modo seguente:

- Puntare il client a MQIPT come proxy SOCKS.
- Abilitare il supporto SOCKS V5 .
- Disabilitare l'autenticazione utente.
- Effettuare solo connessioni remote a MQIPT.

Informazioni su questa attività

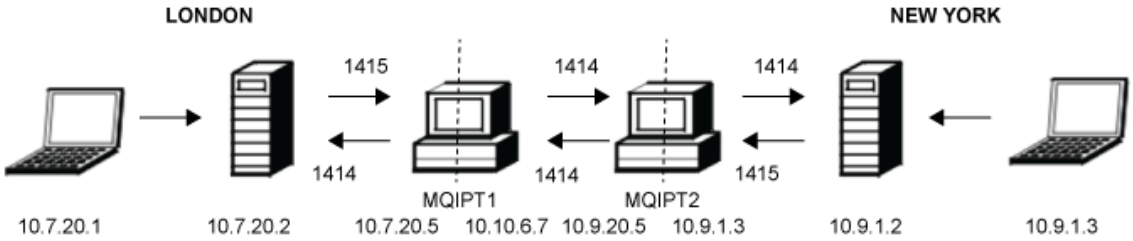


Figura 38. Diagramma di rete cluster

Questo diagramma mostra le connessioni dai client IBM MQ tramite MQIPT ai server IBM MQ .

Solo un'applicazione può essere in ascolto su una determinata porta sullo stesso computer. Se la porta 1414 è già in uso, scegliere una porta libera e sostituirla negli esempi.

È quindi possibile verificare gli instradamenti tra i gestori code inserendo un messaggio sulla coda locale sul server LONDRA e richiamandolo dal server NEWYORK.

Procedura

Per configurare il supporto cluster MQIPT , completare la seguente procedura:

1. Configurare il server LONDRA.

   Aprire un prompt dei comandi e immettere i seguenti comandi:

   ```
   runmqsc
   DEFINE CHANNEL(TO.LONDON) +
          CHLTYPE(CLUSRCVR) TRPTYPE(TCP) +
          CLUSTER(INVENTORY) +
          CONNAME('10.10.6.7(1414)')
   DEFINE CHANNEL(TO.NEWYORK) +
          CHLTYPE(CLUSSDR) TRPTYPE(TCP) +
          CLUSTER(INVENTORY) +
          CONNAME('10.9.20.5(1414)')
   ```

2. Configurare il server NEWYORK

   Aprire un prompt dei comandi e immettere i seguenti comandi:

   ```
   runmqsc
   ALTER QMGR REPOS(INVENTORY)
   DEFINE QLOCAL(MQIPT.LOCAL.QUEUE) +
          CLUSTER(INVENTORY)
   DEFINE CHANNEL(TO.NEWYORK) +
          CHLTYPE(CLUSRCVR) TRPTYPE(TCP) +
          CLUSTER(INVENTORY) +
          CONNAME('10.9.20.5(1414)')
   DEFINE CHANNEL(TO.LONDON) +
          CHLTYPE(CLUSSDR) TRPTYPE(TCP) +
          CLUSTER(INVENTORY) +
          CONNAME('10.10.6.7(1414)')
   ```

3. Impostare MQIPT 1.

   Modificare `mqipt.conf` e aggiungere le seguenti definizioni di instradamento:

   ```
   [route]
   Name=LONDON to NEWYORK
   ListenerPort=1415
   Destination=10.9.20.5
   DestinationPort=1414
   SocksServer=true

   [route]
   Name=MQIPT1 to LONDON
   ListenerPort=1414
   Destination=10.7.20.2
   DestinationPort=1414
   ```

4. Avviare MQIPT 1.

   Aprire un prompt dei comandi e immettere:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
   ```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

   I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

   ```
   5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
   MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
   MQCPI004 Reading configuration information from mqipt.conf
   MQCPI152 MQIPT name is ipt1
   MQCPI021 Password checking has been enabled on the command port
   ```

```
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....10.9.20.5(1414)
MQCPI035 ....using MQ protocol
MQCPI052 ....SOCKS server side enabled
MQCPI078 Route 1415 ready for connection requests
MQCPI006 Route 1414 has started and will forward messages to :
MQCPI034 ....10.7.20.2(1414)
MQCPI035 ....using MQ protocol
MQCPI078 Route 1414 ready for connection requests
```

5. Configurare MQIPT 2.

   Modificare `mqipt.conf` e aggiungere le seguenti definizioni di instradamento:

```
[route]
Name=NEWYORK to LONDON
ListenerPort=1415
Destination=10.10.6.7
DestinationPort=1414
SocksServer=true

[route]
Name=MQIPT2 to NEWYORK
ListenerPort=1414
Destination=10.9.1.2
DestinationPort=1414
```

6. Avviare MQIPT 2.

   Aprire un prompt dei comandi e immettere i seguenti comandi:

```
C:
cd \mqipt\bin
mqipt .. -n ipt2
```

   dove `..` indica che il file di configurazione MQIPT , `mqipt.conf`, si trova nella directory principale e `ipt2` è il nome da fornire all'istanza di MQIPT.

   I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt2
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....10.10.6.7(1414)
MQCPI035 ....using MQ protocol
MQCPI052 ....SOCKS server side enabled
MQCPI078 Route 1415 ready for connection requests
MQCPI006 Route 1414 has started and will forward messages to :
MQCPI034 ....10.9.1.2(1414)
MQCPI035 ....using MQ protocol
MQCPI078 Route 1414 ready for connection requests
```

7. Da un prompt dei comandi sul client LONDRA IBM MQ (10.7.20.1), immettere i seguenti comandi:

   a) Impostare la variabile di ambiente **MQSERVER** :

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.7.20.2(1414)
```

   b) Inserisci un messaggio:

```
amqsputc MQIPT.LOCAL.QUEUE LONDON
Hello world
```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.

   Ciò fa in modo che il gestore code LONDRA invii messaggi alla coda sul gestore code NEW YORK.

8. Da un prompt dei comandi sul client NEW YORK IBM MQ (10.9.1.3), immettere i seguenti comandi:

   a) Impostare la variabile di ambiente **MQSERVER** :

```
SET MQSERVER=MQIPT.CONN.CHANNEL/TCP/10.9.1.2(1414)
```

b) Ottieni il seguente messaggio:

```
amqsgetc MQIPT.LOCAL.QUEUE NEWYORK
```

Viene restituito il messaggio "Hello world".

Assegnazione dei numeri di porta

È possibile controllare gli indirizzi della porta locale utilizzati quando si effettuano connessioni in uscita. Ad esempio, se il firewall consente solo determinati intervalli di numeri di porta, è possibile utilizzare MQIPT per garantire che l'output abbia origine da una porta valida.

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.
- Installare MQIPT su un computer multihomed.

Informazioni su questa attività

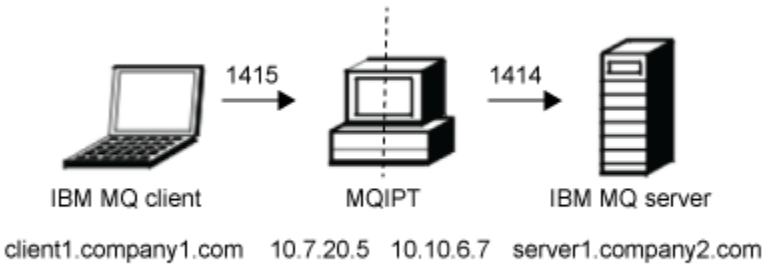


Figura 39. Diagramma di rete assegnazione porta

Questo diagramma mostra la connessione da un client IBM MQ (client1.company1.com sulla porta 1415) tramite MQIPT ad un server IBM MQ (server1.company2.com sulla porta 1414).

Procedura

Per assegnare numeri di porta, completare la seguente procedura:

1. Configura MQIPT.

   Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   LocalAddress=10.10.6.7
   OutgoingPort=2000
   MaxConnectionThreads=20
   ```

2. Avviare MQIPT.

   Aprire un prompt dei comandi sul sistema IBM MQ e immettere il seguente comando:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
   ```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.confe` `ipt1` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 is starting and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocol
MQCPI069 ....binding to local address 10.10.6.7 when making new connections
MQCPI070 ....using local port address range 2000-2019 when making new connections
MQCPI078 Route 1415 ready for connection requests
```

3. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:
   a) Impostare la variabile di ambiente **MQSERVER** :

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.7.20.5(1415)
   ```

   b) Inserisci un messaggio:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
   Hello world
   ```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.

   c) Ottieni il seguente messaggio:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
   ```

   Viene restituito il messaggio "Hello world".

Richiamo di CRL utilizzando un server LDAP

È possibile configurare MQIPT per utilizzare un server LDAP per richiamare i CRL (Certificate Revocation List).

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.
- Accertarsi che MQIPT 2 disponga di un certificato personale, emesso dalla CA (Certificate Authority) attendibile, memorizzato in un file keyring denominato `myCert.pfx`.
- Accertarsi che MQIPT 1 disponga di una copia del certificato CA attendibile che verrà utilizzata per autenticare il certificato inviato da MQIPT 2. Questo certificato viene memorizzato in un file keyring denominato `caCerts.pfx`.
- Le password per accedere ai keyring sono state codificate utilizzando il comando **mqiptPW** .

Informazioni su questa attività

In questo scenario, è possibile connettere IBM MQ client a un gestore code (QM) e inserire un messaggio IBM MQ nella coda di destinazione. L'esecuzione di una traccia MQIPT su MQIPT 1 mostrerà il server LDAP utilizzato.

Per dimostrare il funzionamento dei CRL, verificare che il certificato personale utilizzato da MQIPT 2 sia revocato dalla CA attendibile. Quindi, il client IBM MQ non è autorizzato a stabilire una connessione al gestore code, poiché la connessione da MQIPT 1 a MQIPT 2 viene rifiutata.

Non è intenzione di questo scenario spiegare come installare e configurare un server LDAP né come creare un file di chiavi contenente certificati personali o attendibili. Presuppone che il server LDAP sia disponibile da una CA nota e attendibile. Un server LDAP di backup non viene utilizzato, ma potrebbe essere implementato aggiungendo le proprietà di instradamento appropriate.

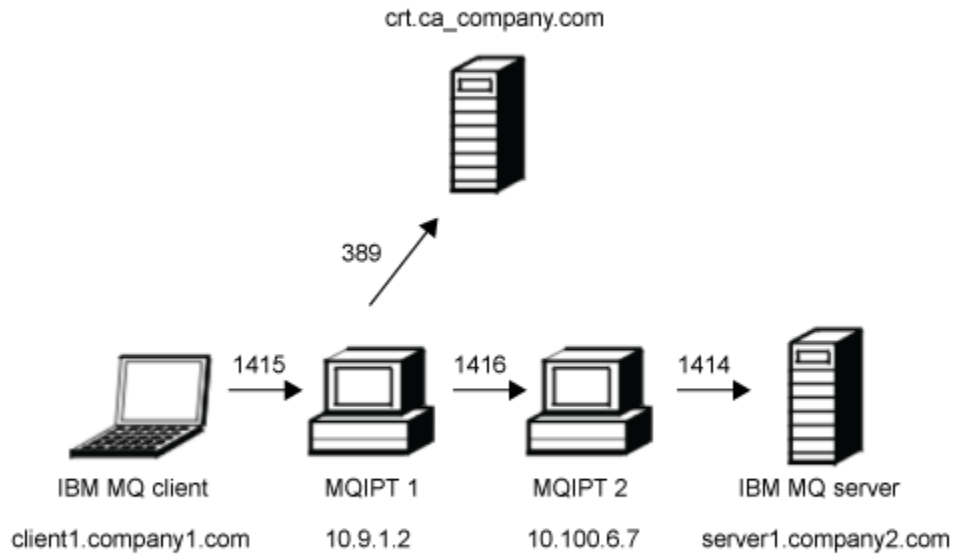


Figura 40. Diagramma di rete del server LDAP

Questo diagramma mostra la connessione dal client IBM MQ (client1.company1.com sulla porta 1415) tramite due istanze di MQIPT al server IBM MQ (server1.company2.com sulla porta 1414). Il primo MQIPT ha un collegamento a un server LDAP (crl.ca_company.com sulla porta 389).

Procedura

Per richiamare i CRL utilizzando un server LDAP, completare la seguente procedura:

1. Sul sistema MQIPT 1:
   a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

```
[route]
ListenerPort=1415
Destination=10.100.6.7
DestinationPort=1416
SSLClient=true
SSLClientCAKeyRing=C:\mqiptHome\ssl\caCerts.pfx
SSLClientCAKeyRingPW=encrypted_key_ring_password
LDAP=true
LDAPServer1=crl.ca_company.com
LDAPServer1Timeout=4
```

   dove *encrypted_key_ring_password* è la password per il keyring `caCerts.pfx` , codificata utilizzando il comando **mqiptPW** .

   b) Aprire un prompt dei comandi e avviare MQIPT:

```
C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

   I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
```

```
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....10.100.6.7(1416)
MQCPI035 ....using MQ protocol
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......CipherSuites <NULL>
MQCPI032 ......key ring file <NULL>
MQCPI047 ......CA key ring file C:\mqiptHome\ssl\caCerts.pfx
MQCPI071 ......site certificate uses UID=*,CN=*,T=*,OU=*,DC=*,O=*,
                                            STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI038 ......peer certificate uses UID=*,CN=*,T=*,OU=*,DC=*,O=*,
                                            STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI075 ....LDAP main server at crl.ca_company.com(389)
MQCPI086 ......timeout of 4 second(s)
MQCPI084 ....CRL cache expiry timeout is 1 hour(s)
MQCPI085 ....CRLs will be saved in the key-ring file(s)
MQCPI078 Route 1415 ready for connection requests
```

2. Sul sistema MQIPT 2:

   a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

   ```
   [route]
   ListenerPort=1416
   Destination=server1.company2.com
   DestinationPort=1414
   SSLServer=true
   SSLServerKeyRing=C:\mqipt\ssl\myCert.pfx
   SSLServerKeyRingPW=encrypted_key_ring_password
   ```

   dove *encrypted_key_ring_password* è la password per il keyring `myCert.pfx` , codificata utilizzando il comando **mqiptPW** .

   b) Aprire un prompt dei comandi e avviare MQIPT:

   ```
   C:
   cd \mqipt\bin
   mqipt .. -n ipt2
   ```

   dove `..` indica che il file di configurazione MQIPT , `mqipt.conf`, si trova nella directory principale e `ipt2` è il nome da fornire all'istanza di MQIPT.

   Il seguente messaggio indica il completamento con esito positivo:

   ```
   5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
   MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
   MQCPI004 Reading configuration information from mqipt.conf
   MQCPI152 MQIPT name is ipt2
   MQCPI021 Password checking has been enabled on the command port
   MQCPI011 The path C:\mqipt\logs will be used to store the log files
   MQCPI006 Route 1416 is starting and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocol
   MQCPI037 ....SSL Server side enabled with properties :
   MQCPI031 ......CipherSuites <NULL>
   MQCPI032 ......key ring file C:\mqipt\ssl\myCert.pfx
   MQCPI047 ......CA key ring file <NULL>
   MQCPI071 ......site certificate uses UID=*,CN=*,T=*,OU=*,DC=*,O=*,
                                               STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
   MQCPI038 ......peer certificate uses UID=*,CN=*,T=*,OU=*,DC=*,O=*,
                                               STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
   MQCPI033 ......client authentication set to false
   MQCPI078 Route 1416 ready for connection requests
   ```

3. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:

   a) Impostare la variabile di ambiente **MQSERVER** :

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

   b) Inserisci un messaggio:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world
```

Premere Invio due volte dopo aver immesso la stringa del messaggio.

c) Ottieni il seguente messaggio:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
```

Viene restituito il messaggio "Hello world".

Esecuzione di MQIPT in modalità proxy TLS

Puoi eseguire MQIPT in modalità proxy TLS, in modo che accetti una richiesta di connessione TLS da un client TLS IBM MQ e la esegua il tunnel a un server TLS IBM MQ .

Prima di iniziare

Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.

Informazioni su questa attività

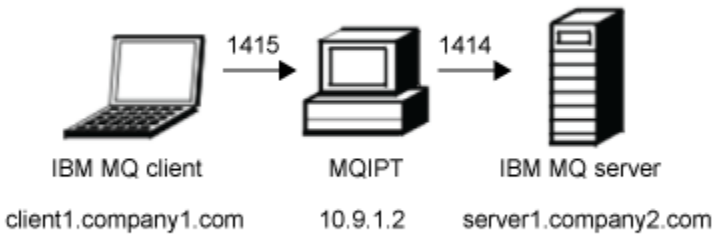


Figura 41. Diagramma di rete in modalità proxy SSL/TLS

This diagram shows the connection flow from the IBM MQ client (client1.company1.com on port 1415) through MQIPT to the IBM MQ server (server1.company2.com on port 1414).

Per ulteriori informazioni sulla configurazione di TLS per IBM MQ, fai riferimento a Utilizzo di SSL/TLS.

Procedura

Per eseguire MQIPT in modalità proxy TLS, completare la seguente procedura:

1. Configurare il client e server IBM MQ per utilizzare una connessione TLS.
   a) Creare un repository delle chiavi per il gestore code.

      Per ulteriori informazioni, vedi Impostazione di un repository delle chiavi su AIX, Linux, and Windows.

   b) Creare un repository delle chiavi per il client nella directory `C:\ProgramData\IBM\MQ` . Chiamalo *clientkey.kdb*.

   c) Creare un certificato personale per il gestore code, nel repository delle chiavi del gestore code creato nel passo “1.a” a pagina 194.

      Per ulteriori informazioni, consultare Creazione di un certificato personale autofirmato su AIX, Linux, and Windows.

   d) Creare un certificato personale per il client, nel repository delle chiavi client creato al passo “1.b” a pagina 194.

e) Estrarre il certificato personale dal repository delle chiavi del server e aggiungerlo al repository del client.

Per ulteriori informazioni, consultare Estrazione della parte pubblica di un certificato autofirmato da un repository delle chiavi su AIX, Linux, and Windowse Aggiunta di un certificato CA (o della parte pubblica di un'autocertificazione) in un repository delle chiavi, su sistemi AIX, Linux, and Windows.

f) Estrarre il certificato personale dal repository delle chiavi del client e aggiungerlo al repository delle chiavi del server.

g) Modificare MQIPT.CONN.CHANNEL per utilizzare TLS utilizzando il comando MQSC:

```
ALTER CHANNEL(MQIPT.CONN.CHANNEL) CHLTYPE(SVRCONN) TRPTYPE(TCP)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
```

2. Per eseguire MQIPT in modalità proxy TLS, completare la seguente procedura:

a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

```
[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414
SSLProxyMode=true
```

b) Avviare MQIPT.

Aprire un prompt dei comandi e immettere il comando seguente:

```
C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
```

dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using SSLProxyMode protocol
MQCPI078 Route 1415 ready for connection requests
```

3. Da un prompt dei comandi sul sistema client IBM MQ , immettere il seguente comando per eseguire il programma di esempio TLS:

```
AMQSSSLC -m MQIPT.QM1 -c MQIPT.CONN.CHANNEL -x 10.9.1.2(1415)
         -k "C:\ProgramData\IBM\MQ\clientkey" -l cert_label -s
TLS_RSA_WITH_AES_128_CBC_SHA256
```

dove `cert_label` è l'etichetta del certificato client creato nel passaggio “1.d” a pagina 194.

Esecuzione di MQIPT in modalità proxy TLS con un gestore sicurezza

Puoi eseguire MQIPT in modalità proxy TLS, in modo che accetti una richiesta di connessione TLS da un client TLS IBM MQ e la esegua il tunnel a un server TLS IBM MQ . Utilizzando un gestore della sicurezza con MQIPT, è possibile limitare gli indirizzi a cui possono essere inviati i messaggi.

Prima di iniziare

Nota: Deprecated L'utilizzo di Java security manager con MQIPT è obsoleto poiché Java security manager è obsoleto per la rimozione in una release futura di Java.

Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.

Informazioni su questa attività

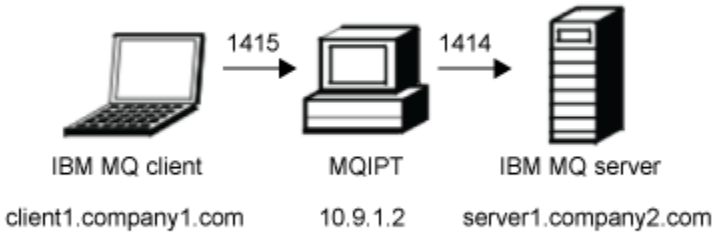


Figura 42. Diagramma di rete in modalità proxy SSL/TLS

This diagram shows the connection flow from the IBM MQ client (client1.company1.com on port 1415) through MQIPT to the IBM MQ server (server1.company2.com on port 1414).

Per ulteriori informazioni sulla configurazione di TLS per IBM MQ, fai riferimento a Utilizzo di SSL/TLS.

Procedura

Per eseguire MQIPT in modalità proxy TLS con un gestore sicurezza, completare la seguente procedura:

1. Configurare il client e server IBM MQ per utilizzare una connessione TLS.
   a) Creare un repository delle chiavi per il gestore code.

      Per ulteriori informazioni, vedi Impostazione di un repository delle chiavi su AIX, Linux, and Windows.
   b) Creare un repository delle chiavi per il client nella directory `C:\ProgramData\IBM\MQ` . Chiamalo *clientkey.kdb*.
   c) Creare un certificato personale per il gestore code, nel repository delle chiavi del gestore code creato nel passo “1.a” a pagina 196.

      Per ulteriori informazioni, consultare Creazione di un certificato personale autofirmato su AIX, Linux, and Windows.
   d) Creare un certificato personale per il client, nel repository delle chiavi client creato al passo “1.b” a pagina 196.
   e) Estrarre il certificato personale dal repository delle chiavi del server e aggiungerlo al repository del client.

      Per ulteriori informazioni, consultare Estrazione della parte pubblica di un certificato autofirmato da un repository delle chiavi su AIX, Linux, and Windowse Aggiunta di un certificato CA (o della parte pubblica di un'autocertificazione) in un repository delle chiavi, su sistemi AIX, Linux, and Windows.
   f) Estrarre il certificato personale dal repository delle chiavi del client e aggiungerlo al repository delle chiavi del server.
   g) Modificare MQIPT.CONN.CHANNEL per utilizzare TLS utilizzando il comando MQSC:

      ```
      ALTER CHANNEL(MQIPT.CONN.CHANNEL) CHLTYPE(SVRCONN) TRPTYPE(TCP)
      SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
      ```
2. Sul computer MQIPT (vedere diagramma), copiare la politica Java security manager di esempio nella directory home MQIPT , immettendo il seguente comando da un prompt dei comandi:

   ```
   copy C:\mqipt\samples\mqiptSample.policy C:\mqiptHome\mqipt.policy
   ```
3. Avviare il programma di utilità Policy Tool utilizzando il seguente comando:

   ```
   C:\mqipt\java\jre\bin\policytool
   ```

Nello strumento della politica:

a) Fare clic su **File** > **Apri** , quindi selezionare `C:\mqiptHome\mqipt.policy.`.

b) Seleziona:

```
file:/C:/Program Files/IBM/IBM MQ Internet Pass-Thru/lib/com.ibm.mq.ipt.jar
```

quindi fare clic su **Modifica voce politica**

c) Modificare `CodeBase` da:

```
file:/C:/Program Files/IBM/IBM MQ Internet Pass-Thru/lib/com.ibm.mq.ipt.jar
```

A:

```
file:/C:/mqipt/lib/com.ibm.mq.ipt.jar
```

d) Modificare le autorizzazioni file per le directory `IBM MQ Internet Pass-Thru`, `errors` e `logs` da:

```
C:\Program Files\IBM\IBM MQ Internet Pass-Thru
```

A:

```
C:\mqiptHome
```

e) Modificare le altre autorizzazioni file da:

```
C:\Program Files\IBM\IBM MQ Internet Pass-Thru
```

A:

```
C:\mqipt
```

f) Fare clic su **Aggiungi autorizzazione**

Completare i campi come di seguito indicato:

Autorizzazione: `java.net.SocketPermission`
Destinazione:: `client1.company1.com:1024-`
Azioni: `accetta, ascolta, risolvi`

g) Fare clic su **File> Salva** per salvare le modifiche al file della politica.

4. Modificare `mqipt.conf`. Aggiungere le seguenti proprietà alla sezione `[global]` e aggiungere la seguente definizione di instradamento:

```
[global]
SecurityManager=true
SecurityManagerPolicy=C:\mqiptHome\mqipt.policy

[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414
SSLProxyMode=true
```

5. Avviare MQIPT.

Aprire un prompt dei comandi e immettere il comando seguente:

```
C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
```

dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.confe` `ipt1` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
```

```
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI055 Setting the java.security.policy to C:\mqiptHome\mqipt.policy
MQCPI053 Starting the Java Security Manager
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\mqipt\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using SSLProxyMode protocol
MQCPI078 Route 1415 ready for connection requests
```

6. Da un prompt dei comandi sul sistema client IBM MQ , immettere il seguente comando per eseguire il programma di esempio TLS:

```
AMQSSSLC -m MQIPT.QM1 -c MQIPT.CONN.CHANNEL -x 10.9.1.2(1415)
         -k "C:\ProgramData\IBM\MQ\clientkey" -l cert_label -s
TLS_RSA_WITH_AES_128_CBC_SHA256
```

dove `cert_label` è l'etichetta del certificato client creato nel passaggio “1.d” a pagina 196.

Utilizzo di un'uscita di sicurezza

In questo scenario, è possibile utilizzare un'uscita di sicurezza di esempio fornita, denominata SampleSecurityExit, in modo che siano consentite soltanto connessioni client che utilizzano un nome canale che inizia con i caratteri `MQIPT.` .

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.
- Installare JavaJava 8.0 JDK.
- Aggiungere la sottodirectory Java `bin` alla variabile d'ambiente **PATH** .

Informazioni su questa attività

L'uscita di esempio utilizzata in questo scenario è `SampleSecurityExit.java`. Viene fornito con MQIPT nella sottodirectory `samples/exits` della directory di installazione di MQIPT .

Se si utilizza il nome del canale di connessione server suggerito `MQIPT.CONN.CHANNEL` (come utilizzato nella maggior parte di questi scenari), la connessione client verrà completata e sarà possibile inserire un messaggio IBM MQ nella coda.

Per dimostrare che l'uscita di sicurezza funziona come previsto, definire un altro canale di connessione server con qualsiasi nome che non inizi con i caratteri `MQIPT.` (ad esempio, `TEST.CONN.CHANNEL`) e ripetere il comando **amqsputc** , ma modificando la variabile di ambiente **MQSERVER** per utilizzare il nuovo nome del canale. Questa volta la connessione verrà rifiutata e verrà restituito un errore 2059 (MQRC_Q_MGR_NOT_AVAILABLE).

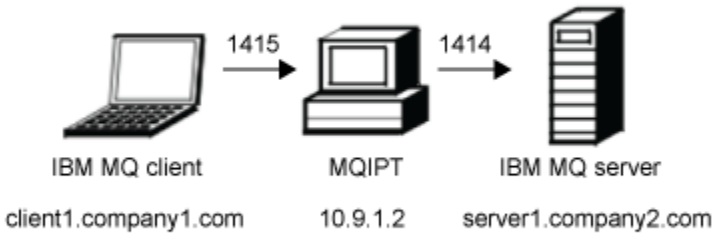


Figura 43. Diagramma di rete dell'uscita di sicurezza

Questo diagramma mostra il flusso di connessione dal client IBM MQ (denominato client1.company1.com sulla porta 1415) tramite MQIPT al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per utilizzare un'uscita di sicurezza, completare la seguente procedura:

1. Sul computer MQIPT :
   a) Creare una directory denominata `exits` nella directory home MQIPT immettendo il seguente comando in un prompt dei comandi:

   ```
   md C:\mqiptHome\exits
   ```

   b) Immettere i comandi seguenti per compilare l'uscita. Non è necessario eseguire questa operazione se il codice di uscita non è stato modificato poiché l'uscita di esempio compilata viene fornita con MQIPT.

   ```
   C:
   cd \mqipt\samples\exits
   javac -classpath C:\mqipt\lib\com.ibm.mq.ipt.jar;. SampleSecurityExit.java
   ```

   c) Immettere il seguente comando per copiare il file di classe di uscita compilato `SampleSecurityExit.class` nella directory `C:\mqiptHome\exits` :

   ```
   copy C:\mqipt\samples\exits\SampleSecurityExit.class C:\mqiptHome\exits
   ```

   d) Modificare `mqipt.conf` e aggiungere una definizione di instradamento:

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   SecurityExit=true
   SecurityExitName=SampleSecurityExit
   ```

   e) Aprire un prompt dei comandi e avviare MQIPT:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
   ```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

   I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

   ```
   5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
   MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
   MQCPI004 Reading configuration information from mqipt.conf
   MQCPI152 MQIPT name is ipt1
   MQCPI021 Password checking has been enabled on the command port
   MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocol
   MQCPI079 ....using security exit C:\mqiptHome\exits\SampleSecurityExit
   MQCPI080 ......and timeout of 30 seconds
   MQCPI078 Route 1415 ready for connection requests
   ```

2. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:
   a) Impostare la variabile di ambiente **MQSERVER** :

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

   b) Inserisci un messaggio:

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
   Hello world
   ```

Premere Invio due volte dopo aver immesso la stringa del messaggio.

c) Ottieni il seguente messaggio:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
```

Viene restituito il messaggio "Hello world".

Instradamento delle richieste di connessione client ai server del gestore code IBM MQ utilizzando le uscite di sicurezza

In questo scenario, è possibile instradare in modo dinamico le richieste di connessione client, in modo round - robin, a un gruppo di tre server gestore code IBM MQ . Il gestore code su ciascun server nel gruppo deve essere identico.

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.
- Installare Java 8.0 JDK.
- Aggiungere la sottodirectory Java `bin` alla variabile d'ambiente **PATH** .

Informazioni su questa attività

L'uscita di esempio utilizzata in questo scenario è `SampleRoutingExit.java`. Viene fornito con MQIPT nella sottodirectory `samples/exits` della directory di installazione di MQIPT .

Il nome e l'ubicazione del file di classe di uscita compilato sono definiti con le proprietà MQIPT **SecurityExitName** e **SecurityExitPath** .

L'elenco di nomi di gestori code e server da utilizzare viene letto da un file di configurazione, denominato `SampleRoutingExit.conf`. L'uscita si aspetta che il file di configurazione esista nella sottodirectory '`exits` della home directory 'MQIPT.

La prima volta che il comando **amqsputc** viene eseguito, il messaggio IBM MQ viene inserito in MQIPT.LOCAL.QUEUE sul primo server. La seconda volta che viene eseguito, il messaggio viene inserito nella coda sul secondo server e così via. Utilizzando questa impostazione, non è possibile per il comando **amqsgetc** richiamare il messaggio appena inserito nella coda, perché la richiesta di connessione client utilizzata dal comando **amqsgetc** viene passata alla coda successiva nell'elenco. Tuttavia, l'esecuzione del comando **amqsputc** tre volte, seguita da tre comandi **amqsgetc** , garantisce che ogni messaggio venga richiamato nello stesso ordine.

Naturalmente, utilizzando un altro client IBM MQ , che si connette direttamente a un gestore code (ossia, non utilizzando MQIPT in questo esempio), è possibile richiamare selettivamente i messaggi da qualsiasi gestore code.

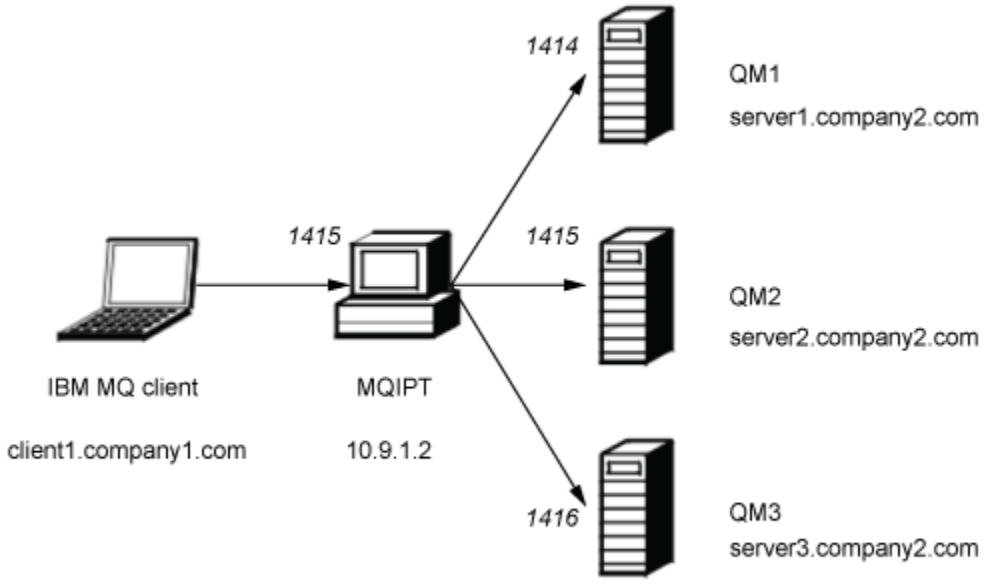


Figura 44. Diagramma di rete uscita di sicurezza instradamento

Questo diagramma mostra il flusso di collegamenti dal client IBM MQ (denominato client1.company1.com sulla porta 1415) attraverso MQIPT a tre server IBM MQ (denominati server1.company2.com, server2.company2.come server3.company2.com).

Procedura

Per instradare le richieste di connessione client in modo sequenzialmente a tre diversi server del gestore code IBM MQ utilizzando le uscite di sicurezza, completare la seguente procedura:

1. Creare tre gestori code identici denominati MQIPT.QM1 su tre server separati.

   Ogni gestore code ha un canale SVRCONN denominato MQIPT.CONN.CHANNEL e una coda locale vuota denominata MQIPT.LOCAL.QUEUE.
2. Sul server MQIPT :
   a) Creare una directory denominata `exits` nella directory home MQIPT immettendo il seguente comando in un prompt dei comandi:

   ```
   md C:\mqiptHome\exits
   ```

   b) Nella directory `C:\mqiptHome\exits` (dove `C:\mqiptHome` è la directory in cui si trova il file `mqipt.conf`), creare un file di configurazione di esempio, denominato `SampleRoutingExit.conf` che contiene i nomi dei tre gestori code.

   Ad esempio, il file di configurazione potrebbe contenere le seguenti voci:

   ```
   server1.company2.com:1414
   server2.company2.com:1415
   server3.company2.com:1416
   ```

   Accertarsi che non vi siano righe vuote prima della prima voce nel file e che ciascuna voce sia un nome server valido. Se sono stati utilizzati nomi server differenti, modificare tali nomi in modo che corrispondano all'ambiente.

c) Aprire un prompt dei comandi e immettere i seguenti comandi per compilare l'uscita. Non è necessario eseguire questa operazione se il codice di uscita non è stato modificato poiché l'uscita di esempio compilata viene fornita con MQIPT.

```
C:
cd \mqipt\samples\exits
javac -classpath C:\mqipt\lib\com.ibm.mq.ipt.jar;. SampleRoutingExit.java
```

d) Immettere il seguente comando per copiare il file di classe di uscita compilato `SampleRoutingExit.class` nella directory `C:\mqiptHome\exits` :

```
copy C:\mqipt\samples\exits\SampleRoutingExit.class C:\mqiptHome\exits
```

e) Modificare `mqipt.conf` e aggiungere una definizione di instradamento:

```
[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414
SecurityExit=true
SecurityExitPath=C:\mqiptHome\exits
SecurityExitName=SampleRoutingExit
```

Notare che non è necessario impostare **SecurityExitPath** se si inserisce `SampleRoutingExit.conf` nella directory `C:\mqiptHome\exits` predefinita.

f) Avviare MQIPT.

Aprire un prompt dei comandi e immettere il comando seguente:

```
C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
```

dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.conf`e `ipt1` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocol
MQCPI079 ....using security exit C:\mqiptHome\exits\SampleRoutingExit
MQCPI080 ......and timeout of 30 seconds
MQCPI078 Route 1415 ready for connection requests
```

3. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:

a) Impostare la variabile di ambiente **MQSERVER** :

```
SET MQSERVER=MQIPT.CONN.CHANNEL/TCP/10.9.1.2(1415)
```

b) Inserire tre messaggi:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world 1
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world 2
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world 3
```

Premere Invio due volte dopo aver immesso ogni stringa di messaggio.

c) Richiamare i messaggi:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
```

Vengono restituiti i messaggi `Hello world 1`, `Hello world 2`e `Hello world 3` .

Instradamento dinamico delle richieste di connessione client

In questo scenario, è possibile instradare dinamicamente le richieste di connessione client a un server di destinazione, in base al nome del canale utilizzato.

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.
- Installare Java 8.0 JDK.
- Aggiungere la sottodirectory Java `bin` alla variabile d'ambiente **PATH** .

Informazioni su questa attività

Se si utilizza il nome del gestore code come prima parte del nome del canale, è necessario utilizzare solo un instradamento MQIPT per soddisfare tutte le richieste di connessione. Ad esempio, per connettersi a QM1, il nome di un canale SVRCONN potrebbe essere QM1.MQIPT.CHANNEL.

L'uscita di esempio utilizzata in questo scenario è `SampleOneRouteExit.java`. Viene fornito con MQIPT nella sottodirectory `samples/exits` della directory di installazione di MQIPT .

Il nome e l'ubicazione del file di classe di uscita compilato sono definiti con le proprietà MQIPT **`SecurityExitName`** e **`SecurityExitPath`** .

L'elenco di nomi di gestori code e server da utilizzare viene letto da un file di configurazione, denominato `SampleOneRouteExit.conf`. L'uscita prevede che il file di configurazione esista nella stessa directory del file di classe di uscita.

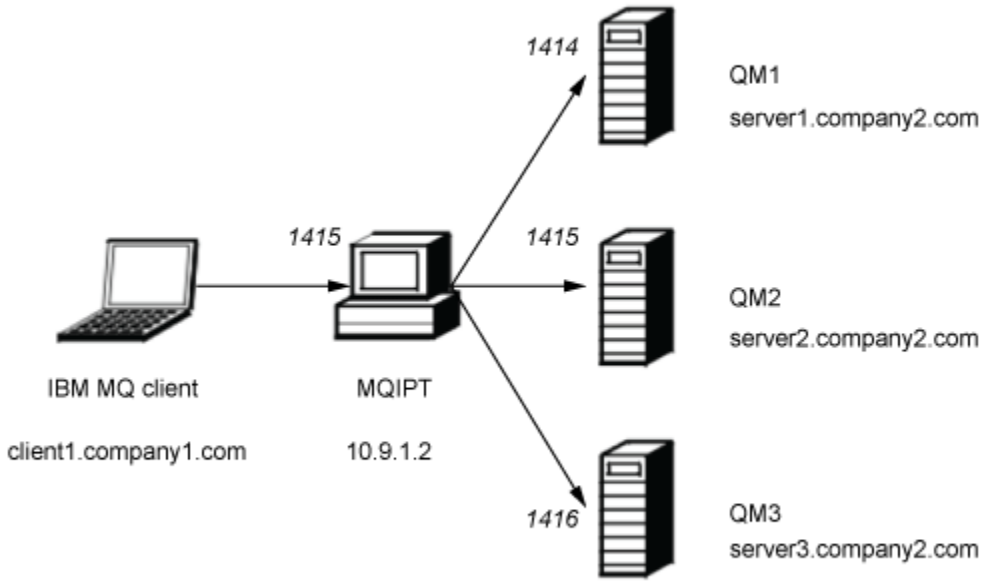


Figura 45. Diagramma di rete di uscita di un instradamento dinamico

Questo diagramma mostra il flusso di collegamenti dal client IBM MQ (denominato client1.company1.com sulla porta 1415) attraverso MQIPT a tre server IBM MQ (denominati server1.company2.com, server2.company2.come server3.company2.com).

Procedura

Per instradare dinamicamente le richieste di connessione client, completare la seguente procedura:

1. Creare tre gestori code differenti su tre server diversi.

   Ogni gestore code ha un canale SVRCONN che prende il nome da se stesso, ad esempio QM1.MQIPT.CHANNEL sul gestore code QM1e una coda locale vuota denominata MQIPT.LOCAL.QUEUE.

2. Sul server MQIPT :

   a) Creare una directory denominata `exits` nella directory home MQIPT immettendo il seguente comando in un prompt dei comandi:

   ```
   md C:\mqiptHome\exits
   ```

   b) Nella directory `C:\mqiptHome\exits` (dove `C:\mqiptHome` è la directory in cui si trova il file `mqipt.conf`), creare un file di configurazione di esempio, denominato `SampleOneRouteExit.conf` che contiene i nomi dei tre gestori code.

   Ad esempio, il file di configurazione potrebbe contenere le seguenti voci:

   ```
   QM1 server1.company2.com:1414
   QM2 server2.company2.com:1415
   QM3 server3.company2.com:1416
   ```

   Accertarsi che non vi siano righe vuote prima della prima voce nel file e che ciascuna voce sia un nome server valido. Se sono stati utilizzati nomi server differenti, modificare tali nomi in modo che corrispondano all'ambiente.

   Tenere presente che tutti i nomi dei gestori code nell'elenco devono essere univoci. Se si elenca lo stesso nome più di una volta, anche se i gestori code si trovano su server differenti, viene registrata solo l'ultima voce per tale nome.

   c) Aprire un prompt dei comandi e immettere i seguenti comandi per compilare l'uscita. Non è necessario eseguire questa operazione se il codice di uscita non è stato modificato poiché l'uscita di esempio compilata viene fornita con MQIPT.

   ```
   C:
   cd \mqipt\samples\exits
   javac -classpath C:\mqipt\lib\com.ibm.mq.ipt.jar;. SampleOneRouteExit.java
   ```

   d) Immettere il seguente comando per copiare il file di classe di uscita compilato `SampleOneRouteExit.class` nella directory `C:\mqiptHome\exits` :

   ```
   copy C:\mqipt\samples\exits\SampleOneRouteExit.class C:\mqiptHome\exits
   ```

   e) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   SecurityExit=true
   SecurityExitName=SampleOneRouteExit
   ```

   f) Aprire un prompt dei comandi e avviare MQIPT:

   ```
   C:\mqipt\bin\mqipt C:\mqiptHome -n ipt2
   ```

   dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.confe` `ipt2` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt2
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocol
MQCPI079 ....using security exit C:\mqiptHome\exits\SampleOneRouteExit
MQCPI080 ......and timeout of 5 seconds
MQCPI078 Route 1415 ready for connection requests
```

3. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:
   a) Impostare la variabile di ambiente **MQSERVER** :

   ```
   SET MQSERVER=QM1.MQIPT.CHANNEL/TCP/10.9.1.2(1415)
   ```

   b) Inserisci un messaggio:

   ```
   amqsputc MQIPT.LOCAL.QUEUE QM1
   Hello world 1
   ```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.

   Il messaggio viene instradato da MQIPT a QM1 in quanto il nome del canale SVRCONN inizia con QM1.

   c) Richiamare il messaggio da QM1:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE QM1
   ```

   Viene restituito il messaggio `Hello world 1` .

   d) Reimpostare la variabili di ambiente **MQSERVER** :

   ```
   SET MQSERVER=QM2.MQIPT.CHANNEL/TCP/10.9.1.2(1415)
   ```

   e) Inserisci un messaggio:

   ```
   amqsputc MQIPT.LOCAL.QUEUE QM2
   Hello world 2
   ```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.

   Il messaggio viene instradato da MQIPT a QM2 in quanto il nome del canale SVRCONN inizia con QM2.

   f) Richiamare il messaggio da QM2:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE QM2
   ```

   Viene restituito il messaggio `Hello world 2` .

   g) Reimpostare nuovamente la variabile di ambiente **MQSERVER** :

   ```
   SET MQSERVER=QM3.MQIPT.CHANNEL/TCP/10.9.1.2(1415)
   ```

   h) Inserisci un messaggio:

   ```
   amqsputc MQIPT.LOCAL.QUEUE QM3
   Hello world 3
   ```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.

   Il messaggio viene instradato da MQIPT a QM3 poiché il nome del canale SVRCONN inizia con QM3.

   i) Richiamare il messaggio da QM3:

   ```
   amqsgetc MQIPT.LOCAL.QUEUE QM3
   ```

Viene restituito il messaggio `Hello world 3` .

Utilizzo di un'uscita certificato per autenticare un server TLS

In questo scenario, è possibile autenticare una connessione TLS utilizzando un'uscita certificato.

Prima di iniziare

- Prima di utilizzare questo scenario, assicurarsi di aver completato le attività prerequisite elencate in “Introduzione aIBM MQ Internet Pass-Thru” a pagina 164.
- Installare Java 8.0 JDK.
- Aggiungere la sottodirectory Java `bin` alla variabile d'ambiente **PATH** .

Informazioni su questa attività

Questo scenario esegue la stessa funzione dello scenario “Autenticazione di un server TLS” a pagina 171 , con l'aggiunta di un'uscita certificato.

L'uscita di esempio utilizzata in questo scenario è `SampleCertificateExit.java`. Viene fornito con MQIPT nella sottodirectory `samples/exits` della directory di installazione di MQIPT .

Modificando il valore della proprietà **SSLExitData** , la connessione TLS tra i due server MQIPT può essere consentita o rifiutata.

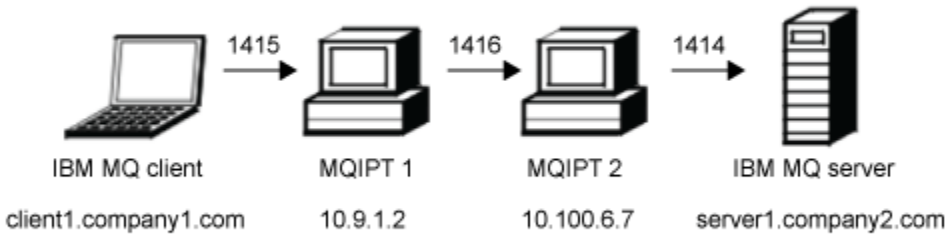


Figura 46. Diagramma di rete del server SSL/TLS

Questo diagramma mostra la connessione dal client IBM MQ (denominato client1.company1.com sulla porta 1415) tramite due istanze di MQIPT al server IBM MQ (denominato server1.company2.com sulla porta 1414).

Procedura

Per utilizzare un'uscita certificato per autenticare un server TLS, completare la seguente procedura:

1. Sul sistema MQIPT 1:
   a) Creare una directory denominata `exits` nella directory home MQIPT immettendo il seguente comando in un prompt dei comandi:

   ```
   md C:\mqiptHome\exits
   ```

   b) Aprire un prompt dei comandi e immettere i seguenti comandi per compilare l'uscita. Non è necessario eseguire questa operazione se il codice di uscita non è stato modificato poiché l'uscita di esempio compilata viene fornita con MQIPT.

   ```
   C:
   cd \mqipt\samples\exits
   javac -classpath C:\mqipt\lib\com.ibm.mq.ipt.jar;. SampleCertificateExit.java
   ```

c) Immettere il seguente comando per copiare il file di classe di uscita compilato `SampleCertificateExit.class` nella directory `C:\mqiptHome\exits` :

```
copy C:\mqipt\samples\exits\SampleCertificateExit.class C:\mqiptHome\exits
```

d) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

```
[route]
ListenerPort=1415
Destination=9.100.6.7
DestinationPort=1416
SSLClient=true
SSLClientKeyRing=C:\mqipt\samples\ssl\sslSample.pfx
SSLClientKeyRingPW=<mqiptPW>1!PCaB1HWrFMOp43ngjwgArg==!6N/vsbqru7iqMhFN+wozxQ==
SSLClientExit=true
SSLExitName=SampleCertificateExit
SSLExitPath=C:\mqiptHome\exits
SSLExitData=allow
```

e) Aprire un prompt dei comandi e avviare MQIPT:

```
C:\mqipt\bin\mqipt C:\mqiptHome -n ipt1
```

dove `C:\mqiptHome` indica l'ubicazione del file di configurazione MQIPT , `mqipt.confe` `ipt1` è il nome da assegnare all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt1
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqiptHome\logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using MQ protocol
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......CipherSuites <null>
MQCPI032 ......keyring file C:\mqipt\samples\ssl\sslSample.pfx
MQCPI047 ......CA keyring file <null>
MQCPI038 ......peer certificate uses UID=*,CN=*,T=*,OU=*,DC=*,O=*,
                                          STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI129 ......using certificate exit C:\mqiptHome\exits\SampleCertificateExit
MQCPI131 ......and certificate exit data 'allow'
MQCPI078 Route 1415 ready for connection requests
```

2. Sul sistema MQIPT 2:

a) Modificare `mqipt.conf` e aggiungere la seguente definizione di instradamento:

```
[route]
ListenerPort=1416
Destination=Server1.company2.com
DestinationPort=1414
SSLServer=true
SSLServerKeyRing=C:\mqipt\samples\ssl\sslSample.pfx
SSLServerKeyRingPW=C:\mqipt\samples\ssl\sslSample.pwd
```

b) Aprire un prompt dei comandi e avviare MQIPT:

```
C:
cd \mqipt\bin
mqipt .. -n ipt2
```

dove `..` indica che il file di configurazione MQIPT , `mqipt.conf`, si trova nella directory principale e `ipt2` è il nome da fornire all'istanza di MQIPT.

I seguenti messaggi indicano che MQIPT è stato avviato correttamente:

```
5724-H72 (C) Copyright IBM Corp. 2000, 2025. All Rights Reserved
MQCPI001 IBM MQ Internet Pass-Thru V9.4.0.0 starting
MQCPI004 Reading configuration information from mqipt.conf
MQCPI152 MQIPT name is ipt2
```

```
MQCPI021 Password checking has been enabled on the command port
MQCPI011 The path C:\mqipt\logs will be used to store the log files
MQCPI006 Route 1416 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocol
MQCPI037 ....SSL Server side enabled with properties :
MQCPI031 ......CipherSuites <null>
MQCPI032 ......key ring file C:\mqipt\samples\ssl\sslSample.pfx
MQCPI047 ......CA key ring file <null>
MQCPI038 ......peer certificate uses UID=*,CN=*,T=*,OU=*,DC=*,O=*,
                                          STREET=*,L=*,ST=*,PC=*,C=*,DNQ=*
MQCPI033 ......client authentication set to false
MQCPI078 Route 1416 ready for connection requests
```

3. Da un prompt dei comandi sul sistema client IBM MQ , immettere i comandi riportati di seguito:
   a) Impostare la variabile di ambiente **MQSERVER** :

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```

   b) Inserisci un messaggio:

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT.QM1
Hello world
```

   Premere Invio due volte dopo aver immesso la stringa del messaggio.

   c) Ottieni il seguente messaggio:

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT.QM1
```

   Viene restituito il messaggio "Hello world".

V 9.4.0 MQ Adv. MQ Adv. VUE MQ Adv. z/OS Scenari di Kafka Connect

Con IBM MQ e Apache Kafka specializzati in diversi aspetti dello spettro di messaggistica, uno sulla connettività e l'altro sui dati, le soluzioni spesso richiedono il flusso di dati tra i due. È possibile ottenere ciò utilizzando Kafka Connect.

Kafka Connect fornisce un framework per spostare i dati da un sistema esterno in un cluster Kafka o da un cluster Kafka in un sistema esterno. Ciò è ottenuto dai connettori.

Sono disponibili connettori per molti sistemi esterni diversi e IBM fornisce connettori da utilizzare con IBM MQ. Esistono due diversi tipi di connettore:

- I connettori di origine trasferiscono i dati da un sistema esterno a Kafka.

  Il connettore di origine IBM MQ utilizza i messaggi da una coda IBM MQ e li pubblica come eventi in un argomento Kafka .
- I connettori sink trasferiscono i dati in un sistema esterno da Kafka.

  Il connettore sink IBM MQ consuma eventi da un argomento Kafka e li invia come messaggi a una coda IBM MQ.

Per ulteriori informazioni, vedere Kafka Connect e connettori.

Gli scenari di Kafka Connect potrebbero includere:

- Un sistema di core banking con IBM MQ utilizzato come backbone di connettività. Vuoi prendere una copia dei messaggi spostandoli in IBM MQ e trasmetterli in Kafka per l'analisi
- Si desidera estendere il sistema bancario principale per emettere i dati in Kafka, ma si desidera che i dati vengano immessi solo Kafka quando la transazione bancaria viene completata correttamente, quindi utilizzare IBM MQ come bridge transazionale
- z/OS È necessario ottenere i dati in z/OS da Multiplatforms. Il team di sviluppo multipiattaforma ha esperienza con Kafka, il team z/OS desidera sfruttare l'integrazione IBM MQ con CICS / IMS

Da IBM MQ 9.4.0, se l'azienda ha diritto a IBM MQ Advanced for z/OS, IBM MQ Advanced for z/OS VUE, IBM MQ Advanced for Multiplatforms o IBM MQ Appliance , si ottiene l'accesso a IBM e ai connettori

source e sink supportati. Il supporto per i connettori IBM MQ Kafka include il supporto per il convertitore XML di Kafka Connect (https://github.com/ibm-messaging/kafka-connect-xml-converter), a condizione che il convertitore sia distribuito in una pipeline Kafka Connect insieme al connettore IBM MQ source o sink, per la comunicazione con IBM MQ.

V 9.4.2 Il convertitore XML di Kafka Connect è incluso insieme ai connettori sink e source da IBM MQ 9.4.2 in poi.

V 9.4.3 Da IBM MQ 9.4.3, il supporto per i connettori IBM MQ Kafka include il supporto per Kafka Connect al solo scopo di far funzionare i connettori source e sink di IBM MQ .

Note:

1. Questi approcci possono essere utilizzati con qualsiasi variante di Kafka, ad esempio Apache Kafka e IBM Event Streams.
2. Il supporto è fornito solo per i due connettori IBM e per il convertitore XML, non per il framework Kafka Connect stesso V 9.4.3 , a meno che il framework Kafka Connect non sia ottenuto dal Kafka Connect fornito da IBM MQ 9.4.3.
3. V 9.4.3 I connettori, i convertitori e il framework Kafka Connect forniti con IBM MQ possono essere utilizzati con le precedenti versioni supportate di IBM MQ.

V 9.4.0 MQ Adv. MQ Adv. VUE MQ Adv. z/OS Topologie comuni di Kafka Connect

Questa sezione descrive i tre approcci che possono essere utilizzati durante l'integrazione di IBM MQ con Kafka tramite i connettori IBM .

Fare riferimento a “Come ottenere i connettori” a pagina 215 per ulteriori informazioni su come ottenere i connettori e a “Utilizzo dei connettori” a pagina 215 per ulteriori informazioni sulle opzioni di configurazione e di connessione del gestore code.

Diretto alla coda (origine)

Le applicazioni che desiderano inviare dati a Kafka utilizzando IBM MQ possono inviare tali messaggi alla coda utilizzata dal connettore di origine IBM MQ . Il connettore di origine IBM MQ prende quindi tali messaggi e li trasferisce all'argomento Kafka pertinente.

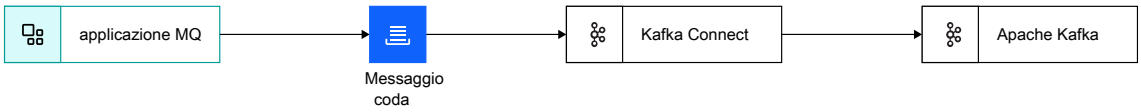


Figura 47. Diretto alla coda (origine)

Questo approccio deve essere utilizzato quando un'applicazione deve inviare dati in Kafka e tali dati non sono già stati inviati a IBM MQ.

L'invio di dati tramite IBM MQ significa che l'invio del messaggio può avvenire all'interno di una transazione coordinata con altri aggiornamenti, ad esempio di un database. Questo approccio evita anche la necessità di configurare una connessione potenzialmente di breve durata a Kafkae di utilizzare invece una connessione esistente a IBM MQ.

Copia coda di flusso (origine)

In molti casi è necessario prendere una copia dei dati esistenti spostandosi attraverso IBM MQ e inviandoli in Kafka, ad esempio, per l'analisi. Questo può essere ottenuto utilizzando code di streaming. Le code di flusso consentono ai messaggi inseriti in una coda di essere copiati dal gestore code in una seconda coda, senza influire sulle applicazioni che utilizzano la prima. Per ulteriori informazioni, consultare “Code di streaming” a pagina 29.

Ad esempio:

```
DEF QL(TO.APP) STREAMQ(TO.KAFKA) STRMQOS(MUSTDUP)
DEF QL(TO.KAFKA)
```

indica che quando un messaggio viene inviato a TO.APP, una copia di tale messaggio deve essere inviata a TO.KAFKA. Il connettore di origine IBM MQ acquisisce quindi tali messaggi da TO.KAFKA e li trasferisce all'argomento Kafka pertinente.

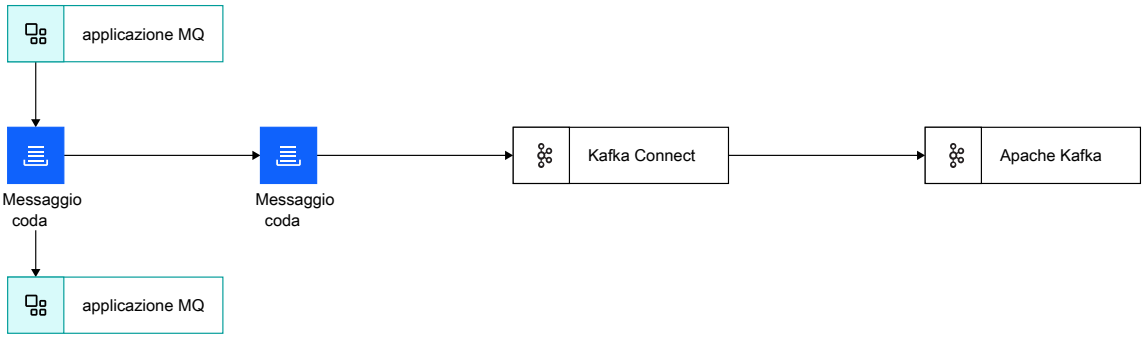


Figura 48. Copia coda di flusso (origine)

L'abilitazione delle code di flusso non ha alcun effetto sulle applicazioni esistenti, in quanto il messaggio originale non cambia. Il messaggio inviato alla seconda coda è identico al messaggio originale con lo stesso payload, ID messaggio, ID correlazione e così via.

Diretto alla coda (sink)

Come per il connettore di origine, il connettore sink può essere configurato per ricevere i dati da un argomento Kafka direttamente in una coda.

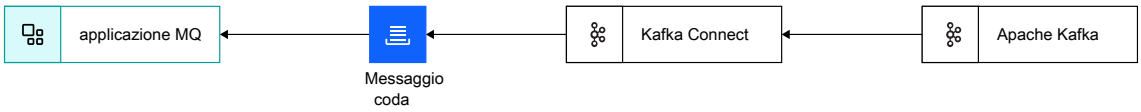


Figura 49. Diretto alla coda (sink)

La ricezione di dati tramite IBM MQ significa che la ricezione del messaggio può essere effettuata all'interno di una transazione coordinata con altri aggiornamenti, ad esempio su un database.

Questo approccio evita anche la necessità di impostare una connessione potenzialmente di breve durata a Kafka, utilizzando invece una connessione esistente a IBM MQ.

Come ottenere i connettori

z/OS In IBM MQ Advanced for z/OS Value Unit Edition e IBM MQ Advanced for z/OS, i connettori e i relativi esempi vengono forniti nella directory `kafka-connect` del componente Connector Pack, in z/OS UNIX System Services (USS). V 9.4.3 Da IBM MQ 9.4.3, è inclusa una versione supportata del framework Kafka Connect.

Multi In 'IBM MQ Advanced for Multiplatforms e 'IBM MQ Appliance, questi connettori e i file di configurazione richiesti possono essere recuperati accedendo a 'Fix Central e cercando '`V.R.M.F-IBM-MQ-Kafka-Connectors.tar.gz`, ad esempio '`9.4.0.0-IBM-MQ-Kafka-Connectors.tar.gz`.
V 9.4.3 Da IBM MQ 9.4.3, è inclusa una versione supportata del framework Kafka Connect.

MQ Adv. MQ Adv. VUE MQ Adv. z/OS Questo è ciò che viene fornito con ogni versione di IBM MQ :

IBM MQ numero versione	Nome file tar IBM MQ for Multiplatforms	Versione connettore di origine	Versione connettore sink	V 9.4.2 Versione del convertitore XML	V 9.4.3 Kafka Collegare
V 9.4.0 V 9.4.0 9.4.0	9.4.0.0-IBM-MQ-Kafka_Connectors.tar.gz	2.0.0	2.1.0	N/A	N/A
V 9.4.1 9.4.1	9.4.1.0-IBM-MQ-Kafka_Connectors.tar.gz	2.1.0	2.2.0	N/A	N/A
V 9.4.2 9.4.2	9.4.2.0-IBM-MQ-Kafka_Connectors.tar.gz	2.3.0	2.2.1	0.2.1	N/A
V 9.4.3 9.4.3	9.4.3.0-IBM-MQ-Kafka_Connectors.tar.gz	2.3.0	2.2.1	0.2.1	2.13-3.9.0

Note:

1. Si consiglia di prendere sempre la versione più recente dei connettori e controllare regolarmente gli aggiornamenti. I connettori forniti con IBM MQ sono i più recenti al momento della spedizione del prodotto e vengono aggiornati periodicamente alla versione più recente.
2. Se il supporto per i connettori IBM MQ viene fornito tramite la titolarità a IBM MQ Advanced for z/OS Value Unit Edition, IBM MQ Advanced for Multiplatforms o IBM MQ Appliance, i connettori devono essere connessi a un gestore code in esecuzione con tale titolarità.

Utilizzo dei connettori

V 9.4.3 Da IBM MQ 9.4.3, i connettori possono essere eseguiti utilizzando una versione supportata di Kafka, che viene fornita con i connettori.

I connettori sono configurati utilizzando le proprietà o i file JSON. I file di esempio vengono forniti con i connettori.

I dettagli sulle opzioni di configurazione e su come impostare i connettori sono disponibili all'indirizzo:

Connettore di origine: Kafka Connect source connector per IBM MQ

Connettore sink: Kafka connettore sink Connect per IBM MQ

V 9.4.0 Per abilitare il supporto exactly-once nel connettore sorgente, vedere Esecuzione del connettore sorgente MQ e per il connettore sink vedere Esecuzione del connettore sink MQ. V 9.4.3 Da IBM MQ 9.4.3, è inclusa una versione supportata del framework Kafka Connect.

V 9.4.0 Per ulteriori informazioni sulle differenze tra la consegna almeno una volta e quella esatta e su come configurare la consegna esattamente una volta, consultare “Supporto esattamente una volta” a pagina 217.

Affinché Kafka Connect possa eseguire i IBM MQ connettori, deve avere i jar dei connettori e vari altri file jar nel suo percorso di classe. Sono richiesti i seguenti file jar:

`jms.jar`
`com.ibm.mq.allclient.jar`
`org.json.jar`
V 9.4.0 `bcpkix-jdk18on.jar`
V 9.4.0 `bcprov-jdk18on.jar`
V 9.4.0 `bcutil-jdk18on.jar`
V 9.4.0 jackson-annotations.jar
V 9.4.0 jackson-core.jar
V 9.4.0 jackson-databind.jar
V 9.4.0 slf4j-api.jar con una versione >= 2.0.7

Tutti questi elementi, a parte `slf4j-api.jar`, sono già disponibili nell'installazione di IBM MQ. `slf4j-api.jar` può essere scaricato da Maven.

Ad esempio:

Connettore di origine

V 9.4.0 V 9.4.0 :

```
export CLASSPATH=$CLASSPATH:/path-to-kafka-jars/kafka-connect-mq-source-2.0.0.jar:
/path-to-mq-jars/jms.jar:/path-to-mq-jars/com.ibm.mq.allclient.jar:/path-to-mq-jars/org.json.jar:
/path-to-mq-jars/bcpkix-jdk18on.jar:/path-to-mq-jars/bcprov-jdk18on.jar:/path-to-mq-jars/bcutil-
jdk18on.jar:
/path-to-mq-jars/jackson-annotations.jar:/path-to-mq-jars/jackson-core.jar:/path-to-mq-jars/jackson-
databind.jar:
/path-to-slfj-jar/slf4j-api.jar
```

Connettore sink

V 9.4.0 V 9.4.0 :

```
export CLASSPATH=$CLASSPATH:/path-to-kafka-jars/kafka-connect-mq-sink-2.1.0.jar:
/path-to-mq-jars/jms.jar:/path-to-mq-jars/com.ibm.mq.allclient.jar:/path-to-mq-jars/org.json.jar:
/path-to-mq-jars/bcpkix-jdk18on.jar:/path-to-mq-jars/bcprov-jdk18on.jar:/path-to-mq-jars/bcutil-
jdk18on.jar:
/path-to-mq-jars/jackson-annotations.jar:/path-to-mq-jars/jackson-core.jar:/path-to-mq-jars/jackson-
databind.jar:
/path-to-slfj-jar/slf4j-api.jar
```

dove:

`path-to-kafka-jars` è il percorso dell'ubicazione in cui sono installati i connettori IBM MQ
`path-to-mq-jars` è il percorso dell'ubicazione in cui è installato il client IBM JMS .
`path-to-slfj-jar` è il percorso della posizione in cui è installato `slf4j-api.jar` .

z/OS Se in esecuzione su z/OS, USS_ROOT/`kafka-connect/source/kafka-connect-mq-source.jar`, nel componente Connector Pack, punta alla versione più recente del connettore di origine

e USS_ROOT/kafka-connect/sink/kafka-connect-mq-sink.jar punta alla versione più recente del connettore sink.

Kafka Connect, e i connettori IBM MQ possono essere eseguiti su qualsiasi piattaforma con una macchina virtuale Java. Non devono essere eseguiti sulla stessa piattaforma dei gestori code o sul cluster Kafka a cui si connettono.

Tuttavia, se c'è una lunga distanza tra i gestori code e i cluster Kafka , è necessario posizionare i connettori relativamente vicini ai gestori code; idealmente nella stessa zona di disponibilità o nello stesso centro dati.

Utilizzo dei connettori su z/OS

z/OS

I connettori sono completamente supportati con i gestori code in esecuzione su tutte le piattaforme, incluso su z/OS. Le connessioni ai gestori code z/OS possono essere effettuate tramite un canale di connessione server o tramite bind locali.

Negli ambienti di test delle prestazioni su IBM z/OS e IBM MQ for z/OS, sono state ottenute prestazioni ottimali eseguendo i connettori su z/OS in z/OS UNIX System Services (USS) e connettendosi ai gestori code utilizzando i bind locali. I dettagli relativi a queste ricerche sono disponibili qui: Kafka Connectors per IBM MQ - una prospettiva MQ per z/OS.

LTS L'esecuzione di Kafka Connect in USS su z/OS richiede alcuni passaggi di configurazione aggiuntivi, la cui documentazione è riportata qui: Esecuzione dei connettori su IBM z/OS.

V 9.4.3 Le istruzioni per l'utilizzo dei connettori di z/OS con il Connect di Kafka fornito nel pacchetto di connettori di IBM MQ 9.4.3 sono riportate qui: “Esecuzione di Kafka Connect su IBM z/OS” a pagina 218. In alternativa, le istruzioni per scaricare manualmente, e regolare, Kafka Connect per farlo funzionare su z/OS sono qui: https://ibm.github.io/event-automation/es/connecting/mq/zos/.

Utilizzo del convertitore XML

V 9.4.2

Da IBM MQ 9.4.2, il jar del convertitore XML si trova all'indirizzo path-to-kafka-jars/kafka-connect-xml-converter-0.2.1.jar.

z/OS Se viene eseguito su z/OS, USS_ROOT/kafka-connect/xml-converter/kafka-connect-xml-converter.jar, nel componente Connector Pack, punta alla versione più recente di XML Converter.

V 9.4.0 MQ Adv. MQ Adv. VUE MQ Adv. z/OS

Supporto esattamente una volta

Esistono due versioni di IBM MQ Kafka Connectors, 1 e 2. I connettori versione 2 forniscono il supporto per la consegna del messaggio esattamente una volta e almeno una volta, mentre i connettori versione 1 forniscono il supporto per la consegna del messaggio almeno una volta.

La consegna del messaggio almeno una volta significa che in caso di errore, in IBM MQ, in IBM MQ Kafka Connector o in Kafka:

- Per il connettore di origine, i messaggi IBM MQ non vengono persi, ma potrebbero essere consegnati a Kafka più volte con conseguente duplicazione di messaggi Kafka .
- Per il connettore sink, i messaggi Kafka non vengono persi, ma potrebbero essere consegnati a IBM MQ più volte, risultando in messaggi IBM MQ duplicati.

La consegna del messaggio esattamente una volta indica che in caso di errore, in IBM MQ, nel connettore IBM MQ Kafka o in Kafka:

- Per il connettore di origine, i messaggi IBM MQ non vengono persi e verranno consegnati a Kafka senza possibilità di duplicati Kafka .

- per il connettore sink, i messaggi Kafka non vengono persi e verranno consegnati a IBM MQ senza alcuna possibilità di duplicare i messaggi IBM MQ .

Il supporto esattamente una volta è disponibile solo nel connettore versione 2 fornito con IBM MQo con IBM Event Streams. Non è disponibile nel connettore versione 1.

Il connettore versione 2 può essere eseguito in modalità almeno una volta o esattamente una volta. Il supporto esattamente una volta è abilitato dalla configurazione appropriata di Kafkae utilizzando una "*coda di stato*". Ogni istanza di un connettore in esecuzione in modalità esattamente una volta ha bisogno della propria coda di stato.

La velocità effettiva e la scalabilità dei connettori in esecuzione in modalità esattamente una volta sono inferiori a quelle in esecuzione in modalità almeno una volta. Abilita la modalità esattamente una volta solo se le tue applicazioni non sono progettate per funzionare con messaggi duplicati.

Consultare Esecuzione del connettore di origine MQ per i dettagli sulla configurazione della modalità esattamente una volta nel connettore di origine e Esecuzione del connettore sink MQ per i dettagli sulla configurazione della modalità esattamente una volta nel connettore sink.

z/OS V 9.4.3 MQ Adv. VUE MQ Adv. z/OS Esecuzione di Kafka Connect su IBM z/OS

Da IBM MQ 9.4.3, il componente Connector Pack contiene un framework Kafka Connect supportato per l'esecuzione dei connettori IBM MQ in z/OS UNIX System Services. Questo framework deve essere utilizzato solo per l'esecuzione dei connettori di IBM MQ , non per l'esecuzione di altri connettori.

Informazioni su questa attività

Per eseguire Kafka Connect in z/OS UNIX System Services, collegandosi a un gestore di code locale, seguire questa procedura.

Procedura

- Preparare l'ambiente per l'esecuzione di Kafka Connect.
  a) Installare il componente Connector Pack seguendo le istruzioni contenute nella directory del programma IBM MQ Advanced for z/OS . Per ulteriori informazioni, vedere Installazione di IBM MQ Advanced for z/OS.

     Il componente Connector Pack contiene una directory *USS_ROOT*/`kafka-connect` , con le seguenti sottodirectory:

     – `kafka-connect`: il framework Kafka Connect
     – `sink`: il connettore del lavello IBM MQ
     – `source`: il connettore della sorgente IBM MQ
     – `xml-convertor`: il convertitore XML

     dove *USS_ROOT* è la radice dell'installazione di IBM MQ z/OS UNIX System Services .
  b) Kafka Connect viene avviato tramite uno script bash. Se non avete già installato bash sul vostro sistema z/OS , ottenetelo da https://www.ibm.com/products/open-enterprise-foundation-zos.
  c) Decidete se eseguire Kafka Connect in modalità standalone o distribuita.

     Per ulteriori informazioni e per decidere quale modalità utilizzare, consultare la spiegazione dei lavoratori di Kafka Connect.
  d) Creare una directory di lavoro per contenere la configurazione personalizzata di Kafka Connect e dei connettori.

     Per il resto di queste istruzioni, questa directory è chiamata `WORK_DIR`.
  e) Copiate `connect-standalone.properties`, per la modalità stand alone, o `connect-distributed.properties`, per la modalità distribuita, da *USS_ROOT*/`kafka-connect/kafka-connect/config` a `WORK_DIR`.

Nel file di proprietà copiato, modificare la proprietà **bootstrap.servers** in modo che punti al broker Kafka . Regolare le altre proprietà in base alle esigenze dell'installazione.

f) Impostare STEPLIB in modo che punti a IBM per l'installazione di z/OS . Questa operazione deve essere eseguita nel JCL utilizzato per avviare Kafka Connect oppure nella sessione z/OS UNIX System Services .

Ad esempio:

```
export STEPLIB=thlqual.SCSQAUTH:thlqual.SCSQANLE:$STEPLIB
```

sostituendo *thlqual* con il qualificatore di set di dati di alto livello scelto durante l'installazione di IBM MQ.

g) Impostare il percorso della libreria nativa in modo che punti all'installazione di IBM per z/OS .

Questa operazione deve essere eseguita nel JCL utilizzato per avviare Kafka Connect oppure nella sessione z/OS UNIX System Services . Ad esempio:

```
export LIBPATH=USS_DIR/java/lib
```

h) Imposta il percorso della classe per i connettori.

Per ulteriori informazioni, consultare “Utilizzo dei connettori” a pagina 215.

- Configurare i connettori.

  I connettori devono essere configurati prima di essere utilizzati.

  a) Se si utilizza il connettore sink, copiare `mq-sink.properties`, per la modalità stand alone, o `mq-sink.json`, per la modalità distribuita, da *USS_ROOT*`/kafka-connect/sink` a `WORK_DIR`.

  b) Se si utilizza il connettore sorgente, copiare `mq-source.properties`, per la modalità stand alone, o `mq-source.json`, per la modalità distribuita, da *USS_ROOT*`/kafka-connect/sink` a `WORK_DIR`.

  c) Configurare la copia delle proprietà o del file JSON seguendo le istruzioni riportate all'indirizzo https://github.com/ibm-messaging/kafka-connect-mq-source/blob/main/README.md, per il connettore di origine, oppure https://github.com/ibm-messaging/kafka-connect-mq-sink/blob/main/README.md per il connettore sink.

  Assicurarsi che **mq.connection.mode** sia impostato su bindings.

- Avviare Kafka Connect in modalità standalone.

  a) Accedere alla directory USS_ROOT`/kafka-connect/kafka-connect` .

  b) Eseguite lo script connect-standalone.sh, passando il file `connect-standalone.properties` modificato e `mq-sink.properties` o `mq-source.properties` da `WORK_DIR`.

  Ad esempio:

  ```
  cd USS_ROOT/kafka-connect/kafka-connect
  ./bin/connect-standalone.sh WORK_DIR/connect-standalone.properties WORK_DIR/mq-
  source.properties
  ```

- Avviare Kafka Connect in modalità distribuita.

  a) Accedere alla directory USS_ROOT`/kafka-connect/kafka-connect` .

  b) Eseguite lo script `connect-distributed.sh` , passando il file `connect-distributed.properties` modificato da `WORK_DIR`. A differenza della modalità standalone, le proprietà di IBM MQ non vengono passate all'avvio.

  Ad esempio:

  ```
  cd USS_ROOT/kafka-connect/kafka-connect
  ./bin/connect-distributed.sh WORK_DIR/connect-distributed.properties
  ```

  c) Avviare un connettore individuale utilizzando l'API REST di Kafka Connect (https://kafka.apache.org/39/documentation/#connect_rest).

  Ad esempio, per avviare un connettore sorgente:

```
curl -X POST http://localhost:8083/connectors -H "Content-Type: application/json" -d
@WORK_DIR/mq-source.json
```

Informazioni particolari

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti.

IBM potrebbe non offrire i prodotti, i servizi o le funzioni descritti in questo documento in altri paesi. Consultare il rappresentante IBM locale per informazioni sui prodotti e sui servizi disponibili nel proprio paese. Ogni riferimento relativo a prodotti, programmi o servizi IBM non implica che solo quei prodotti, programmi o servizi IBM possano essere utilizzati. In sostituzione a quelli forniti da IBM possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino la violazione dei diritti di proprietà intellettuale o di altri diritti dell'IBM. Tuttavia, è responsabilità dell'utente valutare e verificare il funzionamento di qualsiasi prodotto, programma o servizio non IBM.

IBM potrebbe disporre di applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La fornitura di tale documento non concede alcuna licenza a tali brevetti. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Per richieste di licenze relative ad informazioni double-byte (DBCS), contattare il Dipartimento di Proprietà Intellettuale IBM nel proprio paese o inviare richieste per iscritto a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Il seguente paragrafo non si applica al Regno Unito o a qualunque altro paese in cui tali dichiarazioni sono incompatibili con le norme locali: INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE LA PRESENTE PUBBLICAZIONE "NELLO STATO IN CUI SI TROVA" SENZA GARANZIE DI ALCUN TIPO, ESPRESSE O IMPLICITE, IVI INCLUSE, A TITOLO DI ESEMPIO, GARANZIE IMPLICITE DI NON VIOLAZIONE, DI COMMERCIABILITÀ E DI IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni; quindi la presente dichiarazione potrebbe non essere applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate su base periodica; tali modifiche vengono incorporate nelle nuove edizioni della pubblicazione. IBM si riserva il diritto di apportare miglioramenti o modifiche al prodotto/i e/o al programma/i descritti nella pubblicazione in qualsiasi momento e senza preavviso.

Tutti i riferimenti a siti Web non dell'IBM contenuti in questo documento sono forniti solo per consultazione e non rappresenta in alcun modo un'approvazione di tali siti. I materiali reperibili in tali siti Web non fanno parte dei materiali relativi a questo prodotto IBM e l'utilizzo di tali siti è responsabilità dell'utente.

Tutti i commenti e i suggerimenti inviati potranno essere utilizzati liberamente da IBM e diventeranno esclusiva della stessa.

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a:

IBM Corporation
Coordinatore interoperabilità software, Dipartimento 49XA
Autostrada 3605 52 N

© Copyright IBM Corp. 2007, 2025

Rochester, MN 55901
U.S.A.

Queste informazioni possono essere rese disponibili secondo condizioni contrattuali appropriate, compreso, in alcuni casi, il pagamento di un addebito.

Il programma su licenza descritto in queste informazioni e tutto il materiale su licenza disponibile per esso sono forniti da IBM in base ai termini dell' IBM Customer Agreement, IBM International Program License Agreement o qualsiasi altro accordo equivalente tra le parti.

Tutti i dati relativi alle prestazioni contenuti in questo documento sono stati determinati in un ambiente controllato. Pertanto, i risultati ottenuti in altri ambienti operativi possono variare in modo significativo. Alcune misurazioni potrebbero essere state fatte su sistemi a livello di sviluppo e non vi è alcuna garanzia che queste misurazioni saranno le stesse sui sistemi generalmente disponibili. Inoltre, alcune misurazioni potrebbero essere state stimate mediante estrapolazione. I risultati quindi possono variare. Gli utenti di questo documento dovrebbero verificare i dati applicabili per il loro ambiente specifico.

Le informazioni relative a prodotti non IBM provengono dai fornitori di tali prodotti, dagli annunci pubblicati o da altre fonti pubblicamente disponibili. IBM non ha verificato tali prodotti e, pertanto, non può garantirne l'accuratezza delle prestazioni. Eventuali commenti relativi alle prestazioni dei prodotti non IBM devono essere indirizzati ai fornitori di tali prodotti.

Tutte le dichiarazioni riguardanti la direzione o l'intento futuro di IBM sono soggette a modifica o ritiro senza preavviso e rappresentano solo scopi e obiettivi.

Questa pubblicazione contiene esempi di dati e prospetti utilizzati quotidianamente nelle operazioni aziendali, Per poterli illustrare nel modo più completo possibile, gli esempi riportano nomi di persone, società, marchi e prodotti. Tutti questi nomi sono fittizi e qualsiasi somiglianza con nomi ed indirizzi adoperati da imprese realmente esistenti sono una mera coincidenza.

LICENZA SUL COPYRIGHT:

Queste informazioni contengono programmi applicativi di esempio in lingua originale, che illustrano le tecniche di programmazione su diverse piattaforme operative. È possibile copiare, modificare e distribuire questi programmi di esempio sotto qualsiasi forma senza alcun pagamento alla IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire i programmi applicativi in conformità alle API (application programming interface) a seconda della piattaforma operativa per cui i programmi di esempio sono stati scritti. Questi esempi non sono stati testati approfonditamente tenendo conto di tutte le condizioni possibili. IBM, quindi, non può garantire o sottintendere l'affidabilità, l'utilità o il funzionamento di questi programmi.

Se si sta visualizzando queste informazioni in formato elettronico, le fotografie e le illustrazioni a colori potrebbero non apparire.

Informazioni sull'interfaccia di programmazione

Le informazioni sull'interfaccia di programmazione, se fornite, consentono di creare software applicativo da utilizzare con questo programma.

Questo manuale contiene informazioni sulle interfacce di programmazione che consentono al cliente di scrivere programmi per ottenere i servizi di IBM MQ.

Queste informazioni, tuttavia, possono contenere diagnosi, modifica e regolazione delle informazioni. La diagnosi, la modifica e la regolazione delle informazioni vengono fornite per consentire il debug del software applicativo.

Importante: Non utilizzare queste informazioni di diagnosi, modifica e ottimizzazione come interfaccia di programmazione poiché sono soggette a modifica.

Marchi

IBM, il logo IBM , ibm.com, sono marchi di IBM Corporation, registrati in molte giurisdizioni nel mondo. Un elenco aggiornato dei marchi IBM è disponibile sul web in "Copyright and trademark

information"www.ibm.com/legal/copytrade.shtml. Altri nomi di prodotti e servizi potrebbero essere marchi di IBM o altre società.

Microsoft e Windows sono marchi di Microsoft Corporation negli Stati Uniti, in altri paesi o entrambi.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e/o in altri paesi.

Linux è un marchi registrato di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Questo prodotto include il software sviluppato da Eclipse Project (https://www.eclipse.org/).

Java e tutti i marchi e i logo Java sono marchi registrati di Oracle e/o di società affiliate.

Numero parte:

(1P) P/N: