9.2

Planung für IBM MQ

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen” auf Seite 227 gelesen werden.

Diese Ausgabe bezieht sich auf Version 9 Release 2 von IBM® MQ und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Wenn Sie Informationen an IBMsenden, erteilen Sie IBM ein nicht ausschließliches Recht, die Informationen in beliebiger Weise zu verwenden oder zu verteilen, ohne dass eine Verpflichtung für Sie entsteht.

Inhaltsverzeichnis

IBM MQ-Architektur planen

Beachten Sie bei der Planung einer IBM MQ-Umgebung die Unterstützung, die IBM MQ für Architekturen mit einzelnen oder mehreren Warteschlangenmanagern sowie für Punkt-zu-Punkt- und Publish/Subscribe-Messaging bereitstellt. Planen Sie auch den Ressourcenbedarf und die Nutzung von Protokollierungs- und Sicherheitsfunktionen.

Informationen zu diesem Vorgang

Bevor Sie mit der Planung einer IBM MQ-Architektur beginnen, sollten Sie sich mit den grundlegenden IBM MQ-Konzepten vertraut machen. Siehe IBM MQ Technische Übersicht.

IBM MQ-Architekturen reichen von einfachen Architekturen mit einem einzigen Warteschlangenmanager bis hin zu komplexeren Netzen miteinander verbundener Warteschlangenmanager. Mehrere Warteschlangenmanager werden unter Verwendung von verteilten Warteschlangenverfahren miteinander verbunden. Weitere Informationen zum Planen eines einzelnen Warteschlangenmanagers und mehrerer WS-Manager-Architekturen finden Sie in den folgenden Themen:

- „Architekturen auf der Basis eines einzelnen Warteschlangenmanagers” auf Seite 19
- „Architekturen auf der Basis von mehreren Warteschlangenmanagern” auf Seite 20
  - „Verteilte Warteschlangen und Cluster planen” auf Seite 21
  - „Verteiltes Publish/Subscribe-Netz planen” auf Seite 79

z/OS Unter IBM MQ for z/OS können Sie mit gemeinsam genutzten Warteschlangen und Gruppen mit gemeinsamer Warteschlange die Implementierung des Lastausgleichs aktivieren und festlegen, dass Ihre IBM MQ-Anwendungen skalierbar und hoch verfügbar sind. Informationen zu gemeinsam genutzten Warteschlangen und Gruppen mit gemeinsamer Warteschlange finden Sie unter Gemeinsam genutzte Warteschlangen und Gruppen mit gemeinsamer Warteschlange.

IBM MQ stellt zwei verschiedene Release-Modelle bereit:

- Das Long Term Support-Release (LTS) ist am besten für Systeme geeignet, die eine langfristige Implementierung und maximale Stabilität erfordern.
- Das Continuous Delivery-Release (CD) ist für Systeme vorgesehen, die die neuesten funktionalen Erweiterungen für IBM MQ schnell nutzen müssen.

Beide Releasetypen werden auf die gleiche Weise installiert, aber es gibt Überlegungen in Bezug auf die Unterstützung und Migration, die Sie verstehen müssen. Weitere Informationen finden Sie unter IBM MQ -Releasetypen und -Versionssteuerung .

Weitere Informationen zur Planung für mehrere Installationen, Speicher-und Leistungsanforderungen sowie die Verwendung von Clients finden Sie in den anderen Unterabschnitten.

Zugehörige Konzepte

„IBM MQ-Umgebung unter z/OS planen” auf Seite 157
Bei der Planung einer IBM MQ-Umgebung müssen Sie den Ressourcenbedarf für Datasets, Seitengruppen, Db2 und Coupling-Facilitys sowie den Bedarf an Protokollierungs- und Sicherungsfunktionen berücksichtigen. Die Informationen in diesem Thema helfen Ihnen, eine IBM MQ-Umgebung zu planen.

Sicherstellen, dass Nachrichten nicht verloren gehen (Protokollierung)

Verfügbarkeit, Wiederherstellung und Neustart

Zugehörige Tasks

Überprüfen der Anforderungen

IBM MQ -Releasetypen: Überlegungen zur Planung

Ab IBM MQ 9.0 gibt es zwei Haupttypen von Releases: ein Long Term Support -Release (LTS) und ein Continuous Delivery -Release (CD). Für jede unterstützte Plattform wirkt sich der von Ihnen ausgewählte Releasetyp auf Bestellung, Installation, Wartung und Migration aus.

Ausführliche Informationen zu den Releasetypen finden Sie unter IBM MQ -Releasetypen und -Versionssteuerung.

Hinweise zu IBM MQ for Multiplatforms

Bestellung

In Passport Advantage gibt es zwei separate eAssemblies für IBM MQ 9.2. Die eine enthält Installationsimages für IBM MQ 9.2.0 als Long Term Support-Release und die andere enthält Installationsimages für IBM MQ 9.2.x als Continuous Delivery-Release. Laden Sie die Installationsimages von der eAssembly gemäß Ihrer Wahl des Release herunter.

Alle IBM MQ-Versionen gehören zu derselben Produkt-ID; bei IBM MQ 9.2 gilt dies sowohl für die LTS-Releases als auch für die CD-Releases.

Die Berechtigung zur Verwendung von IBM MQ gilt für das gesamte Produkt (PID), und unterliegt lediglich den Einschränkungen der lizenzierten Komponenten und der Preismetriken. Dies bedeutet, dass Sie frei zwischen LTS -Release und CD -Release-Installationsimages für IBM MQ 9.2wählen können.

Installation

Nachdem Sie ein Installationsimage von Passport Advantageheruntergeladen haben, sollten Sie nur die Komponenten für die Installation auswählen, für die Sie eine Berechtigung erworben haben. Weitere Informationen dazu, welche installierbaren Komponenten in den einzelnen gebührenpflichtigen Komponenten enthalten sind, finden Sie unter IBM MQ-Lizenzinformationen.

Sie können IBM MQ 9.2.0 LTS -Release und IBM MQ 9.2.x CD -Release in demselben Betriebssystemimage installieren. Wenn Sie dies tun, werden die Komponenten als unterschiedliche Installationen angezeigt, was durch die Unterstützung mehrerer Versionen von IBM MQ ermöglicht wird. Jede Version verfügt über unterschiedliche Gruppen von Warteschlangenmanagern, die dieser Version zugeordnet sind.

Jedes neue CD-Release wird als separates Installationsimage bereitgestellt. Das neue Release von CD kann zusammen mit einem vorhandenen Release installiert werden oder ein früheres CD -Release kann vom Installationsprogramm auf das neue Release aktualisiert werden.

CD -Releases enthalten funktionale Erweiterungen sowie die neuesten Fehlerkorrekturen und Sicherheitsupdates. Jedes CD -Release ist kumulativ und ersetzt vollständig alle vorherigen für diese Version von IBM MQ. Sie können also ein bestimmtes CD -Release überspringen, wenn es keine Funktion enthält, die für Ihr Unternehmen relevant ist.

Wartung

Das Release LTS wird von der Anwendung von Fixpacks, die Fehlerkorrekturen bereitstellen,und kumulativen Sicherheitsupdates (CSUs), die Sicherheitspatches bereitstellen, gewartet. Die Fixpacks und CSUs werden regelmäßig verfügbar gemacht und sind kumulativ.

Für CDwerden CSUs nur für das neueste CD -Release erstellt, das möglicherweise in einer nachfolgenden Version vorliegt.

Möglicherweise werden Sie gelegentlich vom IBM Support-Team angewiesen, einen vorläufigen Fix anzuwenden. Vorläufige Fixes werden auch als provisorische Fixes oder Testfixes bezeichnet und verwendet, um dringende Updates anzuwenden, die nicht auf die nächste Wartungsbereitstellung warten können.

Migration zwischen LTS-Release und CD-Release

Es gibt Einschränkungen und Grenzen, aber im Allgemeinen kann ein einzelner Warteschlangenmanager von der Verwendung des LTS-Release-Codes auf den CD-Release-Code oder von der Verwendung des

CD-Release-Codes auf den LTS-Release-Code migriert werden, sofern das Ziel-Release höher ist, als das vor der Migration verwendete.

Es sind zwei Ansätze möglich:

- Installieren Sie den neuen Releasecode anstelle einer vorhandenen Installation von IBM MQ, damit diese aktualisiert wird. Alle Warteschlangenmanager, die der Installation zugeordnet sind, verwenden das neue Release von Code, wenn sie gestartet werden.
- Installieren Sie das neue Release von Code als neue Installation, und verschieben Sie dann mit dem Befehl setmqm einzelne WS-Manager-Instanzen in die neue Installation.

Wenn ein Warteschlangenmanager mit der Ausführung eines CD -Release von Code startet, wird die Befehlsebene des Warteschlangenmanagers aktualisiert, um den neuen Release-Level anzugeben. Dies bedeutet, dass alle im Release bereitgestellten neuen Funktionen aktiviert sind und Sie den Warteschlangenmanager nicht mehr mit einem Code-Release mit einer niedrigeren VRM -Nummer erneut starten können.

Hinweise zu IBM MQ for z/OS

z/OS

Bestellung

Bei der Bestellung von IBM MQ for z/OS 9.2 werden in ShopZ zwei verschiedene Funktionen angeboten. Die beiden Funktionen entsprechen dem LTS-Release und dem CD-Release. Beide Funktionen sind auf dieselbe Produkt-ID (PID) anwendbar. Es handelt sich um die Produkt-ID, die lizenziert ist. Wenn eine Komponente lizenziert ist, besteht die Berechtigung, bei Bedarf die Alternativfunktion zu verwenden. Bei der Bestellung wählen Sie das Feature aus, das dem Release LTS oder dem Release CD entspricht.

Wenn Sie Produkte für die Aufnahme in ein ServerPacauswählen, können Sie das LTS -Release und das CD -Release nicht in derselben ServerPac -Reihenfolge auswählen, da die Produkte nicht mit SMP/E in derselben Zielzone installiert werden können.

Installation

LTS-Releases und CD-Releases werden in unterschiedlichen Gruppen von FMIDs bereitgestellt. Beachten Sie, dass diese FMIDs nicht in derselben SMP/E-Zielzone installiert werden können. Gehen Sie wie folgt vor, wenn Sie sowohl das Release LTS als auch das Release CD benötigen:

- Das LTS-Release und das CD-Release in verschiedenen Zielzonen installieren
- Separater Ziel-und Verteilungsbibliotheken für die beiden Releases verwalten

Wenn sich Ihr Warteschlangenmanager in einer Gruppe mit gemeinsamer Warteschlange befindet und Sie ein Upgrade auf die neueste CD-Version durchführen, müssen Sie alle Warteschlangenmanager in der Gruppe aktualisieren.

Die Befehlsebene eines Warteschlangenmanagers ist die dreistellige VRM-Ebene. Ein IBM MQ -Programm kann `MQINQ`aufrufen und dabei den Selektor `MQIA_COMMAND_LEVEL` übergeben, um die Befehlsebene des Warteschlangenmanagers abzurufen, mit dem es verbunden ist.

Da die Releases unterschiedliche FMIDs verwenden, können Sie ein CD -Release nicht mit Wartung für ein LTS -Release oder umgekehrt aktualisieren. Ebensowenig ist es möglich, einer Version des Produktcodes vom LTS-Release auf das CD-Release oder umgekehrt umzustellen. Sie können einen Warteschlangenmanager jedoch zwischen den Releasemodellen wechseln. Siehe Migration zwischen LTS-Release und CD-Release.

Anmerkung:

Die Releases IBM MQ 9.0.x und IBM MQ 9.1.x CD hatten separate Versions-und Releaseabhängige FMIDs. Für die Umstellung von 9.0.x CD auf 9.1.x CD ist mindestens eine vollständige SMP/E-Installation erforderlich.

Ab IBM MQ for z/OS 9.2.0verwendet das CD -Release eine Gruppe von FMIDs, die für alle IBM MQ for z/OS -Releases mit der Versionsnummer 9gleich bleiben. Da jede neue Version von IBM MQ sowohl als CD -als auch als LTS -Release verfügbar ist, können Sie ein Upgrade für CD -Releases durchführen,

indem Sie PTFs auf eine einzelne SMP/E-Installation anwenden, auch wenn Sie eine Hauptversionsgrenze überschreiten. Sie können beispielsweise von IBM MQ for z/OS 9.2.0 CDzu IBM MQ for z/OS 9.2.2 CD, zu IBM MQ for z/OS 9.2.4 CDund zu IBM MQ for z/OS 9.3.0 CDwechseln, indem Sie nur PTFs anlegen.

Sie können ein LTS- von einem CD-Release mit demselben VRM-Stand unterscheiden, indem Sie die Nachricht CSQY000I im Jobprotokoll des Warteschlangenmanagers anzeigen.

Wartung

IBM MQ for z/OS verwendet PTFs für die Wartung.

LTS PTFs sind für eine bestimmte Gruppe von Bibliotheken vorgesehen, die einem bestimmten Release entsprechen. Für UNIX System Services-Features (d. h. JMS und Webbenutzerschnittstelle, Connector Pack und Managed File Transfer) sind die z/OS -PTFs direkt an den Multiplatforms-Fixpacks und kumulativen Sicherheitsupdates (CSUs)ausgerichtet. Diese Fixes sind kumulativ und werden gleichzeitig mit dem entsprechenden Multiplatforms-Fixpack oder CSUverfügbar gemacht.

CD CD CSUs werden normalerweise nicht zwischen CD-Releases zur Verfügung gestellt, sind aber im nächsten IBM MQ for z/OS CD -Release enthalten. Sie können sich auch an den Support wenden, um ein + + USERMOD-Modul anzufordern.

Andere Fixes in IBM MQ for z/OS sind unterschiedliche Fixes für bestimmte Teile. Diese Fixes lösen bestimmte Probleme, sind nicht kumulativ und werden verfügbar gemacht, wenn sie erstellt werden.

Migration zwischen LTS-Release und CD-Release

Es gibt Einschränkungen und Grenzen, aber in der Regel kann ein einzelner Warteschlangenmanager von der Verwendung des LTS-Release-Codes auf den CD-Release-Code oder von der Verwendung des CD-Release-Codes auf den LTS-Release-Code migriert werden, sofern das Ziel-Release höher ist, als vor der Migration.

V 9.2.0 V 9.2.0 Ab IBM MQ for z/OS 9.2.0können Sie zwischen CD -und LTS -Releases mit demselben VRM so oft wie nötig hin-und hermigrieren, ohne dass sich dies auf die Rückwärtsmigration auswirkt. Beispielsweise kann ein WS-Manager in IBM MQ for z/OS 9.2.0 LTSgestartet werden, in IBM MQ for z/OS 9.2.0 CDbeendet und gestartet werden, in IBM MQ for z/OS 9.2.0 LTSbeendet und gestartet werden.

IBM MQ for z/OS hat traditionell eine Rückgriffsfunktion (Rückwärtsmigration) bereitgestellt, sodass Sie nach einem Zeitraum nach einer Migration auf das vorherige Release zurückgreifen können.

V 9.2.0 V 9.2.0 Diese Fähigkeit wird für LTS-Releases und die CD-Releases mit dem Modifikator 0, wie z. B. 9.2.0 CD, beibehalten, dies ist jedoch nicht möglich, wenn die Quelle oder das Ziel einer Migration ein CD-Release mit einer Modifikatornummer ungleich null ist, z. B. 9.1.5 oder 9.2.1.

Im Folgenden finden Sie gültige Migrationsszenarios und veranschaulichen, wie dieses Prinzip funktioniert:

Quellenrelease	Zielrelease	Anmerkungen
8.0.0 LTS	9.2.0 LTS oder 9.2.0 CD	Die Rückwärtsmigration wird nicht unterstützt, da es für die Version 8.0.0 LTS keine Standardunterstützung mehr gibt.
9.0.0 LTS	9.2.0 LTS oder 9.2.0 CD	Die Rückwärtsmigration wird unterstützt.
9.1.0 LTS	9.2.0 LTS oder 9.2.0 CD	Die Rückwärtsmigration wird unterstützt.

Quellenrelease	Zielrelease	Anmerkungen
9.1.5 CD	9.2.0 LTS oder 9.2.0 CD	Eine Rückwärtsmigration wird nicht unterstützt, da das Quellenrelease ein CD-Release mit einem Modifikator ungleich null ist.
V 9.2.0 9.2.0 LTS oder V 9.2.0 9.2.0 CD	9.2.1 CD	Eine Rückwärtsmigration wird nicht unterstützt, da das Zielrelease ein CD-Release mit einem Modifikator ungleich null ist. `Write to operator with reply` CSQY041D wird ausgegeben, um die Migration zu bestätigen.

Zugehörige Tasks
Wartung unter z/OS anwenden und entfernen
Zugehörige Informationen
Download von IBM MQ 9.2

IBM MQ und IBM MQ Appliance lokal - Überlegungen zur DSGVO-Umsetzung

Für folgende Produkt-IDs:

- 5724-H72 IBM MQ
- 5655-AV9 IBM MQ Advanced for z/OS
- 5655-AV1 IBM MQ Advanced for z/OS Value Unit Edition
- 5655-AM9 IBM MQ Advanced Message Security for z/OS
- 5725-Z09 IBM MQ Appliance M2001
- 5737-H47 IBM MQ Appliance M2002
- 5655-MQ9 IBM MQ for z/OS
- 5655-VU9 IBM MQ for z/OS Value Unit Edition
- 5655-MF9 IBM MQ Managed File Transfer for z/OS
- 5655-ADV IBM WebSphere MQ Advanced for z/OS
- 5655-AMS IBM WebSphere MQ Advanced Message Security for z/OS
- 5724-A39 IBM WebSphere MQ for HP NonStop Server
- 5655-W97 IBM WebSphere MQ for z/OS
- 5655-VU8 IBM WebSphere MQ for z/OS Value Unit Edition
- 5655-VUE IBM WebSphere MQ for z/OS Value Unit Edition
- 5655-MFT IBM WebSphere MQ Managed File Transfer for z/OS

Hinweis:

Dieses Dokument soll Ihnen bei den Vorbereitungen für die Umsetzung der EU-Datenschutz-Grundverordnung (DSGVO) helfen. Es enthält Informationen zu den Features von IBM MQ, die Sie konfigurieren können, sowie Aspekte der Verwendung des Produkts, die Sie in Betracht ziehen sollten, um die Umsetzung der DSGVO in Ihrer Organisation zu fördern. Diese Informationen sind keine erschöpfende Liste, da die Kunden viele Möglichkeiten haben, Funktionen auszuwählen und zu konfigurieren, und die große Vielfalt

an Möglichkeiten, die das Produkt in sich selbst und mit Anwendungen und Systemen anderer Hersteller verwendet werden kann.

Es liegt allein in der Verantwortung der Kunden, die Einhaltung der verschiedenen Gesetze und Verordnungen sicherzustellen, z. B. der DSGVO. Es obliegt allein den Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Auslegung aller relevanten Gesetze und Vorschriften beraten zu lassen, die ihre Geschäftstätigkeit und die von ihnen eventuell einzuleitenden Maßnahmen zur Einhaltung dieser Gesetze und Vorschriften betreffen.

Die hier beschriebenen Produkte, Services und anderen Funktionen sind nicht für alle Kundensituationen geeignet und können eine eingeschränkte Verfügbarkeit haben. IBM gibt keine Rechts-, Buchhaltungs- oder Wirtschaftsprüfungsberatung und übernimmt keine Verantwortung bzw. bietet keine Gewährleistung, dass seine Services und Produkte die Einhaltung von Gesetzen oder Verordnungen durch den Kunden sicherstellen.

Inhaltsverzeichnis

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) wurde von der Europäischen Union ("EU") verabschiedet und gilt seit dem 25. Mai 2018.

Warum ist die DSGVO wichtig?

Mit der DSGVO wird ein strengerer datenschutzrechtlicher Rahmen für die Verarbeitung personenbezogener Daten geschaffen. Folgende Änderungen sieht die DSGVO vor:

- Neue und erweiterte Rechte für Einzelpersonen
- Eine erweiterte Definition von personenbezogenen Daten
- Neue Verpflichtungen für "Auftragsverarbeiter"
- Potenzielle finanzielle Sanktionen bei Nichtkonformität
- Zwingende Meldepflicht bei Datenschutzverletzungen

Weitere Informationen zur DSGVO finden Sie hier:

- Informationsportal zur EU-Datenschutz-Grundverordnung
- ibm.com/GDPR-Website

Produktkonfiguration -Überlegungen zur DSGVO-Bereitschaft

In den folgenden Abschnitten finden Sie Hinweise zur Konfiguration von IBM MQ, um Ihre Organisation bei der Umsetzung der DSGVO zu unterstützen.

Datenlebenszyklus

IBM MQ ist ein auf dem transaktionsorientierten Nachrichtenaustausch basierendes Middlewareprodukt, das Anwendungen den asynchronen Austausch von Daten ermöglicht, die von Anwendungen bereitgestellt werden. IBM MQ unterstützt eine Reihe von Messaging-APIs, -Protokollen und -Bridges, um Verbindungen zwischen den Anwendungen zu ermöglichen. Daher kann IBM MQ zum Austausch vielfältiger Formen von Daten verwendet werden, die potenziell der DSGVO unterliegen können. Es gibt auch verschiedene Produkte von Drittanbietern, mit denen IBM MQ Daten austauschen kann. Einige dieser Produkte gehören IBM, doch viele andere Produkte werden von anderen Technologieunternehmen bereitgestellt. Auf der Website Software Product Compatibility Reports sind Listen der zugehörigen Software aufgeführt. Für Überlegungen zur DSGVO-Bereitschaft eines Fremdprodukts sollten Sie die Produktdokumentation zu Rate ziehen. IBM MQ-Administratoren steuern über die Definition von Warteschlangen, Themen und Subskriptionen die Art und Weise, in der IBM MQ mit den Daten interagiert, die das Programm durchlaufen.

Welche Datentypen durchlaufen IBM MQ?

Da IBM MQ Messaging-Services für die asynchrone Übertragung von Anwendungsdaten bereitstellt, gibt es keine definitive Antwort auf diese Farge, weil die Anwendungsfälle von den jeweils bereitgestellten Anwendungen abhängt. Anwendungsnachrichtendaten werden in Warteschlangendateien (Seitengruppen oder Coupling-Facility unter z/OS), Protokollen und Archiven gespeichert, und die Nachricht selbst kann Daten enthalten, die von GDPR gesteuert werden. Die von den Anwendungen bereitgestellten Nachrichtendaten können auch in Dateien enthalten sein, die zu Fehlerbestimmungszwecken erfasst werden, wie z. B. Fehlerprotokolle, Tracedateien und FFSTs. Unter z/OS können die von den Anwendungen bereitgestellten Nachrichtendaten auch in Speicherauszügen des Adressraums oder der Coupling-Facility enthalten sein.

Es folgen einige typische Beispiele für personenbezogene Daten, die mithilfe von IBM MQ zwischen Anwendungen ausgetauscht werden können:

- Personenbezogene Daten der Mitarbeiter des IBM Kunden (z. B. wenn mit IBM MQ eine Verbindung zum Lohnbuchhaltungs- oder Personalabteilungssystem des IBM Kunden hergestellt wird)
- Personenbezogene Daten der Kunden des IBM Kunden (z. B. wenn ein IBM Kunde die Daten seiner eigenen Kunden mit IBM MQ zwischen Anwendungen austauscht, wie z. B. Anfragen von Kaufinteressenten und die im CRM-System gespeicherten Kundendaten)
- Sensible personenbezogene Daten der Kunden des IBM Kunden (z. B. wenn IBM MQ in branchenspezifischen Kontexten eingesetzt wird, in denen spezielle personenbezogene Daten ausgetauscht werden müssen, wie z. B. beim Austausch von Patientenakten nach dem HL7-Protokoll zwischen medizintechnischen Anwendungen.

Zusätzlich zu den von Anwendungen bereitgestellten Nachrichtendaten verarbeitet IBM MQ auch folgende Datentypen:

- Authentifizierungsnachweise (z. B. Benutzername und Kennwort, API-Schlüssel usw.)
- Technisch identifizierbare personenbezogen Daten (z. B. Einheiten-IDs, Nutzungskennungen, IP-Adresse usw. bei Verknüpfung mit einer Einzelperson)

Personenbezogene Daten, die für den Onlinekontakt mit IBM verwendet werden

IBM MQ Kunden können Kommentare/Feedback/Anfragen online einreichen, um IBM über IBM MQ Themen auf verschiedene Arten zu kontaktieren, in erster Linie:

- Öffentlicher Kommentarbereich auf Seiten im IBM MQ-Bereich auf IBM Developer
- Bereich der öffentlichen Kommentare auf Seiten von IBM MQ-Produktinformationen in IBM Documentation
- Öffentliche Kommentare in den IBM Unterstützungsforen
- Öffentliche Kommentare in IBM-Integrationsideen

In der Regel werden nur der Name und die E-Mail-Adresse des Kunden verwendet, um persönliche Antworten für den Betreff des Kontakts zu ermöglichen, und die Verwendung personenbezogener Daten entspricht der IBM Online-Datenschutzerklärung.

Datenerfassung

IBM MQ kann zum erfassen von personenbezogenen Daten verwendet werden. Wenn Sie Ihre Verwendung von IBM MQ sowie Ihren Maßnahmenbedarf zur Einhaltung der DSGVO-Bestimmungen überprüfen, sollten Sie die Arten personenbezogener Daten berücksichtigen, die in Ihrem Fall IBM MQ durchlaufen. Sie können z. B. Aspekte wie die folgenden berücksichtigen:

- Wie kommen die Daten zu Ihren Warteschlangenmanagern? (Über welche Protokolle? Sind die Daten verschlüsselt? Sind die Daten signiert?)
- Wie werden Daten von Ihren Warteschlangenmanagern gesendet? (Über welche Protokolle? Sind die Daten verschlüsselt? Sind die Daten signiert?)
- Wie werden Daten beim Durchlaufen eines Warteschlangenmanagers gespeichert? (Jede Messaging-Anwendung hat das Potenzial, Nachrichtendaten in statusabhängige Medien zu schreiben, selbst wenn eine Nachricht nicht persistent ist. Sind Sie sich bewusst, wie die Messaging-Funktionen Aspekte der Anwendungsnachrichtendaten, die das Produkt passieren, zugänglich machen könnten?)
- Wie werden die Berechtigungsnachweise erfasst und ggf. gespeichert, wenn sie von IBM MQ für den Zugriff auf Drittanbieteranwendungen benötigt werden?

IBM MQ muss möglicherweise mit anderen Systemen und Services kommunizieren, für die eine Authentifizierung erforderlich ist, z. B. LDAP. Bei Bedarf werden Authentifizierungsdaten (Benutzer-IDs, Kennwörter) konfiguriert und von IBM MQ für die Verwendung in dieser Kommunikation gespeichert. Wenn möglich, sollten Sie die Verwendung persönlicher Berechtigungsnachweise für die IBM MQ-Authentifizierung vermeiden. Berücksichtigen Sie den Schutz des Speichers, der für Authentifizierungsdaten verwendet wird. (Siehe Datenspeicherung weiter unten.)

Datenspeicherung

Wenn Nachrichtendaten über Warteschlangenmanager übertragen werden, wird IBM MQ die Daten (und möglicherweise mehrere Kopien davon) direkt dauerhaft auf statusabhängige Datenträger speichern. IBM MQ-Benutzer sollten die Nachrichtendaten lieber sichern, während sie sich in Ruhe befinden.

In den folgenden Punkten werden Bereiche hervorgehoben, in denen IBM MQ die von Anwendungen bereitgestellten Daten dauerhaft speichert und die deshalb bei Überlegungen zur Einhaltung der DSGVO-Bestimmungen von den Benutzern sorgfältig bedacht werden sollten.

- Anwendungsnachrichtenwarteschlangen:

  IBM MQ stellt Nachrichtenwarteschlangen bereit, um den asynchronen Datenaustausch zwischen Anwendungen zu ermöglichen. Nicht persistente und persistente Nachrichten, die in einer Warteschlange gespeichert sind, werden in statusabhängige Datenträger geschrieben.
- Dateiübertragungsagentenwarteschlangen:

  Um die zuverlässige Übertragung von Dateidaten zu koordinieren, verwendet IBM MQ Managed File Transfer Nachrichtenwarteschlangen, in denen Dateien, die personenbezogene Daten enthalten, und Datensätze von Übertragungen gespeichert sind.
- Übertragungswarteschlangen:

  Damit Nachrichten zuverlässig zwischen Warteschlangenmanagern übertragen werden können, werden Nachrichten temporär in Übertragungswarteschlangen gespeichert.
- Warteschlangen für nicht zustellbare Nachrichten:

  Es gibt Situationen, in denen Nachrichten nicht in eine Zielwarteschlange gestellt werden können und in einer Warteschlange für dead-Mail gespeichert werden, wenn eine solche Warteschlange auf dem Warteschlangenmanager konfiguriert ist.
- Rücksetzwarteschlangen:

  JMS-und XMS-Messaging-Schnittstellen bieten die Möglichkeit, falsch formatierte Nachrichten nach einer Reihe von Rücksetzungen in eine Rücksetzwarteschlange zu verschieben, damit andere gültige Nachrichten verarbeitet werden können.
- AMS-Fehlerwarteschlange:

IBM MQ Advanced Message Security verschiebt Nachrichten, die einer Sicherheitsrichtlinie nicht entsprechen, in SYSTEM.PROTECTION.ERROR.QUEUE Fehlerwarteschlange auf ähnliche Weise wie die Warteschlange für nicht zustellbare Nachrichten.

- Ständige Veröffentlichungen:

  IBM MQ stellt eine Funktion für ständige Veröffentlichungen bereit, mit subskribierende Anwendungen vorherige Veröffentlichungen erneut abrufen können.

- Verzögerte Zustellung:

  IBM MQ unterstützt das die Funktion der Zustellungsverzögerung von JMS 2.0, mit dem Nachrichten zu einem späteren Zeitpunkt an ihr Ziel zugestellt werden können. Nachrichten, die noch nicht zugestellt wurden, werden in der Warteschlange SYSTEM.DDELAY.LOCAL.QUEUE gespeichert.

Weitere Informationen finden Sie hier:

- Protokollierung: Stellen Sie sicher, dass die Nachrichten nicht verloren gehen.
- MFT Agent-Warteschlangeneinstellungen
- Verwenden der Warteschlange für dead-Mail
- Behandlung von Giftnachrichten in IBM MQ-Klassen für JMS
- AMS-Fehlerbehandlung
- Zurückgehaltene Veröffentlichungen
- JMS 2.0 Zustellungsverzögerung

In den folgenden Punkten werden Bereiche hervorgehoben, in denen IBM MQ die von Anwendungen bereitgestellten Daten eventuell indirekt dauerhaft speichert und die deshalb bei Überlegungen zur Einhaltung der DSGVO-Bestimmungen von den Benutzern ebenfalls sorgfältig bedacht werden sollten.

- Trace-Route-Messaging:

  IBM MQ stellt Trace-Route-Funktionen zur Aufzeichnung der Route bereit, die eine Nachricht zwischen den Anwendungen durchläuft. Die generierten Ereignisnachrichten können technisch identifizierbare personenbezogene Daten, wie z. B. IP-Adressen, enthalten.

- Anwendungsaktivitätstrace:

  IBM MQstellt einen Anwendungsaktivitätstrace bereit, der die Messaging-API-Aktivitäten von Anwendungen und Kanälen aufzeichnet. Der Anwendungsaktivitätstrace kann den Inhalt der von Anwendungen bereitgestellten Nachrichtendaten in Ereignisnachrichten speichern.

- Service-Trace:

  IBM MQ stellt Service-Tracefunktionen bereit, mit denen die internen Codepfade aufgezeichnet werden, die die Nachrichtendatenflüsse durchlaufen. Im Rahmen dieser Funktionen kann IBM MQ den Inhalt der von Anwendungen bereitgestellten Nachrichtendaten in Tracedateien auf einem Datenträger speichern.

- Warteschlangenmanagerereignisse:

  IBM MQ kann Ereignisnachrichten generieren, die personenbezogene Daten enthalten können, z. B. Berechtigungs-, Befehls- und Konfigurationsereignisse.

Weitere Informationen finden Sie hier:

- Trace-Route-Messaging
- Trace verwenden
- Ereignisüberwachung
- WS-Manager-Ereignisse

Wenn Sie den Zugriff auf Kopien der von den Anwendungen bereitgestellten Nachrichtendaten schützen möchten, können Sie die folgende Aktionen in Betracht ziehen:

- Beschränken Sie den Zugriff privilegierter Benutzer auf IBM MQ-Daten im Dateisystem, z. B. indem Sie auf UNIX and Linux®-Plattformen die Benutzerzugehörigkeit zur Gruppe 'mqm' beschränken.

- Beschränken Sie den Anwendungszugriff auf IBM MQ-Daten mithilfe von dedizierten Warteschlangen und Zugriffssteuerung. Vermeiden Sie, wenn möglich, eine unnötige gemeinsame Nutzung von Ressourcen, wie z. B. Warteschlangen, durch mehrere Anwendungen und sorgen Sie für eine differenzierte Zugriffssteuerung für Warteschlangen- und Themenressourcen.
- Schränken Sie den Zugriff auf replizierte Kopien von IBM MQ-Daten in Hochverfügbarkeits-(HA-) oder Disaster-Recovery-(DR-)Konfigurationen ein und sichern Sie die für die Replikation verwendeten Verbindungen.
- Verwenden Sie IBM MQ Advanced Message Security für die Bereitstellung einer durchgängigen Signierung und/oder Verschlüsselung der Nachrichtendaten.
- Verwenden Sie die Verschlüsselung auf Datei- oder Datenträgerebene, um den Inhalt des Verzeichnisses zu schützen, in dem die Traceprotokolle gespeichert werden.
- Nachdem Sie einen Service-Trace an IBM hochgeladen haben, können Sie Ihre Service-Tracedateien und FFST-Daten löschen, wenn Sie besorgt sind, dass diese möglicherweise personenbezogene Daten enthalten.

Weitere Informationen finden Sie hier:

- Privilegierte Benutzer
- Unterstützung von Dateisystemen auf Multiplatforms planen

Ein IBM MQ-Administrator kann einen Warteschlangenmanager mit Berechtigungsnachweisen (Benutzername und Kennwort, API-Schlüssel usw.) konfigurieren für 3rd wie LDAP, Salesforceusw. Diese Daten werden in der Regel im Datenverzeichnis des Warteschlangenmanagers gespeichert, das durch Dateisystemberechtigungen geschützt ist.

Beim Erstellen eines IBM MQ-Warteschlangenmanagers wird dessen Datenverzeichnis mit gruppenbasierter Zugriffssteuerung eingerichtet, damit IBM MQ die Konfigurationsdateien lesen und die Berechtigungsnachweise für Verbindungen zu diesen Systemen verwenden kann. Da IBM MQ-Administratoren als privilegierte Benutzer betrachtet werden und Mitglieder dieser Gruppe sind, haben sie Lesezugriff auf diese Dateien. Einige Dateien sind verschleiert, aber sie sind nicht verschlüsselt. Aus diesem Grund sollten Sie die folgenden Aktionen in Betracht ziehen, um den Zugriff auf Berechtigungsnachweise vollständig zu schützen:

- Beschränken Sie den Zugriff privilegierter Benutzer auf IBM MQ-Daten, z. B. indem Sie auf UNIX and Linux-Plattformen die Zugehörigkeit zur Gruppe 'mqm' beschränken.
- Verwenden Sie die Verschlüsselung auf Datei- oder Datenträgerebene, um den Inhalt des Datenverzeichnisses des Warteschlangenmanagers zu schützen.
- Verschlüsseln Sie die Backups des Produktionskonfigurationsverzeichnisses und speichern Sie sie mit entsprechenden Zugriffssteuerungen.
- Sie können Prüfprotokolle für Authentifizierungsfehler, Zugriffssteuerung und Konfigurationsänderungen mit Sicherheits-, Befehls-und Konfigurationsereignissen bereitstellen.

Weitere Informationen finden Sie hier:

- IBM MQ schützen

Datenzugriff

Die folgenden Produktschnittstellen können auf die Daten von IBM MQ-Warteschlangenmanagern zugreifen, wobei einige für den Zugriff über eine ferne Verbindung und andere für den Zugriff über eine lokale Verbindung konfiguriert sind.

- IBM MQ-Konsole [nur fern]
- IBM MQ-Administrative-REST-API [nur fern]
- IBM MQ-Messaging-REST-API [nur fern]
- MQI [Lokal und Fern]
- JMS [Lokal und Fern]

- XMS [Lokal und Fern]
- IBM MQ Telemetry (MQTT) [nur fern]
- IBM MQ Light (AMQP) [Nur Remote]
- IBM MQ IMS-Brücke [nur lokal]
- IBM MQ CICS-Bridge [nur lokal]
- IBM MQ MFT Protokollbridges [nur fern]
- IBM MQ Connect:Direct-Bridges [nur fern]
- IBM MQ Bridge to Salesforce [nur fern]
- IBM MQ Bridge to Blockchain [nur fern]
- IBM MQ MQAI [lokal und fern]
- IBM MQ-PCF-Befehle [lokal und fern]
- IBM MQ-MQSC-Befehle [lokal und fern]
- IBM MQ Explorer [lokal und fern]
- IBM MQ-Benutzerexits [nur lokal]
- IBM MQ Internet Pass-Thru [nur fern]
- Metriken für Red Hat® OpenShift® Monitoring (Prometheus) (die Metriken sind numerische Daten zu Statistiken der Warteschlangenmanager)
- Integration des IBM Cloud Pak for Integration Operations-Dashboard, das übergeordnete Tracedaten an eine zentrale Quelle übergibt (nur CP4I)
- IBM MQ Appliance - serielle Konsole [nur lokal]
- IBM MQ Appliance-SSH [nur fern]
- IBM MQ Appliance-REST-API [nur fern]
- IBM MQ Appliance-Webbenutzerschnittstelle [nur fern]

Die Schnittstellen sind so konzipiert, dass Benutzer Änderungen an einem IBM MQ-Warteschlangenmanager und den darin gespeicherten Nachrichten vornehmen können. Die Verwaltungs- und Messaging-Operationen sind so gesichert, dass es drei Stufen gibt, wenn eine Anforderung gestellt wird.

- Authentifizierung
- Rollenzuordnung
- Autorisierung

Authentifizierung:

Wenn die Nachricht oder die Verwaltungsoperation von einer lokalen Verbindung angefordert wurde, ist die Quelle dieser Verbindung ein laufender Prozess auf demselben System. Der Benutzer, der den Prozess ausführt, muss alle vom Betriebssystem zur Verfügung gestellten Authentifizierungsschritte durchlaufen haben. Der Benutzername des Eigners des Prozesses, von dem aus die Verbindung hergestellt wurde, wird als Identität bestätigt. Dies könnte z. B. der Name des Benutzers sein, der die Shell ausführt, von der eine Anwendung gestartet wurde. Die möglichen Formen der Authentifizierung für lokale Verbindungen sind:

1. Bestätigter Benutzername (lokales Betriebssystem)
2. Optionaler Benutzername und Kennwort (OS, LDAP oder benutzerdefinierte Repositorys von Drittanbietern)

Wenn die Verwaltungsaktion von einer fernen Verbindung angefordert wurde, wird die Kommunikation mit IBM MQ über eine Netzschnittstelle ausgeführt. Die folgenden Formen der Identität können für die Authentifizierung über Netzwerkverbindungen dargestellt werden:

1. Bestätigter Benutzername (vom fernen Betriebssystem)
2. Benutzername und Kennwort (Betriebssystem, LDAP oder benutzerdefinierte Repositorys von Drittanbietern)

3. Quellennetzadresse (z. B. IP-Adresse)
4. Digitales X.509-Zertifikat (gegenseitige SSL/TLS-Authentifizierung)
5. Sicherheitstokens (z. B. LTPA2-Token)
6. Andere benutzerdefinierte Sicherheit (Funktionalität, die von Drittanbieterexits bereitgestellt wird)
7. SSH-Schlüssel

Die Integration von IBM MQin IBM Cloud Pak for Integration fügt einen neuen Authentifizierungstyp für die Webkonsole hinzu: Single Sign-on mit Cloud Pak. (Nur CP4I)

Rollenzuordnung:

In der Rollenzuordnungsstufe können die Berechtigungsnachweise, die in der Authentifizierungsstufe bereitgestellt wurden, einer alternativen Benutzer-ID zugeordnet werden. Wenn der zugeordneten Benutzer-ID die Erlaubnis zum Fortfahren erteilt wird (z. B. können Benutzer mit Verwaltungsaufgaben durch Kanalauthentifizierungsregeln blockiert werden), wird die zugeordnete Benutzer-ID an die finale Stufe weitergeleitet, in der Aktivitäten für IBM MQ-Ressourcen autorisiert werden.

Autorisierung:

IBM MQ bietet die Möglichkeit, verschiedenen Benutzern für verschiedene Messaging-Ressourcen, z. B. Warteschlangen, Themen und andere Warteschlangenmanagerobjekte, unterschiedliche Berechtigungen zuzuweisen.

Protokollierungsaktivität:

Einige Benutzer von IBM MQ müssen möglicherweise einen Prüfsatz erstellen, um auf MQ-Ressourcen zugreifen zu können. Beispiele für wünschenswerte Prüfprotokolle können Konfigurationsänderungen enthalten, die Informationen über die Änderung enthalten, die zusätzlich zu den angeforderten Änderungen enthalten sind.

Für die Implementierung dieser Anforderung stehen die folgenden Informationsquellen zur Verfügung:

1. Ein IBM MQ-Warteschlangenmanager kann so konfiguriert werden, dass er ein Befehlsereignis generiert, wenn ein Verwaltungsbefehl erfolgreich ausgeführt wurde.
2. Ein IBM MQ-Warteschlangenmanager kann so konfiguriert werden, dass er Konfigurationsereignisse generiert, wenn eine Warteschlangenmanagerressource erstellt, geändert oder gelöscht wird.
3. Ein IBM MQ-Warteschlangenmanager kann so konfiguriert werden, dass er ein Berechtigungsereignis generiert, wenn eine Berechtigungsprüfung für eine Ressource fehlschlägt.
4. Fehlermeldungen, die auf fehlgeschlagene Berechtigungsprüfungen hinweisen, werden in die Fehlerprotokolle des Warteschlangenmanagers geschrieben.
5. Die IBM MQ-Konsole schreibt Prüfnachrichten in ihre Protokolle, wenn Authentifizierungs- bzw. Berechtigungsprüfungen fehlschlagen oder wenn Warteschlangenmanager erstellt, gestartet, gestoppt oder gelöscht werden.
6. Die IBM MQ Appliance schreibt Prüfnachrichten in ihre Protokolle, um Benutzeranmeldungen und Systemänderungen aufzuzeichnen.

Wenn diese Lösungsmöglichkeiten in Betracht gezogen werden, sollten die IBM MQ-Benutzer folgende Punkte berücksichtigen:

- Ereignisnachrichten sind nicht persistent, so dass beim erneuten Starten eines Warteschlangenmanagers die Informationen verloren gehen. Alle Ereignismonitore sollten so konfiguriert werden, dass sie ständig alle verfügbaren Nachrichten konsumieren und den Inhalt auf persistente Datenträger übertragen.
- Privilegierte IBM MQ-Benutzer haben ausreichende Berechtigungen, um Ereignisse zu deaktivieren, den Inhalt von Protokollen zu löschen oder Warteschlangenmanager zu löschen.

Weitere Informationen zur Sicherung des Zugriffs auf IBM MQ-Daten und Bereitstellung eines Prüfprotokolls finden Sie in folgenden Abschnitten:

- IBM MQ-Sicherheitsmechanismen

- Konfigurationsereignisse
- Befehlsereignisse
- Fehlerprotokolle

Datenverarbeitung

Verschlüsselung mit einer PKI-Infrastruktur (Public Key Infrastructure):

Sie können Netzverbindungen zu IBM MQ sichern, indem Sie angeben, dass die Verbindungen TLS verwenden, die auch die gegenseitige Authentifizierung der einleitenden Seite der Verbindung bereitstellen können.

Die Verwendung der PKI-Sicherheitseinrichtungen, die durch Transportmechanismen bereitgestellt werden, ist der erste Schritt, um die Datenverarbeitung mit IBM MQ zu sichern. Ohne weitere Sicherheitsfunktionen zu aktivieren, besteht das Verhalten einer konsumierenden Anwendung jedoch darin, alle Nachrichten zu verarbeiten, die an sie übermittelt wurden, ohne zu überprüfen, wo der Ursprung der Nachricht ist oder ob die Nachricht während der Übertragung geändert wurde.

IBM MQ-Benutzer, die für die Verwendung von AMS-Funktionen (Advanced Message Security) lizenziert sind, können durch die Definition und Konfiguration von Sicherheitsrichtlinien steuern, wie die in Nachrichten enthaltenen personenbezogenen Daten von Anwendungen verarbeitet werden. Sicherheitsrichtlinien ermöglichen es, dass digitale Signatur und/oder Verschlüsselung auf Nachrichtendaten zwischen Anwendungen angewendet werden können.

Es ist möglich, Sicherheitsrichtlinien zu verwenden, um eine digitale Signatur zu fordern und zu validieren, wenn Nachrichten konsumiert werden, um sicherzustellen, dass Nachrichten authentisch sind. Die AMS-Verschlüsselung stellt eine Methode zur Verfügung, mit der Nachrichtendaten von einem lesbaren Formular in eine verschlüsselte Version konvertiert werden, die nur von einer anderen Anwendung decodiert werden kann, wenn es sich um den beabsichtigten Empfänger oder die Nachricht handelt und Zugriff auf den richtigen Entschlüsselungsschlüssel hat.

Weitere Informationen zur Verwendung von SSL und Zertifikaten zum Sichern Ihrer Netzverbindungen finden Sie in den folgenden Abschnitten in der Produktdokumentation zu IBM MQ:

- TLS-Sicherheit für IBM MQ konfigurieren
- AMS-Übersicht

Datenlöschung

IBM MQ stellt Befehle und Benutzerschnittstellenaktionen zur Verfügung, mit denen Daten gelöscht werden, die dem Produkt bereitgestellt wurden. Das bedeutet, dass Benutzer von IBM MQ Daten löschen können, die sich auf bestimmte Personen beziehen, falls dies erforderlich sein sollte.

- Bereiche des IBM MQ-Verhaltens, die für die Einhaltung der DSGVO-Bestimmungen in Bezug auf das Löschen von Kundendaten bedacht werden sollten
  - Löschen von Nachrichtendaten, die in einer Anwendungswarteschlange gespeichert sind, durch:
    - Einzelne Nachrichten unter Verwendung der Messaging-API oder -Tools oder unter Verwendung von Nachrichtenverfallszeit entfernen
    - Angeben, dass Nachrichten nicht persistent sind, in einer Warteschlange gehalten werden, in der die nicht persistente Nachrichtenklasse normal ist und der Warteschlangenmanager erneut gestartet wird.
    - Die Warteschlange wird administrativ gelöscht.
    - Die Warteschlange wird gelöscht.
  - Gespeicherter Veröffentlichungsdaten, die in einem Thema gespeichert sind, löschen von:
    - Angeben, dass Nachrichten nicht persistent sind und den Warteschlangenmanager erneut starten.
    - Die aufbewahrten Daten durch neue Daten ersetzen oder die Nachrichtenablaufzeit verwenden.
    - Die Themenzeichenfolge wird administrativ gelöscht.

  - Löschen Sie auf einem Warteschlangenmanager gespeicherte Daten, indem Sie den gesamten Warteschlangenmanager und alle replizierten Kopien für die Hochverfügbarkeit oder Disaster-Recovery löschen.
  - Löschen Sie die Daten, die von den Service-Trace-Befehlen gespeichert werden, indem Sie die Dateien im Traceverzeichnis löschen.
  - Löschen Sie FFST-Daten, die gespeichert werden, indem Sie die Dateien im Fehlerverzeichnis löschen.
  - Löschen Sie die Speicherauszüge des Adressraums und der Coupling-Facility (unter z/OS).
  - Löschen Sie Archiv-, Backup-oder andere Kopien dieser Daten.
- Bereiche des IBM MQ-Verhaltens, die für die Einhaltung der DSGVO-Bestimmungen in Bezug auf das Löschen von Benutzeraccountdaten bedacht werden sollten
  - Sie können Benutzeraccountdaten und Vorgaben löschen, die von IBM MQ zum Herstellen von Verbindungen zu Warteschlangenmanagern und Drittanbieterservices gespeichert werden, indem Sie Folgendes löschen (einschließlich der Archiv- und Sicherungsdateien sowie anderweitig replizierter Kopien davon):
    - Authentifizierungsdaten des Warteschlangenmanagers, die Berechtigungsnachweise speichern.
    - WS-Manager-Berechtigungsdatensätze, die auf Benutzer-IDs verweisen.
    - WS-Manager-Kanalauthentifizierungsregeln, die bestimmte IP-Adressen, DNs oder Benutzer-IDs von Zertifikaten zuordnen oder blockieren.
    - Berechtigungsnachweisdateien, die von IBM MQ Managed File Transfer Agent, Logger und dem MFT-Plug-in für MQ Explorer für die Authentifizierung bei Warteschlangenmanager- und Dateiservern verwendet werden.
    - Digitale X.509-Zertifikate, die aus Keystores stammende Informationen zu einer Einzelperson darstellen oder enthalten, die von SSL/TLS-Verbindungen oder IBM MQ Advanced Message Security (AMS) verwendet werden.
    - Einzelne Benutzeraccounts aus IBM MQ Appliance, einschließlich des Verweises auf diese Accounts in Systemprotokolldateien.
    - Metadaten des Arbeitsbereichs von IBM MQ Explorer und Einstellungen für Eclipse
    - Kennwortspeicher von IBM MQ Explorer, wie im Abschnitt Password Preferences (Kennwortvorgaben) beschrieben.
    - Konfigurationsdateien für die IBM MQ-Konsole und den mqweb-Server.
    - Salesforce-Verbindungsdatenkonfigurationsdateien.
    - Blockchain-Verbindungsdatenkonfigurationsdateien.
    - IBM MQ Internet Pass-Thru-Konfigurationsdateien und -Keystores.

Weitere Informationen finden Sie hier:

- IBM MQ Bridge für Salesforce konfigurieren
- IBM MQ für die Verwendung mit Blockchain konfigurieren
- MFT-und IBM MQ-Verbindungsauthentifizierung
- Berechtigungsnachweise für einen Dateiserver mithilfe der Datei "ProtocolBridgeCredentials.xml" zuordnen
- Benutzer und Rollen von IBM MQ Console konfigurieren

Datenüberwachung

IBM MQ stellt eine Reihe von Überwachungsfunktionen bereit, mit denen Benutzer die Leistung von Anwendungen und Warteschlangenmanagern besser überwachen können.

Außerdem stellt IBM MQ einige Funktionen zur Verwaltung von Fehlerprotokollen von Warteschlangenmanagern bereit.

Weitere Informationen finden Sie hier:

- IBM MQ-Netz überwachen
- Diagnosenachrichtenservices
- QMErrorLog-Service
- IBM MQ Appliance - Überwachung und Berichterstellung

Funktionalität für die Einschränkung der Verwendung von persönlichen Daten

Mithilfe der in diesem Dokument zusammengefassten Funktionen ermöglicht IBM MQ den Endbenutzern, die Verwendung ihrer personenbezogenen Daten zu beschränken.

IBM MQ-Nachrichtenwarteschlangen sollten nicht in derselben Weise wie eine Datenbank als permanenter Datenspeicher verwendet werden, was insbesondere bei der Verarbeitung von Anwendungsdaten zutrifft, die der DSGVO unterliegen.

Im Gegensatz zu einer Datenbank, in der Daten über eine Suchabfrage gefunden werden können, kann es schwierig sein, Nachrichtendaten zu finden, es sei denn, Sie kennen die Warteschlangen-, Nachrichten- und Korrelations-IDs einer Nachricht.

Wenn Nachrichten, die Daten einer bestimmten Einzelperson enthalten, leicht identifiziert und aufgefunden werden können, ist es mithilfe der standardmäßigen IBM MQ-Messaging-Funktionen möglich, auf die Nachrichtendaten zuzugreifen und sie zu bearbeiten.

Dateiverwaltung

1. IBM MQ Managed File Transfer führt keine Malware-Scans auf Dateien aus, die übertragen werden. Dateien werden übertragen, und es wird eine Integritätsprüfung durchgeführt, um sicherzustellen, dass die Dateidaten während der Übertragung nicht geändert werden. Die Quell- und Ziel-Prüfsummen werden als Teil der Übertragungsstatus-Publikation veröffentlicht. Es wird empfohlen, dass Endbenutzer geeignete Malware-Scans für ihre Umgebung implementieren, bevor MFT die Datei überträgt und nachdem MFT eine Datei an einen fernen Endpunkt übergibt.
2. IBM MQ Managed File Transfer führt keine Aktionen auf der Basis des MIME-Typs bzw. der Dateierweiterung durch. MFT liest die Datei und überträgt die Bytes genau wie aus der Eingabedatei gelesen.

Architekturen auf der Basis eines einzelnen Warteschlangenmanagers

Zu den einfachsten IBM MQ-Architekturen gehören solche, für die nur ein einzelner Warteschlangenmanager konfiguriert und verwendet wird.

Bevor Sie mit der Planung einer IBM MQ-Architektur beginnen, sollten Sie sich mit den grundlegenden IBM MQ-Konzepten vertraut machen. Siehe IBM MQ Technische Übersicht.

Eine Reihe möglicher Architekturen mit einem einzigen Warteschlangenmanager werden in den folgenden Abschnitten beschrieben:

- „Einzelwarteschlangenmanager mit lokalen Anwendungen, die auf einen Service zugreifen” auf Seite 19
- „Einzelnes Warteschlangenmanager mit fernen Anwendungen, die auf einen Service als Clients zugreifen” auf Seite 20
- „Einzelwarteschlangenmanager mit einer Publish/Subscribe-Konfiguration” auf Seite 20

Einzelwarteschlangenmanager mit lokalen Anwendungen, die auf einen Service zugreifen

Die erste Architektur auf der Basis eines einzigen Warteschlangenmanagers besteht darin, dass die Anwendungen, die auf einen Service zugreifen, auf demselben System ausgeführt werden wie die An-

wendungen, die den Service bereitstellen. ein IBM MQ-Warteschlangenmanager stellt die asynchrone Kommunikation zwischen den Anwendungen, die den Service anfordern, und den Anwendungen, die den Service bereitstellen, bereit. Dies bedeutet, dass die Kommunikation zwischen den Anwendungen auch dann fortgesetzt werden kann, wenn eine der Anwendungen für einen längeren Zeitraum offline ist.

Einzelnes Warteschlangenmanager mit fernen Anwendungen, die auf einen Service als Clients zugreifen

Die zweite Architektur auf der Basis eines einzelnen Warteschlangenmanagers verfügt über die Anwendungen, die über Remotezugriff von den Anwendungen ausgeführt werden, die den Service bereitstellen. Die fernen Anwendungen werden auf verschiedenen Systemen für die Services ausgeführt. Die Anwendungen stellen eine Verbindung als Clients mit dem einzelnen Warteschlangenmanager her. Dies bedeutet, dass der Zugriff auf einen Service mehreren Systemen über einen einzigen Warteschlangenmanager zur Verfügung gestellt werden kann.

Eine Einschränkung dieser Architektur besteht darin, dass eine Netzverbindung verfügbar sein muss, damit eine Anwendung ausgeführt werden kann. Die Interaktion zwischen der Anwendung und dem WS-Manager über die Netzverbindung erfolgt synchron.

Einzelwarteschlangenmanager mit einer Publish/Subscribe-Konfiguration

Eine alternative Architektur, die einen einzelnen WS-Manager verwendet, ist die Verwendung einer Publish/Subscribe-Konfiguration. Beim Publish/Subscribe-Messaging können Sie den Anbieter von Informationen von den Konsumenten dieser Informationen entkoppeln. Dies unterscheidet sich vom Punkt-zu-Punkt-Messaging-Stile in den zuvor beschriebenen Architekturen, wo die Anwendungen Informationen über die Zielanwendung kennen müssen, z. B. den Namen der Warteschlange, in die Nachrichten gestellt werden sollen. Über IBM MQ Publish/Subscribe veröffentlicht die sendende Anwendung ein bestimmtes Thema, das auf dem Inhalt der Informationen basiert. IBM MQ sorgt für die Verteilung der Nachricht an Anwendungen, die mithilfe einer Subskription ihr Interesse an diesem Inhalt angemeldet haben. Die empfangenden Anwendungen müssen außerdem nichts über die Quelle der Nachrichten wissen, um sie zu empfangen. Weitere Informationen finden Sie unter Publish/Subscribe-Nachrichtenübermittlung und Beispiel für eine Publish/Subscribe-Konfiguration eines einzelnen Warteschlangenmanagers.

Zugehörige Konzepte

Einführung in IBM MQ

Zugehörige Tasks

„IBM MQ-Architektur planen” auf Seite 5
Beachten Sie bei der Planung einer IBM MQ-Umgebung die Unterstützung, die IBM MQ für Architekturen mit einzelnen oder mehreren Warteschlangenmanagern sowie für Punkt-zu-Punkt- und Publish/Subscribe-Messaging bereitstellt. Planen Sie auch den Ressourcenbedarf und die Nutzung von Protokollierungs- und Sicherheitsfunktionen.

Warteschlangenmanager auf Multiplatforms erstellen und verwalten

Architekturen auf der Basis von mehreren Warteschlangenmanagern

Sie können Methoden zur Steuerung der Warteschlangen für verteilte Nachrichten verwenden, um eine IBM MQ-Architektur zu erstellen, die die Konfiguration und Verwendung mehrerer Warteschlangenemanager umfasst.

Bevor Sie mit der Planung einer IBM MQ-Architektur beginnen, sollten Sie sich mit den grundlegenden IBM MQ-Konzepten vertraut machen. Siehe IBM MQ Technische Übersicht.

Eine IBM MQ-Architektur kann geändert werden, ohne dass Änderungen an Anwendungen, die Services bereitstellen, erforderlich sind, indem zusätzliche Warteschlangenmanager hinzugefügt werden.

Anwendungen können auf derselben Maschine wie ein Warteschlangenmanager gehostet werden und dann asynchrone Kommunikation mit einem Service erhalten, der auf einem anderen Warteschlangenma-

nager auf einem anderen System gehostet wird. Alternativ können Anwendungen, die auf einen Service zugreifen, als Clients eine Verbindung zu einem Warteschlangenmanager herstellen, der dann den asynchronen Zugriff auf den Service auf einem anderen Warteschlangenmanager bereitstellt.

Routes, die verschiedene Warteschlangenmanager und ihre Warteschlangen verbinden, werden mithilfe von verteilten Warteschlangenverfahren definiert. Die Warteschlangenmanager in der Architektur werden über Kanäle miteinander verbunden. Kanäle werden verwendet, um Nachrichten automatisch von einem Warteschlangenmanager in eine andere Richtung in eine andere Richtung zu versetzen, abhängig von der Konfiguration der Warteschlangenmanager.

Eine Übersicht über die Planung eines IBM MQ-Netzes finden Sie unter „Entwerfen verteilter WS-Manager-Netze” auf Seite 22.

Informationen zur Planung von Kanälen für die IBM MQ-Architektur finden Sie unter IBM MQ - Methode zur verteilten Warteschlangensteuerung.

Über die verteilte Warteschlangenverwaltung können Sie die Kommunikation zwischen Warteschlangenmanagern erstellen und überwachen. Weitere Informationen zur verteilten Warteschlangenverwaltung finden Sie im Abschnitt Einführung in die verteilte Warteschlangenverwaltung .

Zugehörige Tasks

„IBM MQ-Architektur planen” auf Seite 5
Beachten Sie bei der Planung einer IBM MQ-Umgebung die Unterstützung, die IBM MQ für Architekturen mit einzelnen oder mehreren Warteschlangenmanagern sowie für Punkt-zu-Punkt- und Publish/Subscribe-Messaging bereitstellt. Planen Sie auch den Ressourcenbedarf und die Nutzung von Protokollierungs- und Sicherheitsfunktionen.

Warteschlangenmanager auf Multiplatforms erstellen und verwalten

Verteilte Warteschlangen und Cluster planen

Sie können Warteschlangen, die sich auf verteilten Warteschlangenmanagern befinden, manuell verbinden, oder Sie können einen WS-Manager-Cluster erstellen und das Produkt die Warteschlangenmanager für Sie verbinden. Um eine geeignete Topologie für Ihr verteiltes Messaging-Netzwerk auszuwählen, müssen Sie Ihre Anforderungen für die manuelle Steuerung, die Netzgröße, die Häufigkeit von Änderungen, die Verfügbarkeit und die Skalierbarkeit in Betracht ziehen.

Vorbereitende Schritte

In dieser Task wird davon ausgegangen, dass Sie wissen, welche verteilten Nachrichtenübertragungsnetze und wie sie funktionieren. Eine technische Übersicht finden Sie unter Verteilte Steuerung von Warteschlangen und Clustern.

Informationen zu diesem Vorgang

Wenn Sie ein verteiltes Messaging-Netz erstellen möchten, können Sie Kanäle manuell konfigurieren, um Warteschlangen zu verbinden, die sich auf verschiedenen Warteschlangenmanagern befinden, oder Sie können einen Warteschlangenmanager-Cluster erstellen. Durch das Clustering können WS-Manager miteinander kommunizieren, ohne zusätzliche Kanaldefinitionen oder ferne Warteschlangendefinitionen einzurichten, wodurch ihre Konfiguration und Verwaltung vereinfacht wird.

Wenn Sie eine geeignete Topologie für Ihr verteiltes Publish/Subscribe-Netz auswählen möchten, müssen Sie die folgenden allgemeinen Fragen berücksichtigen:

- Wie viel manuelle Kontrolle benötigen Sie über die Verbindungen in Ihrem Netzwerk?
- Wie groß wird Ihr Netzwerk sein?
- Wie dynamisch wird es sein?
- Was sind Ihre Verfügbarkeits-und Skalierbarkeitsanforderungen?

Prozedur

- Überlegen Sie, wie viel manuelle Steuerung Sie über die Verbindungen in Ihrem Netzwerk benötigen.

  Wenn Sie nur ein paar Verbindungen benötigen oder wenn einzelne Verbindungen sehr genau definiert werden müssen, sollten Sie das Netzwerk wahrscheinlich manuell erstellen.

  Wenn Sie mehrere Warteschlangenmanager benötigen, die logisch miteinander verknüpft sind und die Daten und Anwendungen gemeinsam nutzen müssen, sollten Sie sie in Betracht ziehen, sie in einem Warteschlangenmanager-Cluster zusammenzufassen.
- Schätzen Sie, wie groß Ihr Netzwerk sein muss.
  a) Schätzen Sie, wie viele Warteschlangenmanager Sie benötigen. Denken Sie daran, dass Warteschlangen in mehr als einem Warteschlangenmanager gehostet werden können.
  b) Wenn Sie einen Cluster verwenden möchten, fügen Sie zwei zusätzliche Warteschlangenmanager hinzu, um als vollständige Repositorys zu agieren.

  Bei größeren Netzen kann die manuelle Konfiguration und Verwaltung von Verbindungen sehr zeitaufwendig sein, und Sie sollten in Betracht ziehen, einen Cluster zu verwenden.
- Überlegen Sie, wie dynamisch die Netzaktivität sein wird.

  Planen Sie, dass ausgelastete Warteschlangen auf performanten WS-Managern gehostet werden.

  Wenn Sie erwarten, dass Warteschlangen häufig erstellt und gelöscht werden, sollten Sie einen Cluster verwenden.
- Berücksichtigen Sie Ihre Verfügbarkeits-und Skalierbarkeits
  a) Entscheiden Sie, ob Sie die hohe Verfügbarkeit von Warteschlangenmanagern gewährleisten müssen. Ist dies der Fall, schätzen Sie die Anzahl der Warteschlangenmanager, für die diese Anforderung gilt, ab.
  b) Überlegen Sie, ob einige Ihrer WS-Manager weniger fähig sind als andere.
  c) Überlegen Sie, ob die Kommunikationsverbindungen zu einigen Ihrer WS-Manager empfindlicher als andere sind.
  d) Ziehen Sie das Hosting von Warteschlangen auf mehreren Warteschlangenmanagern in Betracht

  Manuell konfigurierte Netze und Cluster können so konfiguriert werden, dass sie hoch verfügbar und skalierbar sind. Wenn Sie einen Cluster verwenden, müssen Sie zwei zusätzliche WS-Manager als vollständige Repositorys definieren. Wenn zwei vollständige Repositorys vorhanden sind, wird sichergestellt, dass der Cluster weiter betrieben wird, wenn eines der vollständigen Repositorys nicht mehr verfügbar ist. Stellen Sie sicher, dass die vollständigen WS-Manager-Repositorys robust, leistungsfähig und eine gute Netzkonnektivität sind. Es ist nicht geplant, die vollständigen WS-Manager-Repositorys für andere Arbeiten zu verwenden.
- Basierend auf diesen Berechnungen können Sie mithilfe der bereitgestellten Links entscheiden, ob Verbindungen zwischen Warteschlangenmanagern manuell konfiguriert werden sollen oder ob ein Cluster verwendet werden soll.

Nächste Schritte

Sie können jetzt Ihr verteiltes Messaging-Netz konfigurieren.

Zugehörige Tasks

Verteilte Warteschlangensteuerung konfigurieren

WS-Manager-Cluster konfigurieren

Entwerfen verteilter WS-Manager-Netze

IBM MQ sendet und empfängt Daten, die mithilfe von Warteschlangenmanagern und Kanälen über Netze zwischen Anwendungen ausgetauscht werden. Die Netzplanung umfasst die Definition von Anforderungen zum Erstellen eines Frameworks für die Verbindung dieser Systeme über ein Netz.

Kanäle können zwischen Ihrem System und jedem anderen System, mit dem Sie Kommunikation benötigen, erstellt werden. Multi-Hop-Kanäle können erstellt werden, um eine Verbindung zu Systemen

herzustellen, auf denen Sie keine direkten Verbindungen haben. Die in den Szenarios beschriebenen Nachrichtenkanalverbindungen werden in Abbildung 1 auf Seite 23 als Netzdiagramm dargestellt.

IBM MQ Internet Pass-Thru vereinfacht die Konfiguration von Kanälen zwischen Systemen in verschiedenen physischen Netzen sowie die Einrichtung von Kanälen, die über eine Firewall kommunizieren. Weitere Informationen finden Sie unter IBM MQ Internet Pass-Thru.

Namen der Kanal-und Übertragungswarteschlangen

Der Übertragungswarteschlange kann ein beliebiger Name gegeben werden. Um jedoch Unklarheiten zu vermeiden, können Sie ihnen dieselben Namen wie die Namen des Zielwarteschlangenmanagers oder die Aliasnamen des Warteschlangenmanagers geben. Dadurch wird die Übertragungswarteschlange der Route zugeordnet, die sie verwenden, und gibt einen klaren Überblick über parallele Routen, die über temporäre (mehrere-hackte) Warteschlangenmanager erstellt werden.

Es ist nicht so klar, dass die Kanalnamen abgeschnitten sind. Die Kanalnamen in Abbildung 1 auf Seite 23 für QM2 müssen sich beispielsweise für eingehende und abgehende Kanäle unterscheiden. Alle Kanalnamen können noch ihre Namen für die Übertragungswarteschlange enthalten, aber sie müssen qualifiziert sein, um sie eindeutig zu machen.

In WSM2 gibt es beispielsweise einen WSM3-Kanal von WSM1 und ein WSM3-Kanal zu QM3. Um die Namen eindeutig zu machen, kann der erste Name QM3_from_QM1 heißen und der zweite Name mit dem Namen QM3_von_QM2 benannt werden. Auf diese Weise zeigen die Kanalnamen den Namen der Übertragungswarteschlange im ersten Teil des Namens an. Die Richtung und der benachbarte WS-Manager-Name werden im zweiten Teil des Namens angezeigt.

Eine Tabelle mit den vorgeschlagenen Kanalnamen für Abbildung 1 auf Seite 23 finden Sie in Tabelle 1 auf Seite 23.

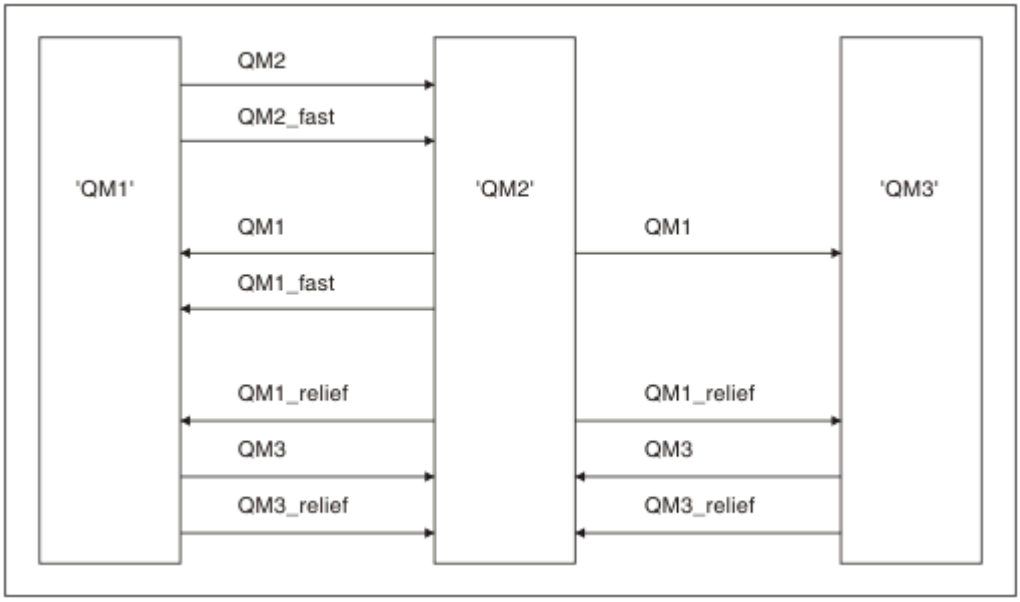


Abbildung 1. Netzdiagramm mit allen Kanälen

Tabelle 1. Beispiel für Kanalnamen

Leitwegname	Kanal des Warteschlangenmanagers	Name der Übertragungswarteschlange	Empfohlene Kanalbezeichnung
QM1	QM1 & QM2	WSM1 (bei WSM2)	QM1.from.QM2
QM1	QM2 & QM3	WSM1 (bei WSM3)	QM1.from.QM3

Tabelle 1. Beispiel für Kanalnamen (Forts.)			
Leitwegname	**Kanal des Warteschlangenmanagers**	**Name der Übertragungswarteschlange**	**Empfohlene Kanalbezeichnung**
QM1_fast	QM1 & QM2	QM1_schnell (bei WSM2)	QM1_fast.from.QM2
QM1_relief	QM1 & QM2	QM1_relief (bei QM2)	QM1_relief.from.QM2
QM1_relief	QM2 & QM3	QM1_relief (bei QM3)	QM1_relief.from.QM3
QM2	QM1 & QM2	WSM2 (bei WSM1)	QM2.from.QM1
QM2_fast	QM1 & QM2	QM2_schnell (bei QM1)	QM2_fast.from.QM1
QM3	QM1 & QM2	WSM3 (bei WSM1)	QM3.from.QM1
QM3	QM2 & QM3	WSM3 (bei WSM2)	QM3.from.QM2
QM3_relief	QM1 & QM2	QM3_relief (bei QM1)	QM3_relief.from.QM1
QM3_relief	QM2 & QM3	QM3_relief (bei QM2)	QM3_relief.from.QM2

Anmerkung:

1. z/OS In IBM MQ for z/OS dürfen Warteschlangenmanagernamen nur vier Zeichen haben.
2. Nennen Sie alle Kanäle in Ihrem Netzwerk eindeutig. Wie in Tabelle 1 auf Seite 23 gezeigt, ist dies eine gute Möglichkeit, die Namen der Quellen-und Zielwarteschlangenmanager in den Kanalnamen zu verwenden.

Netzplaner

Bei der Erstellung eines Netzes wird davon ausgegangen, dass eine andere, übergeordnete Funktion von *network planner* vorhanden ist, deren Pläne von den anderen Mitgliedern des Teams implementiert werden.

Für weit verbreitete Anwendungen ist es ökonomischer, in Bezug auf lokale Zugriffsseiten für die Konzentration des Nachrichtenverkehrs zu denken. Verwenden Sie die Breitband-Verbindungen zwischen den lokalen Zugriffsseiten (siehe Abbildung 2 auf Seite 25).

In diesem Beispiel gibt es zwei Hauptsysteme und eine Reihe von Satellitensystemen. Die tatsächliche Konfiguration hängt von den Geschäftsaspekten ab. Es gibt zwei Konzentratorwarteschlangenmanager, die sich in praktischen Centern befinden. Jeder QM-Konzentrator verfügt über Nachrichtenkanäle zu den lokalen WS-Managern:

- Der QM-Konzentrator 1 verfügt über Nachrichtenkanäle zu jedem der drei lokalen WS-Manager QM1, QM2 und QM3. Die Anwendungen, die diese WS-Manager verwenden, können über die QM-Konzentratoren miteinander kommunizieren.
- Der QM-Konzentrator 2 verfügt über Nachrichtenkanäle zu jedem der drei lokalen WS-Manager QM4, QM5 und QM6. Die Anwendungen, die diese WS-Manager verwenden, können über die QM-Konzentratoren miteinander kommunizieren.
- Die QM-Konzentratoren haben Nachrichtenkanäle untereinander, so dass jede Anwendung in einem WS-Manager Nachrichten mit jeder anderen Anwendung in einem anderen WS-Manager austauschen kann.

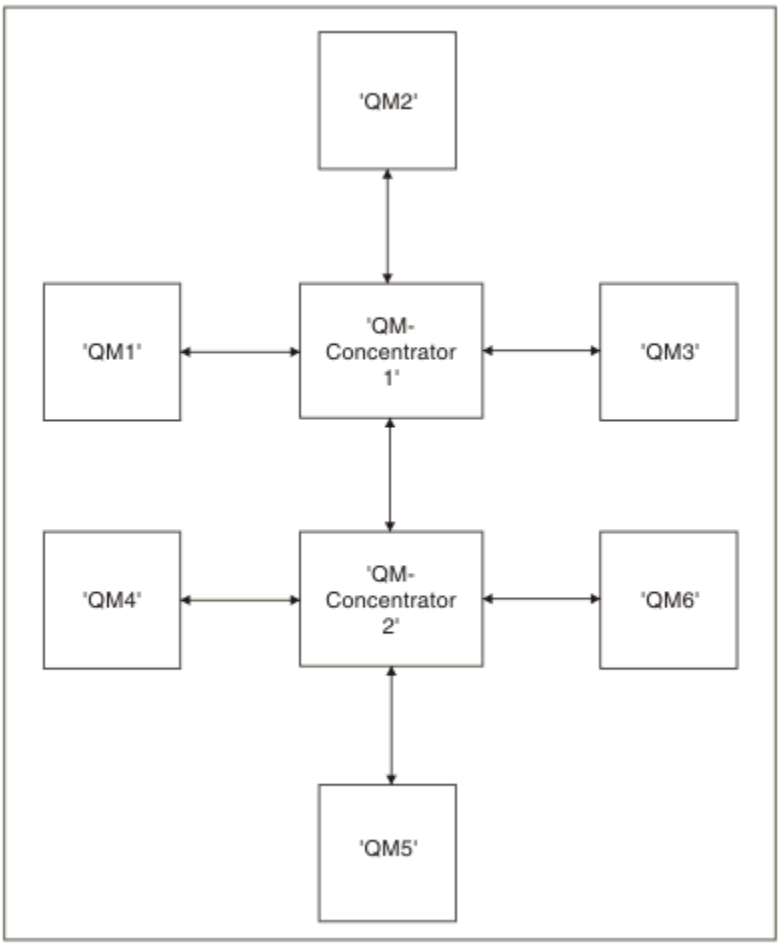


Abbildung 2. Netzdiagramm mit QM-Konzentratoren

Cluster entwerfen

Cluster bieten einen Mechanismus für die Verbindung von Warteschlangenmanagern in einer Weise, die sowohl die Erstkonfiguration als auch die laufende Verwaltung vereinfacht. Cluster müssen sorgfältig entworfen werden, um sicherzustellen, dass sie ordnungsgemäß funktionieren, und dass sie die erforderliche Verfügbarkeit und Reaktionsfähigkeit erreichen.

Vorbereitende Schritte

Eine Einführung in Clustering-Konzepte finden Sie in den folgenden Themen:

- Verteilte Steuerung von Warteschlangen und Clustern
- „Vergleich von Clustering und verteilter Steuerung von Warteschlangen” auf Seite 32
- Komponenten eines Clusters

Wenn Sie den WS-Manager-Cluster entwerfen, müssen Sie einige Entscheidungen treffen. Sie müssen zuerst entscheiden, welche WS-Manager im Cluster die vollständigen Repositorys der Clusterinformationen enthalten sollen. Jeder Warteschlangenmanager, den Sie erstellen, kann in einem Cluster arbeiten. Sie können eine beliebige Anzahl von Warteschlangenmanagern für diesen Zweck auswählen, aber die ideale Zahl ist zwei. Informationen zum Auswählen von Warteschlangenmanagern zum Speichern der vollständigen Repositorys finden Sie unter „Clusterwarteschlangenmanager für die Aufnahme von vollständigen Repositorys auswählen” auf Seite 35.

Weitere Informationen zum Entwerfen des Clusters finden Sie in den folgenden Abschnitten:

- „Beispielcluster” auf Seite 42

- „Cluster verwalten” auf Seite 36
- „Namenskonventionen für Cluster” auf Seite 37
- z/OS „Gruppen mit gemeinsamer Warteschlange und Cluster” auf Seite 38
- „Überlappende Cluster” auf Seite 39

Nächste Schritte

Weitere Informationen zum Konfigurieren und Arbeiten mit Clustern finden Sie in den folgenden Abschnitten:

- Kommunikation in einem Cluster einrichten
- Warteschlangenmanager-Cluster konfigurieren
- Nachrichten an und von Clustern weiterleiten
- Cluster für das Workload-Management verwenden

Weitere Informationen zum Konfigurieren des Clusters finden Sie unter „Tipps zum Clustering” auf Seite 40.

Verwendung mehrerer Clusterübertragungswarteschlangen planen

Sie können Übertragungswarteschlangen explizit definieren oder das System die Übertragungswarteschlangen für Sie generieren lassen. Wenn Sie die Übertragungswarteschlangen selbst definieren, haben Sie mehr Kontrolle über die Warteschlangendefinitionen. z/OS Unter z/OS haben Sie auch mehr Kontrolle über die Seitengruppe, in der die Nachrichten gespeichert werden.

Übertragungswarteschlangen definieren

Es gibt zwei Methoden zum Definieren von Übertragungswarteschlangen:

- Automatisch unter Verwendung des Warteschlangenmanagerattributs DEFCLXQ wie folgt:

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

  DEFCLXQ (SCTQ) gibt an, dass die Standardübertragungswarteschlange für alle Clustersenderkanäle SYSTEM.CLUSTER.TRANSMIT.QUEUE ist. Dies ist der Standardwert.

  DEFCLXQ (CHANNEL) gibt an, dass jeder Clustersenderkanal standardmäßig eine eigene Übertragungswarteschlange mit dem Namen SYSTEM.CLUSTER.TRANSMIT. *channel name* verwendet. Jede Übertragungswarteschlange wird automatisch vom WS-Manager definiert. Weitere Informationen finden Sie unter „Automatisch definierte Clusterübertragungswarteschlangen” auf Seite 28.
- Manuell, indem eine Übertragungswarteschlange mit einem Wert definiert wird, der für das Attribut CLCHNAME angegeben wurde. Das Attribut CLCHNAME gibt an, welche Clustersenderkanäle die Übertragungswarteschlange verwenden sollen. Weitere Informationen finden Sie unter „Planung für manuell definierte Clusterübertragungswarteschlangen” auf Seite 29.

Welche Sicherheit brauche ich?

Um einen Schalter einzuleiten, entweder automatisch oder manuell, benötigen Sie die Berechtigung zum Starten eines Kanals.

Um die Warteschlange definieren zu können, die als Übertragungswarteschlange verwendet werden soll, benötigen Sie die IBM MQ-Standardberechtigung.

Wann ist ein geeigneter Zeitpunkt für die Umsetzung der Änderung?

Wenn Sie die Übertragungswarteschlange ändern, die von Clustersenderkanälen verwendet wird, müssen Sie eine Zeit zuordnen, in der die Aktualisierung unter Berücksichtigung der folgenden Punkte gemacht werden soll:

- Die Zeit, die für einen Kanal benötigt wird, um die Übertragungswarteschlange zu wechseln, hängt von der Gesamtzahl der Nachrichten in der alten Übertragungswarteschlange, von der Anzahl der zu verschiebungsbedürftigen Nachrichten und von der Größe der Nachrichten ab.
- Anwendungen können Nachrichten weiterhin in die Übertragungswarteschlange stellen, während die Änderung stattfindet. Dies kann zu einer Erhöhung der Übergangszeit führen.
- Sie können den Parameter CLCHNAME einer beliebigen Übertragungswarteschlange oder DEFCLXQ zu einem beliebigen Zeitpunkt ändern, vorzugsweise wenn die Auslastung niedrig ist.

  Beachten Sie, dass nichts sofort passiert.
- Änderungen treten nur auf, wenn ein Kanal gestartet oder neu gestartet wird. Wenn ein Kanal gestartet wird, überprüft er die aktuelle Konfiguration und wechselt bei Bedarf in eine neue Übertragungswarteschlange.
- Es gibt mehrere Änderungen, die die Zuordnung eines Clustersenderkanals mit einer Übertragungswarteschlange ändern können:
  - Ändern Sie den Wert des CLCHNAME-Attributs einer Übertragungswarteschlange, wodurch CLCHNAME weniger spezifisch oder leer ist.
  - Ändern des Werts für das Attribut CLCHNAME einer Übertragungswarteschlange, wodurch CLCHNAME spezifischer wird.
  - Es wird eine Warteschlange mit dem angegebenen CLCHNAME gelöscht.
  - Ändern des Warteschlangenmanagerattributs DEFCLXQ.

Wie lange dauert der Wechsel?

Während des Übergangszeitraums werden alle Nachrichten für den Kanal von einer Übertragungswarteschlange in eine andere übertragen. Die Zeit, die für einen Kanal benötigt wird, um die Übertragungswarteschlange zu wechseln, hängt von der Gesamtzahl der Nachrichten in der alten Übertragungswarteschlange und von der Anzahl der zu verschiebungsbedürftigen Nachrichten ab.

Für Warteschlangen, die einige tausend Nachrichten enthalten, sollte es unter einer Sekunde dauern, bis die Nachrichten verschoben werden. Die tatsächliche Zeit hängt von der Anzahl und Größe der Nachrichten ab. Ihr Warteschlangenmanager sollte in der Lage sein, Nachrichten in vielen Megabyte pro Sekunde zu verschieben.

Anwendungen können Nachrichten weiterhin in die Übertragungswarteschlange stellen, während die Änderung stattfindet. Dies kann zu einer Erhöhung der Übergangszeit führen.

Jeder betroffene Clustersenderkanal muss erneut gestartet werden, damit die Änderung wirksam wird. Daher ist es am besten, die Konfiguration der Übertragungswarteschlange zu ändern, wenn der Warteschlangenmanager nicht ausgelastungslos ist, und es werden nur wenige Nachrichten in den Clusterübertragungswarteschlangen gespeichert.

Der **runswchl** -Befehl, z/OS oder der Befehl SWITCH CHANNEL (*) STATUS in CSQUTIL unter z/OS, kann verwendet werden, um den Status von Clustersenderkanälen und die anstehenden Änderungen abzufragen, die an ihrer Konfiguration der Übertragungswarteschlange ausstehen.

Vorgehensweise zum Implementieren der Änderung

Weitere Informationen dazu, wie Sie die Änderungen an mehreren Clusterübertragungswarteschlangen vornehmen, entweder automatisch oder manuell, finden Sie im Abschnitt System mit mehreren Clusterübertragungswarteschlangen implementieren .

Änderung rückgängig machen

Weitere Informationen zum Zurücknehmen von Änderungen finden Sie im Abschnitt Änderungen rückgängig machen , wenn Probleme auftreten.

Automatisch definierte Clusterübertragungswarteschlangen
Sie können das System die Übertragungswarteschlangen für Sie generieren lassen.

Informationen zu diesem Vorgang

Wenn ein Kanal nicht über eine manuell definierte Clusterübertragungswarteschlange verfügt, die ihm zugeordnet ist, und Sie DEFCLXQ (CHANNEL) angeben, definiert der Kanal beim Starten des Kanals automatisch eine permanent-dynamische Warteschlange für den Clustersenderkanal. Die Modellwarteschlange SYSTEM.CLUSTER.TRANSMIT.MODEL.queue wird verwendet, um die permanente dynamische Clusterübertragungswarteschlange mit dem Namen SYSTEM.cluster.transmit `ChannelName` automatisch zu definieren.

z/OS Informationen zum manuellen Festlegen der Clusterübertragungswarteschlangen finden Sie in „Planung für manuell definierte Clusterübertragungswarteschlangen” auf Seite 29.

Wichtig: z/OS

Wenn der Warteschlangenmanager auf IBM MQ 8.0migriert wird, verfügt er nicht über das SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE.

Definieren Sie diese Warteschlange zuerst, so dass der Befehl ALTER QGMR DEFCLXQ (CHANNEL) wirksam wird.

Die folgende JCL ist ein Beispiel für den Code, den Sie zum Definieren der Modellwarteschlange verwenden können:

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

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

* MODEL QUEUE ATTRIBUTES
DEFTYPE( PERMDYN ) +

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

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

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

Vorgehensweise

1. Verwenden Sie das WS-Manager-Attribut *DEFCLXQ* .

   Weitere Informationen zu diesem Attribut finden Sie in ALTER QMGR .

   Es gibt zwei Optionen:

   SCTQ
   Diese Option ist die Standardeinstellung und bedeutet, dass Sie die einzelne Warteschlange SYSTEM.CLUSTER.TRANSMIT.QUEUE verwenden.

   CHANNEL
   Bedeutet, dass Sie mehrere Clusterübertragungswarteschlangen verwenden.
2. Gehen Sie wie folgt vor, um zu der neuen Zuordnung
   - Stoppen Sie den Kanal und starten Sie ihn erneut.
   - Der Kanal verwendet die neue Definition der Übertragungswarteschlange.
   - Nachrichten werden von einem Übergangsschalterprozess aus der alten Warteschlange in die neue Übertragungswarteschlange übertragen.

   Beachten Sie, dass alle Anwendungsnachrichten in die alte Definition gestellt werden.

   Wenn die Anzahl der Nachrichten in der alten Warteschlange null erreicht, werden neue Nachrichten direkt in die neue Übertragungswarteschlange gestellt.
3. Gehen Sie wie folgt vor, um zu überwachen, wann der Switching
   a) Ein Switch der Übertragungswarteschlange, der von einem Kanal eingeleitet wird, wird im Hintergrund ausgeführt, und Ihr Administrator kann das Jobprotokoll des Warteschlangenmanagers überwachen, um festzustellen, wann es abgeschlossen ist.
   b) Überwachen Sie Nachrichten im Jobprotokoll, um den Fortschritt des Switch anzuzeigen.
   c) Um sicherzustellen, dass nur die gewünschten Kanäle diese Übertragungswarteschlange verwenden, geben Sie den Befehl DIS CLUSQMGR(*) ein, wobei die Eigenschaft der Übertragungswarteschlange, die die Übertragungswarteschlange definiert, z. B. `APPQMGR.CLUSTER1.XMITQ`lautet.
   d) z/OS
   Verwenden Sie den Befehl SWITCH CHANNEL (*) STATUS unter CSQUTIL.

   Diese Option gibt Auskunft darüber, welche anstehenden Änderungen ausstehen und wie viele Nachrichten zwischen den Übertragungswarteschlangen verschoben werden müssen.

Ergebnisse

Sie haben die Clusterübertragungswarteschlange oder die Warteschlangen für die Clusterübertragung konfiguriert.

Zugehörige Tasks

„Planung für manuell definierte Clusterübertragungswarteschlangen” auf Seite 29
Wenn Sie die Übertragungswarteschlangen selbst definieren, haben Sie mehr Kontrolle über die Definitionen und die Seitengruppe, auf der die Nachrichten gehalten werden.

Zugehörige Verweise

ALTER QMGR

DISPLAY CLUSQMGR

Planung für manuell definierte Clusterübertragungswarteschlangen
Wenn Sie die Übertragungswarteschlangen selbst definieren, haben Sie mehr Kontrolle über die Definitionen und die Seitengruppe, auf der die Nachrichten gehalten werden.

Informationen zu diesem Vorgang

Ihr Administrator definiert eine Übertragungswarteschlange manuell und verwendet ein neues Warteschlangenattribut CLCHNAME, um zu definieren, welcher Clustersenderkanal bzw. die Kanäle diese Warteschlange als Übertragungswarteschlange verwenden.

Beachten Sie, dass CLCHNAME am Anfang oder am Ende ein Platzhalterzeichen enthalten kann, damit eine einzige Warteschlange für mehrere Kanäle verwendet werden kann.

Informationen zum automatischen Festlegen von Clusterübertragungswarteschlangen finden Sie in „Automatisch definierte Clusterübertragungswarteschlangen” auf Seite 28.

Vorgehensweise

1. Geben Sie z. B. Folgendes ein:

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

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

   Tipp: Sie müssen planen, welche Seitengruppe (und Pufferpool) Sie für Ihre Übertragungswarteschlangen verwenden. Sie können unterschiedliche Seitengruppen für verschiedene Warteschlangen haben und die Isolation zwischen ihnen bereitstellen, sodass eine Seitengruppe, die gefüllt wird, keine Auswirkungen auf die Übertragungswarteschlangen in anderen Seitengruppen hat.

   Informationen dazu, wie jeder Kanal die entsprechende Warteschlange auswählt, finden Sie im Abschnitt Mit Clusterübertragungswarteschlangen und Clustersenderkanälen arbeiten .

   Wenn der Kanal startet, wechselt er seine Zuordnung zur neuen Übertragungswarteschlange. Um sicherzustellen, dass keine Nachricht verloren geht, überträgt der Warteschlangenmanager Nachrichten automatisch aus der alten Clusterübertragungswarteschlange in die neue Übertragungswarteschlange in der Reihenfolge.
2. Verwenden Sie die Funktion CSQUTIL SWITCH, um in die neue Zuordnung zu wechseln.

   Weitere Informationen finden Sie im Abschnitt Die Übertragungswarteschlange, die Clustersenderkanälen (SWITCH) zugeordnet ist) umschalten.

   a) STOP den Kanal oder die Kanäle, deren Übertragungswarteschlange geändert werden soll, so dass sie sich im Status STOPPED befinden.

      Beispiel:

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

   b) Ändern Sie das Attribut `CLCHNAME(XXXX)` in der Übertragungswarteschlange.

   c) Verwenden Sie die Funktion SWITCH, um die Nachrichten zu wechseln oder die Vorgänge zu überwachen.

      Verwenden Sie den Befehl:

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

      um die Nachrichten zu verschieben, ohne den Kanal zu starten.

   d) Starten Sie den Kanal oder die Kanäle, und überprüfen Sie, ob der Kanal die richtigen Warteschlangen verwendet.

      Beispiel:

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

Tipp:

- Der folgende Prozess verwendet die Funktion CSQUTIL SWITCH. Weitere Informationen finden Sie im Abschnitt Die Übertragungswarteschlange, die Clustersenderkanälen (SWITCH) zugeordnet ist, wechseln .

  Sie müssen diese Funktion nicht verwenden, aber mit dieser Funktion stehen weitere Optionen zur Auswahl:

  – Mit SWITCH CHANNEL (*) STATUS können Sie den Schaltstatus von Clustersenderkanälen auf einfache Weise ermitteln. Es ermöglicht Ihrem Administrator, zu sehen, welche Kanäle derzeit geschaltet werden, und die Kanäle, die einen Switch anstehen, die wirksam werden, wenn diese Kanäle nächsten Start sind.

    Ohne diese Funktion muss der Administrator mehrere DISPLAY-Befehle verwenden und anschließend die resultierende Ausgabe verarbeiten, um diese Informationen zu ermitteln. Ihr Administrator kann auch bestätigen, dass eine Konfigurationsänderung das erforderliche Ergebnis hat.

  – Wenn CSQUTIL zum Starten des Switch verwendet wird, überwacht CSQUTIL den Fortschritt dieser Operation weiter und wird nur beendet, wenn der Switch abgeschlossen ist.

    Dies kann die Ausführung dieser Operationen im Stapelbetrieb erheblich erleichtern. Wenn CSQUTIL zum Umschalten mehrerer Kanäle ausgeführt wird, führt CSQUTIL diese Aktionen nacheinander aus. Dies kann weniger Auswirkungen auf Ihr Unternehmen haben als mehrere Switches, die parallel ausgeführt werden.

Ergebnisse

Sie haben die Clusterübertragungswarteschlange oder die Warteschlangen für die Clusterübertragung konfiguriert.

Zugriffssteuerung und mehrere Clusterübertragungswarteschlangen

Wählen Sie zwischen drei Prüfmodi aus, wenn eine Anwendung Nachrichten in ferne Clusterwarteschlangen einreiht. Die Modi sind: Prüfung über Fernzugriff gegen die Clusterwarteschlange, lokale Prüfung gegen SYSTEM.CLUSTER.TRANSMIT.QUEUE oder Prüfung gegen lokale Profile für die Clusterwarteschlange oder den Clusterwarteschlangenmanager.

IBM MQ gibt Ihnen die Möglichkeit, entweder lokal oder lokal und remote zu überprüfen, ob ein Benutzer berechtigt ist, eine Nachricht in eine ferne Warteschlange einzureihen. Eine typische IBM MQ-Anwendung verwendet nur die lokale Überprüfung und ist darauf angewiesen, dass der ferne Warteschlangenmanager der Zugriffsprüfung vertraut, die auf dem lokalen Warteschlangenmanager durchgeführt wurde. Wenn die ferne Prüfung nicht verwendet wird, wird die Nachricht mit der Berechtigung des fernen Nachrichtenkanalprozesses in die Zielwarteschlange gestellt. Um die Fernprüfung verwenden zu können, müssen Sie die Berechtigung 'put' für den empfangenden Kanal auf die Kontextsicherheit setzen.

Die lokalen Prüfungen werden für die Warteschlange, die die Anwendung öffnet, durchgeführt. Bei der verteilten Steuerung von Warteschlangen öffnet die Anwendung in der Regel eine Definition einer fernen Warteschlange und die Zugriffsprüfungen werden auf die Definition der fernen Warteschlange gestellt. Wenn die Nachricht mit einem vollständigen Routing-Header verbunden wird, werden die Prüfungen für die Übertragungswarteschlange durchgeführt. Wenn eine Anwendung eine Clusterwarteschlange öffnet, die sich nicht im lokalen WS-Manager befindet, gibt es kein lokales Objekt, das überprüft werden kann. Die Zugriffssteuerungsprüfungen werden anhand der Clusterübertragungswarteschlange SYSTEM.CLUSTER.TRANSMIT.QUEUE durchgeführt. Selbst bei mehreren Clusterübertragungswarteschlangen werden lokale Zugriffssteuerungsprüfungen für ferne Clusterwarteschlangen anhand von SYSTEM.CLUSTER.TRANSMIT.QUEUEdurchgeführt.

Die Auswahl der lokalen oder fernen Prüfung ist eine Auswahl zwischen zwei Extremwerte. Die ferne Überprüfung ist in differenzierter Ausführung. Jeder Benutzer muss über ein Zugriffssteuerungsprofil auf jedem WS-Manager im Cluster verfügen, um in eine beliebige Clusterwarteschlange zu stellen. Die

lokale Überprüfung ist grob-grainiert. Jeder Benutzer benötigt nur ein Zugriffssteuerungsprofil für die Clusterübertragungswarteschlange auf dem Warteschlangenmanager, mit dem sie verbunden sind. Mit diesem Profil können sie eine Nachricht in jede Clusterwarteschlange auf einem beliebigen WS-Manager in einem beliebigen Cluster einlegen.

Administratoren haben eine andere Möglichkeit, die Zugriffssteuerung für Clusterwarteschlangen einzurichten. Mit dem Befehl **setmqaut** können Sie ein Sicherheitsprofil für eine Clusterwarteschlange auf einem beliebigen Warteschlangenmanager im Cluster erstellen. Das Profil wirkt sich darauf aus, wenn Sie eine ferne Clusterwarteschlange lokal öffnen und dabei nur den Namen der Warteschlange angeben. Sie können auch ein Profil für einen fernen WS-Manager einrichten. Wenn Sie dies tun, kann der Warteschlangenmanager das Profil eines Benutzers überprüfen, der eine Clusterwarteschlange öffnet, indem er einen vollständig qualifizierten Namen bereitstellt.

Die neuen Profile funktionieren nur, wenn Sie die Zeilengruppe des Warteschlangenmanagers **ClusterQueueAccessControl** in RQMNameändern. Der Standardwert ist Xmitq . Sie müssen Profile für alle vorhandenen Clusterwarteschlangen erstellen, die Clusterwarteschlangen verwenden. Wenn Sie die Zeilengruppe in RQMName ändern, ohne Profile zu erstellen, werden die Anwendungen wahrscheinlich fehlschlagen.

Tipp: Die Zugriffsprüfung für Clusterwarteschlangen gilt nicht für die ferne Warteschlangensteuerung. Es werden weiterhin Zugriffsprüfungen für lokale Definitionen durchgeführt. Die Änderungen bedeuten, dass Sie denselben Ansatz verfolgen können, um die Zugriffsprüfung für Clusterwarteschlangen und Clusterthemen zu konfigurieren. z/OS Außerdem führen die Änderungen zu einer Annäherung zwischen der Zugriffsprüfungsmethode für Clusterwarteschlangen und z/OS. Unter z/OS werden zwar andere Befehle zum Konfigurieren der Zugriffsprüfung verwendet, doch in beiden Fällen wird die Zugriffsberechtigung anhand eines Profils und nicht anhand des Objekts selbst geprüft.

Zugehörige Konzepte

„Clustering: Anwendungsisolation mit mehreren Clusterübertragungswarteschlangen” auf Seite 52
Sie können die Nachrichtenflüsse zwischen Warteschlangenmanagern in einem Cluster isolieren. Sie können Nachrichten, die von verschiedenen Clustersenderkanälen transportiert werden, in verschiedene Clusterübertragungswarteschlangen stellen. Sie können den Ansatz in einem einzelnen Cluster oder mit überlappenden Clustern verwenden. Das Thema enthält Beispiele und einige bewährte Verfahren, die Sie bei der Auswahl eines zu verwendenden Ansatzes führen.

Zugehörige Tasks

Einstellung ClusterQueueAccessControl

Vergleich von Clustering und verteilter Steuerung von Warteschlangen

Vergleichen Sie die Komponenten, die für die Verbindung von WS-Managern mit verteilter Steuerung von Warteschlangen und Clustering definiert werden müssen.

Wenn Sie keine Cluster verwenden, sind Ihre Warteschlangenmanager unabhängig und kommunizieren mit der verteilten Steuerung von Warteschlangen. Wenn ein Warteschlangenmanager Nachrichten an einen anderen senden muss, müssen Sie Folgendes definieren:

- eine Übertragungswarteschlange
- Ein Kanal zum fernen Warteschlangenmanager

Abbildung 3 auf Seite 33 zeigt die Komponenten, die für die verteilte Steuerung von Warteschlangen erforderlich sind.

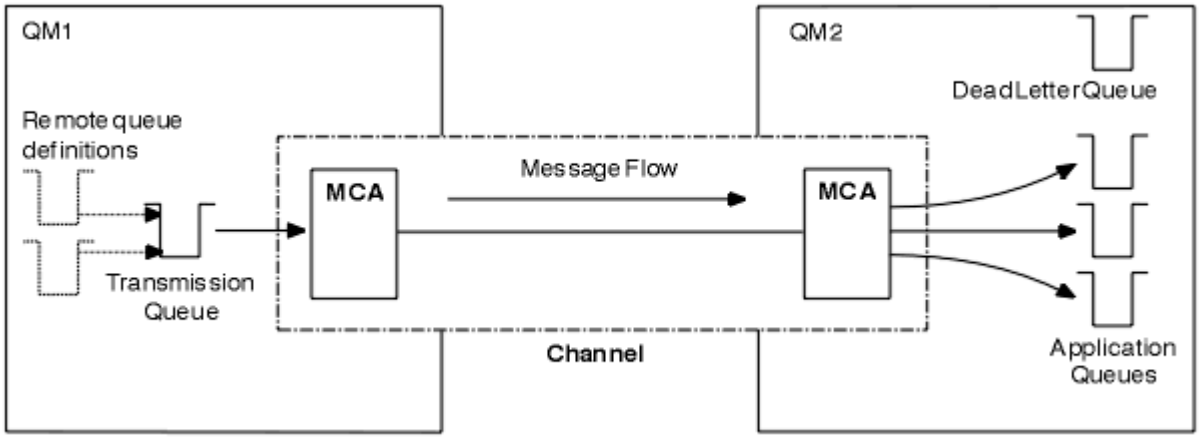


Abbildung 3. Verteilte Steuerung von Warteschlangen

Wenn Sie Warteschlangenmanager in einem Cluster gruppieren, stehen Warteschlangen in einem beliebigen WS-Manager allen anderen Warteschlangenmanagern im Cluster zur Verfügung. Jeder WS-Manager kann ohne explizite Definitionen eine Nachricht an jeden anderen Warteschlangenmanager in demselben Cluster senden. Sie stellen keine Kanaldefinitionen, Definitionen für ferne Warteschlangen oder Übertragungswarteschlangen für die einzelnen Ziele zur Verfügung. Jeder WS-Manager in einem Cluster verfügt über eine einzige Übertragungswarteschlange, von der er Nachrichten an jeden anderen WS-Manager im Cluster übertragen kann. Jeder WS-Manager in einem Cluster muss nur Folgendes definieren:

- Ein Clusterempfängerkanal, auf dem Nachrichten empfangen werden sollen.
- Ein Clustersenderkanal, mit dem er sich selbst einführt und die Informationen zum Cluster

Definitionen zum Festlegen eines Clusters im Vergleich zu verteilten Warteschlangensteuerung

Sehen Sie sich Abbildung 4 auf Seite 33 an, in dem jeweils vier Warteschlangenmanager mit jeweils zwei Warteschlangen angezeigt werden. Überlegen Sie, wie viele Definitionen benötigt werden, um diese WS-Manager mit Hilfe der verteilten Steuerung von Warteschlangen zu verbinden. Vergleichen Sie die Anzahl der Definitionen, die zum Festlegen des gleichen Netzes wie ein Cluster benötigt werden.

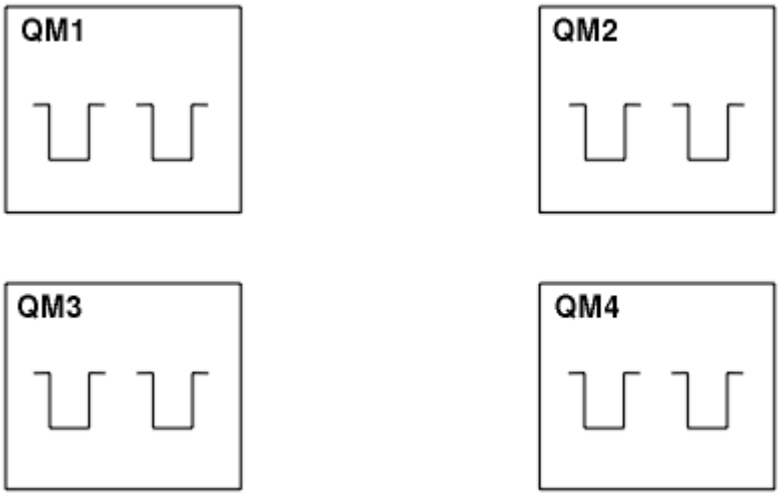


Abbildung 4. Ein Netz mit vier Warteschlangenmanagern

Definitionen zum Festlegen eines Netzes unter Verwendung der verteilten Steuerung von Warteschlangen

Um das in Abbildung 3 auf Seite 33 unter Verwendung der verteilten Warteschlangensteuerung gezeigte Netz einzurichten, können Sie die folgenden Definitionen verwenden:

Tabelle 2. Definitionen für verteilte Steuerung von Warteschlangen

Beschreibung	Anzahl pro WS-Manager	Gesamtanzahl
Eine Senderkanaldefinition für einen Kanal, auf dem Nachrichten an alle anderen Warteschlangenmanager gesendet werden sollen.	3	12
Eine Empfängerkanaldefinition für einen Kanal, auf dem Nachrichten von jedem anderen WS-Manager empfangen werden sollen.	3	12
Eine Übertragungswarteschlangendefinition für eine Übertragungswarteschlange zu jedem anderen Warteschlangenmanager	3	12
Eine lokale Warteschlangendefinition für jede lokale Warteschlange.	2	8
Eine Definition einer fernen Warteschlange für jede ferne Warteschlange, in die dieser WS-Manager Nachrichten einlegen möchte.	6	24

Sie können diese Anzahl von Definitionen unter Verwendung generischer Empfängerkanaldefinitionen reduzieren. Die maximale Anzahl von Definitionen kann bis zu 17 auf jedem Warteschlangenmanager betragen, was insgesamt 68 für dieses Netz ist.

Definitionen zum Festlegen eines Netzes mit Clustern

Um das in Abbildung 3 auf Seite 33 gezeigte Netz unter Verwendung von Clustern einzurichten, benötigen Sie die folgenden Definitionen:

Tabelle 3. Definitionen für Clustering

Beschreibung	Anzahl pro WS-Manager	Gesamtanzahl
Clustersenderkanaldefinition für einen Kanal, auf dem Nachrichten an einen Repository-WS-Manager gesendet werden sollen	1	4
Eine Clusterempfängerkanaldefinition für einen Kanal, auf dem Nachrichten von anderen Warteschlangenmanagern im Cluster empfangen werden sollen.	1	4
Eine lokale Warteschlangendefinition für jede lokale Warteschlange.	2	8

Um diesen Cluster von Warteschlangenmanagern (mit zwei vollständigen Repositorys) zu konfigurieren, benötigen Sie auf jedem Warteschlangenmanager vier Definitionen, insgesamt sind insgesamt 16 Definitionen vorhanden. Außerdem müssen Sie die WS-Manager-Definitionen für zwei der Warteschlangenmanager ändern, damit sie vollständige WS-Manager-Repository-WS-Manager für den Cluster bilden.

Es ist nur eine `CLUSSDR` -und eine `CLUSRCVR` -Kanaldefinition erforderlich. Wenn der Cluster definiert ist, können Sie Warteschlangenmanager (außer den Repository-WS-Managern) hinzufügen oder entfernen, ohne dass die anderen WS-Manager gestört werden.

Wenn Sie einen Cluster verwenden, wird die Anzahl der Definitionen reduziert, die zum Festlegen eines Netzes mit vielen Warteschlangenmanagern erforderlich sind.

Wenn weniger Definitionen vorhanden sind, besteht die Gefahr eines Fehlers:

- Objektnamen stimmen immer überein, z. B. der Kanalname in einem Sender-Empfänger-Paar.

- Der in einer Kanaldefinition angegebene Übertragungswarteschlangenname stimmt immer mit der korrekten Übertragungswarteschlangendefinition oder dem Namen der Übertragungswarteschlange überein, die in einer Definition einer fernen Warteschlange angegeben ist.
- Eine QREMOTE -Definition verweist immer auf die richtige Warteschlange auf dem fernen Warteschlangenmanager.

Sobald ein Cluster konfiguriert ist, können Sie Clusterwarteschlangen von einem Warteschlangenmanager in einen anderen im Cluster verschieben, ohne dass Systemverwaltungsaufgaben für einen anderen Warteschlangenmanager ausgeführt werden müssen. Es besteht keine Möglichkeit, die Definitionen von Kanal-, Fernwarteschlangen-oder Übertragungswarteschlangen zu löschen oder zu ändern. Sie können neue Warteschlangenmanager zu einem Cluster hinzufügen, ohne dass das vorhandene Netz unterbrochen wird.

Clusterwarteschlangenmanager für die Aufnahme von vollständigen Repositorys auswählen

In jedem Cluster müssen Sie mindestens eine, vorzugsweise zwei WS-Manager auswählen, um vollständige Repositorys zu speichern. Zwei vollständige Repositorys sind für alle, aber die außergewöhnlichsten Umstände ausreichend. Wählen Sie, wenn möglich, Warteschlangenmanager aus, die auf stabilen und permanent verbundenen Plattformen gehostet sind, die keine übereinstimmenden Ausfälle haben und die sich geographisch in einer zentralen Position befinden. Beachten Sie außerdem, dass Systeme als vollständige Repository-Hosts dedizieren sind und diese Systeme nicht für andere Tasks verwenden.

Vollständige Repositorys sind WS-Manager, die ein vollständiges Bild des Status des Clusters erhalten. Um diese Informationen gemeinsam nutzen zu können, ist jedes vollständige Repository über CLUSSDR -Kanäle (und die zugehörigen CLUSRCVR -Definitionen) mit jedem anderen vollständigen Repository im Cluster verbunden. Sie müssen diese Kanäle manuell definieren.

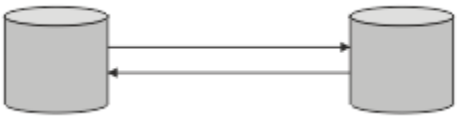


Abbildung 5. Zwei verbundene vollständige Repositorys.

Jeder andere WS-Manager im Cluster verwaltet ein Bild dessen, was er derzeit über den Status des Clusters in einem *Teilrepository* weiß. Diese WS-Manager veröffentlichen Informationen über sich selbst und fordern Informationen zu anderen Warteschlangenmanagern unter Verwendung von zwei verfügbaren vollständigen Repositorys an. Wenn ein ausgewähles vollständiges Repository nicht verfügbar ist, wird ein anderes verwendet. Wenn das ausgewählte vollständige Repository wieder verfügbar wird, erfasst es die neuesten neuen und geänderten Informationen von den anderen, so dass sie in Schritt halten. Wenn alle vollständigen Repositorys außer Betrieb sind, verwenden die anderen WS-Manager die Informationen, die sie in ihren Teilrepositorys haben. Sie beschränken sich jedoch auf die Verwendung der Informationen, die sie haben; neue Informationen und Anforderungen für Aktualisierungen können nicht verarbeitet werden. Wenn die vollständigen Repositorys wieder eine Verbindung zum Netz herstellen, werden Nachrichten ausgetauscht, um alle Repositorys (sowohl vollständige als auch partielle) auf dem neuesten Stand zu bringen.

Wenn Sie die Zuordnung von vollständigen Repositorys planen, müssen Sie die folgenden Aspekte berücksichtigen:

- Die Warteschlangenmanager, die zum Speichern der vollständigen Repositorys ausgewählt wurden, müssen zuverlässig und verwaltet sein. Wählen Sie die Warteschlangenmanager aus, die auf einer stabilen und permanent verbundenen Plattform gehostet werden.
- Berücksichtigen Sie die geplanten Ausfälle für die Systeme, die als Host für Ihre vollständigen Repositorys verwendet werden, und stellen Sie sicher, dass sie nicht übereinstimmende Ausfälle aufweisen.
- Berücksichtigen Sie die Netzleistung: Wählen Sie die Warteschlangenmanager aus, die sich geographisch in einer zentralen Position befinden oder die dasselbe System wie andere Warteschlangenmanager im Cluster gemeinsam nutzen.

- Überlegen Sie, ob ein Warteschlangenmanager Mitglied von mehreren Clustern ist. Es kann administrativ praktisch sein, denselben WS-Manager für die Verwendung der vollständigen Repositorys für mehrere Cluster zu verwenden, vorausgesetzt, dieser Vorteil ist ausgeglichen, wie ausgelastert die Auslastung des Warteschlangenmanagers ist.
- Sie sollten einige Systeme dedizieren, um nur vollständige Repositorys zu enthalten, und diese Systeme nicht für andere Tasks zu verwenden. Auf diese Weise wird sichergestellt, dass diese Systeme nur für die Konfiguration des Warteschlangenmanagers gewartet werden müssen und nicht aus dem Service für die Wartung anderer Geschäftsanwendungen entfernt werden. Außerdem stellt sie sicher, dass die Task zum Verwalten des Repositorys nicht mit Anwendungen für Systemressourcen konkursfähig ist. Dies kann besonders in großen Clustern (beispielsweise Cluster mit mehr als tausend Warteschlangenmanagern) von Vorteil sein, wenn die Auslastung des Clusterstatus durch die vollständigen Repositorys erheblich höher ist.

Es ist möglich, mehr als zwei vollständige Repositorys zu verwenden, wird aber selten empfohlen. Obwohl Objektdefinitionen (d. a. Warteschlangen, Themen und Kanäle) in alle verfügbaren vollständigen Repositorys fließen, werden nur Anforderungen von einem Teilrepository an maximal zwei vollständige Repositorys gestellt. Dies bedeutet, dass, wenn mehr als zwei vollständige Repositorys definiert sind und alle zwei vollständigen Repositorys nicht mehr verfügbar sind, einige Teilrepositorys möglicherweise keine Aktualisierungen empfangen, die sie erwarten würden. Weitere Informationen finden Sie unter MQ-Cluster: Warum nur zwei vollständige Repositorys?

Eine Situation, in der Sie möglicherweise mehr als zwei vollständige Repositorys definieren können, ist die Migration vorhandener vollständiger Repositorys auf neue Hardware oder neue Warteschlangenmanager. In diesem Fall sollten Sie die Ersatz-Vollrepositorys einführen und bestätigen, dass sie vollständig gefüllt wurden, bevor Sie die vorherigen vollständigen Repositorys entfernen. Wenn Sie ein vollständiges Repository hinzufügen, müssen Sie sich daran erinnern, dass Sie es mit CLUSSDR -Kanälen direkt mit jedem anderen vollständigen Repository verbinden müssen.

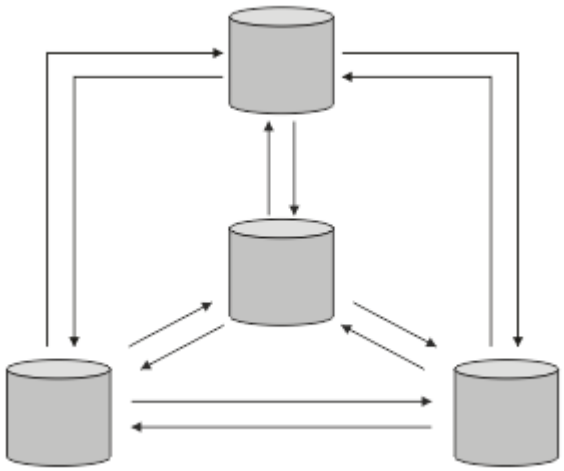


Abbildung 6. Mehr als zwei verbundene vollständige Repositorys

Zugehörige Informationen

MQ-Cluster: Warum nur zwei vollständige Repositorys?

Wie groß kann ein MQ-Cluster sein?

Cluster verwalten

Wählen Sie aus, welche WS-Manager mit welchem vollständigen Repository verknüpft werden sollen. Berücksichtigen Sie den Leistungseinwirkungseffekt, die Version des Warteschlangenmanagers und die Angabe, ob mehrere CLUSSDR -Kanäle wünschenswert sind.

Nachdem Sie die Warteschlangenmanager ausgewählt haben, um vollständige Repositorys zu speichern, müssen Sie festlegen, welche WS-Manager mit welchem vollständigen Repository verknüpft werden sollen. Die Kanaldefinition CLUSSDR verknüpft einen Warteschlangenmanager mit einem vollständigen Repository, aus dem es Informationen zu den anderen vollständigen Repositorys im Cluster herausfindet.

Von da an sendet der Warteschlangenmanager Nachrichten an alle zwei vollständigen Repositorys. Es wird immer versucht, zuerst die Kanaldefinition in CLUSSDR zu verwenden. Sie können auswählen, ob ein Warteschlangenmanager mit einem vollständigen Repository verknüpft werden soll. Wählen Sie bei der Auswahl die Topologie Ihrer Konfiguration und die physische oder geografische Position der Warteschlangenmanager aus.

Da alle Clusterinformationen an zwei vollständige Repositorys gesendet werden, kann es zu Situationen kommen, in denen Sie eine zweite CLUSSDR -Kanaldefinition erstellen möchten. Sie können einen zweiten CLUSSDR -Kanal in einem Cluster definieren, der über viele vollständige Repositorys verfügt, die sich über einen weiten Bereich erstrecken. Sie können dann steuern, an welche zwei vollständigen Repositorys Ihre Daten gesendet werden.

Namenskonventionen für Cluster

Sie sollten die Benennung von Warteschlangenmanagern in demselben Cluster unter Verwendung einer Namenskonvention berücksichtigen, die den Cluster angibt, zu dem der Warteschlangenmanager gehört. Verwenden Sie eine ähnliche Namenskonvention für Kanalnamen und erweitern Sie diese, um die Kanalmerkmale zu beschreiben.

Bewährte Verfahren bei der Benennung von MQ -Clustern

Obwohl Clusternamen bis zu 48 Zeichen umfassen können, sind relativ kurze Clusternamen hilfreich, wenn Namenskonventionen auf andere Objekte angewendet werden. Weitere Informationen finden Sie unter „Bewährte Verfahren bei der Auswahl von Clusterkanalnamen” auf Seite 37.

Bei der Auswahl eines Clusternamens ist es normalerweise hilfreich, den 'Zweck 'des Clusters (der wahrscheinlich langlebig ist) und nicht den 'Inhalt' darzustellen. Beispiel: 'B2BPROD' oder 'ACTTEST' statt 'QM1_QM2_QM3_CLUS'.

Bewährte Verfahren bei der Auswahl von Clusterwarteschlangenmanagernamen

Wenn Sie einen neuen Cluster und seine Member völlig neu erstellen, ziehen Sie eine Namenskonvention für die Warteschlangenmanager in Betracht, die ihre Clusternutzung widerspiegelt. Jeder WS-Manager muss einen anderen Namen haben. Sie können jedoch Warteschlangenmanagern in einem Cluster eine Gruppe ähnlicher Namen geben, um logische Gruppierungen zu identifizieren und sich daran zu erinnern (z. B. 'ACTTQM1, ACTTQM2).

Relatively short queue manager names (for example less than 8 characters) help if you choose to use the convention described in the next section, or something similar, for channel names.

Bewährte Verfahren bei der Auswahl von Clusterkanalnamen

Da Warteschlangenmanager und Cluster Namen mit bis zu 48 Zeichen haben können und ein Kanalname auf 20 Zeichen begrenzt ist, müssen Sie beim ersten Benennen von Objekten darauf achten, dass Sie die Namenskonvention nicht mitten in einem Projekt ändern müssen (siehe vorherigen Abschnitt).

Denken Sie beim Definieren von Kanälen daran, dass automatisch erstellte Clustersenderkanäle auf jedem Warteschlangenmanager im Cluster ihren Namen von dem entsprechenden Clusterempfängerkanal übernehmen, der auf dem empfangenden Warteschlangenmanager im Cluster konfiguriert ist. Diese müssen daher eindeutig sein und *auf fernen Warteschlangenmanagern im Cluster sinnvoll sein.*

Eine allgemeine Methode ist die Verwendung des Namens des Warteschlangenmanagers, dem der Clustername vorangestellt ist. Wenn der Clustername beispielsweise CLUSTER1 lautet und die Warteschlangenmanager QM1, QM2 sind, lauten die Clusterempfängerkanäle CLUSTER1.QM1, CLUSTER1.QM2.

Sie können diese Konvention erweitern, wenn Kanäle unterschiedliche Prioritäten haben oder unterschiedliche Protokolle verwenden. For example:

- CLUSTER1.QM1.S1
- CLUSTER1.QM1.N3
- CLUSTER1.QM1.T4

In diesem Beispiel könnte S1 der erste SNA-Kanal, N3 der NetBIOS -Kanal mit der Netzpriorität 3 und T4 TCP-IP-Adresse, die ein IPV4 -Netz verwendet, sein.

Gemeinsame Kanaldefinitionen benennen

Eine einzelne Kanaldefinition kann von mehreren Clustern gemeinsam genutzt werden. In diesem Fall müssen die hier vorgeschlagenen Namenskonventionen geändert werden. Wie in Kanaldefinitionen verwalten beschrieben ist es jedoch in der Regel vorzuziehen, für jeden Cluster diskrete Kanäle zu definieren.

Ältere Namenskonventionen für Kanäle

Außerhalb von Clusterumgebungen war es in der Vergangenheit üblich, eine 'FROMQM.TO.TARGETQM' -Namenskonvention zu verwenden, sodass Sie möglicherweise feststellen, dass vorhandene Cluster etwas Ähnliches verwendet haben (z. B. CLUSTER.TO.TARGET). Dies wird nicht als Teil eines neuen Clusterbenennungsschemas empfohlen, weil es die verfügbaren Zeichen weiter reduziert, um 'nützliche' Informationen in Ihrem Kanalnamen zu vermitteln.

z/OS **Kanalnamen unter IBM MQ for z/OS**

Sie können generische VTAM-Ressourcen oder generische DDNS-Namen (*Dynamic Domain Name Server*) definieren. Sie können Verbindungsnamen mit generischen Namen definieren. Wenn Sie jedoch eine Clusterempfängerdefinition erstellen, verwenden Sie keinen generischen Verbindungsnamen.

Das Problem bei der Verwendung generischer Verbindungsnamen für Clusterempfängerdefinitionen ist wie folgt: Wenn Sie einen CLUSRCVR mit einem generischen CONNAME definieren, gibt es keine Garantie, dass Ihre CLUSSDR -Kanäle auf die Warteschlangenmanager verweisen, die Sie beabsichtigen. Der ursprüngliche CLUSSDR-Kanal kann auf jeden Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange verweisen, nicht notwendigerweise auf einen Warteschlangenmanager, der ein vollständiges Repository enthält. Wenn ein Kanal erneut versucht, eine Verbindung herzustellen, stellt er möglicherweise eine Verbindung zu einem anderen Warteschlangenmanager mit demselben generischen Namen her, was den Nachrichtenfluss unterbricht.

z/OS ***Gruppen mit gemeinsamer Warteschlange und Cluster***

Gemeinsam genutzte Warteschlangen können Clusterwarteschlangen sein und Warteschlangenmanager in einer Gruppe mit gemeinsamer Warteschlange können auch Clusterwarteschlangenmanager sein.

Unter IBM MQ for z/OS können Sie Warteschlangenmanager in Gruppen mit gemeinsamer Warteschlange zusammenfassen. Ein Warteschlangenmanager in einer Gruppe mit gemeinsamer Warteschlange kann eine lokale Warteschlange definieren, die von bis zu 32 Warteschlangenmanagern gemeinsam genutzt werden kann.

Gemeinsam genutzte Warteschlangen können auch Clusterwarteschlangen sein. Außerdem können sich die Warteschlangenmanager in einer Gruppe mit gemeinsamer Warteschlange in einem oder mehreren Clustern befinden.

Sie können generische VTAM-Ressourcen oder generische DDNS-Namen (*Dynamic Domain Name Server*) definieren. Sie können Verbindungsnamen mit generischen Namen definieren. Wenn Sie jedoch eine Clusterempfängerdefinition erstellen, verwenden Sie keinen generischen Verbindungsnamen.

Das Problem bei der Verwendung generischer Verbindungsnamen für Clusterempfängerdefinitionen ist wie folgt: Wenn Sie einen CLUSRCVR mit einem generischen CONNAME definieren, gibt es keine Garantie, dass Ihre CLUSSDR -Kanäle auf die Warteschlangenmanager verweisen, die Sie beabsichtigen. Der ursprüngliche CLUSSDR-Kanal kann auf jeden Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange verweisen, nicht notwendigerweise auf einen Warteschlangenmanager, der ein vollständiges Repository enthält. Wenn ein Kanal erneut versucht, eine Verbindung herzustellen, stellt er möglicherweise eine Verbindung zu einem anderen Warteschlangenmanager mit demselben generischen Namen her, was den Nachrichtenfluss unterbricht.

Ein CLUSRCVR-Kanal, der den Listener-Port der Gruppe verwendet, kann nicht gestartet werden, da in diesem Fall nicht angegeben werden kann, mit welchem Warteschlangenmanager CLUSRCVR jedes Mal

eine Verbindung herstellt. Die Clustersystemwarteschlangen, in denen Informationen über den Cluster aufbewahrt werden, werden nicht gemeinsam genutzt. Jeder Warteschlangenmanager hat seine eigene.

Clusterkanäle werden nicht nur zum Übertragen von Anwendungsnachrichten, sondern auch von internen Systemnachrichten über die Konfiguration des Clusters verwendet. Jeder Warteschlangenmanager im Cluster muss diese internen Systemnachrichten empfangen, um ordnungsgemäß an der Clusterbildung teilnehmen zu können. Daher wird ein eigener CLUSRCVR-Kanal benötigt, auf dem diese Nachrichten empfangen werden können.

Ein gemeinsam genutzter CLUSRCVR kann auf jedem Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange (QSG) gestartet werden und so zu einer inkonsistenten Versorgung der internen Systemnachrichten mit den QSG-Warteschlangenmanagern führen, was bedeutet, dass keiner ordnungsgemäß an dem Cluster teilnehmen kann. Um sicherzustellen, dass keine gemeinsam genutzten CLUSRCVR-Kanäle verwendet werden können, schlägt jeder Versuch mit einer CSQX502E-Nachricht fehl.

Überlappende Cluster

Überlappende Cluster bieten zusätzliche Verwaltungsfunktionen. Verwenden Sie Namenslisten, um die Anzahl der Befehle zu reduzieren, die für die Verwaltung von überlappenden Clustern erforderlich sind.

Sie können Cluster erstellen, die sich überschneiden. Es gibt eine Reihe von Gründen für die Definition von überlappenden Clustern, z. B.:

- Damit andere Organisationen ihre eigene Verwaltung haben können.
- Damit unabhängige Anwendungen separat verwaltet werden können.
- Zum Erstellen von Serviceklassen.

In Abbildung 7 auf Seite 40 ist der Warteschlangenmanager STF2 ein Mitglied beider Cluster. Wenn ein Warteschlangenmanager Mitglied mehrerer Cluster ist, können Sie die Namenslisten nutzen, um die Anzahl der benötigten Definitionen zu reduzieren. Namelists enthalten eine Liste mit Namen, z. B. Clusternamen. Sie können eine Namensliste erstellen, die die Cluster benennt. Geben Sie die Namensliste im Befehl ALTER QMGR für STF2 an, um sie zu einem vollständigen Warteschlangenmanager-Repository für beide Cluster zu machen.

Wenn Sie mehr als einen Cluster in Ihrem Netzwerk haben, müssen Sie ihnen unterschiedliche Namen geben. Wenn zwei Cluster mit demselben Namen jemals zusammengeführt werden, ist es nicht möglich, sie wieder zu trennen. Es ist auch eine gute Idee, den Clustern und Kanälen unterschiedliche Namen zu geben. Sie lassen sich einfacher unterscheiden, wenn Sie die Ausgabe der DISPLAY-Befehle anzeigen. Die Namen von Warteschlangenmanagern müssen innerhalb eines Clusters eindeutig sein, damit sie ordnungsgemäß funktionieren.

Serviceklassen definieren

Stellen Sie sich eine Universität vor, die über einen Warteschlangenmanager für jedes Mitglied des Personals und jeden Schüler verfügt. Nachrichten zwischen Mitarbeitern sind auf Kanälen mit hoher Priorität und hoher Bandbreite zu bereisen. Nachrichten zwischen Studenten werden auf billigeren, langsameren Kanälen zu reisen. Sie können dieses Netz mit Hilfe der traditionellen Methoden zur verteilten Steuerung von Warteschlangen konfigurieren. IBM MQ wählt die Kanäle, die verwendet werden sollen, anhand der Namen von Zielwarteschlange und Warteschlangenmanager aus.

Um die Mitarbeiter und Studenten eindeutig zu unterscheiden, können Sie ihre Warteschlangenmanager in zwei Clustern gruppieren (siehe Abbildung 7 auf Seite 40). IBM MQ verschiebt Nachrichten in die Sitzungswarteschlange im Mitarbeitercluster nur über Kanäle, die in diesem Cluster definiert sind. Die Nachrichten für die Warteschlange 'gossip' im Cluster 'students' gehen über Kanäle, die in diesem Cluster definiert sind, und empfängt die entsprechende Serviceklasse.

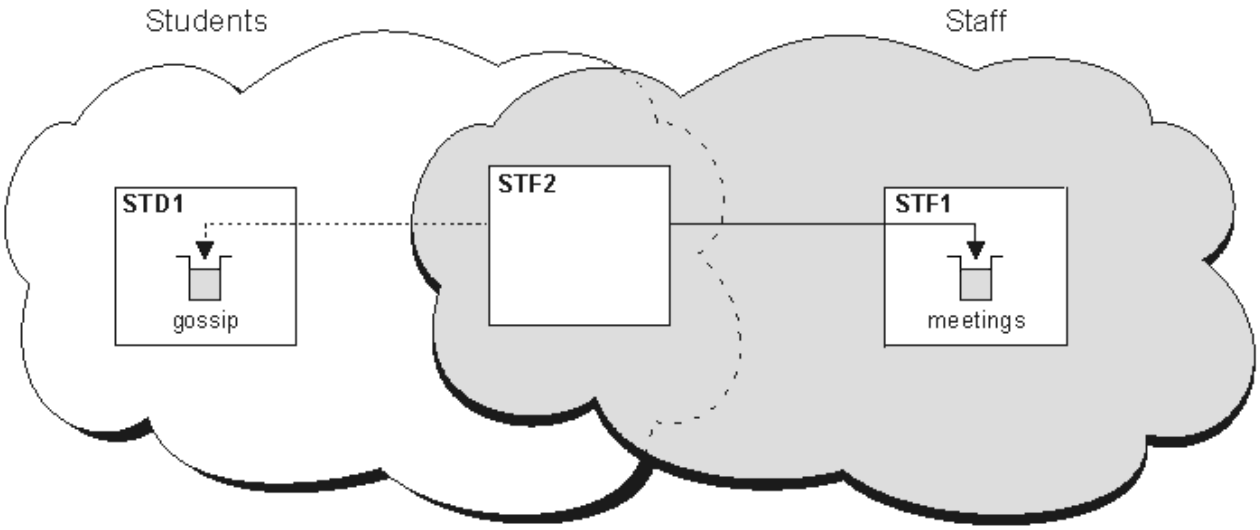


Abbildung 7. Serviceklassen

Tipps zum Clustering

Möglicherweise müssen Sie einige Änderungen an Ihren Systemen oder Anwendungen vornehmen, bevor Sie Clustering verwenden. Es gibt sowohl Ähnlichkeiten als auch Unterschiede zwischen dem Verhalten der verteilten Steuerung von Warteschlangen.

- Sie müssen manuelle Konfigurationsdefinitionen zu Warteschlangenmanagern außerhalb eines Clusters hinzufügen, damit sie auf Clusterwarteschlangen zugreifen können.
- Wenn Sie zwei Cluster mit demselben Namen zusammenführen, können Sie sie nicht erneut trennen. Daher ist es ratsam, allen Clustern einen eindeutigen Namen zu geben.
- Wenn eine Nachricht in einem Warteschlangenmanager ankommt, aber keine Warteschlange vorhanden ist, wird die Nachricht in die Warteschlange für dead-Mail gestellt. Wenn es keine Warteschlange für dead-letter gibt, schlägt der Kanal fehl und versucht erneut, die Warteschlange zu wiederholen. Die Verwendung der Warteschlange "dead-letter" ist mit der Verwendung der verteilten Steuerung von Warteschlangen identisch.
- Die Integrität persistenter Nachrichten wird beibehalten. Nachrichten werden aufgrund der Verwendung von Clustern nicht dupliziert oder gehen verloren.
- Die Verwendung von Clustern reduziert die Systemverwaltung. Cluster machen es einfach, größere Netzwerke mit vielen mehr WS-Managern zu verbinden, als Sie in der Lage wären, die verteilte Steuerung von Warteschlangen zu verwenden. Es besteht die Gefahr, dass Sie übermäßige Netzressourcen in Anspruch nehmen, wenn Sie versuchen, die Kommunikation zwischen jedem WS-Manager in einem Cluster zu aktivieren.
- Da IBM MQ Explorer die Warteschlangenmanager in einer Baumstruktur darstellt, kann die Ansicht sehr großer Cluster eventuell umständlich sein.
- Multi Der Zweck von Verteilerlisten besteht darin, einen einzelnen MQPUT -Befehl zu verwenden, um dieselbe Nachricht an mehrere Ziele zu senden. Verteilerliste werden von IBM MQ for Multiplatforms unterstützt. Sie können Verteilerlisten mit WS-Manager-Clustern verwenden. In einem Cluster werden alle Nachrichten zum Zeitpunkt MQPUT erweitert. Der Vorteil in Bezug auf den Datenaustausch im Netz ist nicht so hoch wie in einer Nicht-Clustering-Umgebung. Der Vorteil von Verteilerlisten besteht darin, dass die zahlreichen Kanäle und Übertragungswarteschlangen nicht manuell definiert werden müssen.
- Wenn Sie Cluster verwenden möchten, um die Auslastung Ihrer Workload zu überprüfen, untersuchen Sie Ihre Anwendungen. Sie können feststellen, ob Nachrichten von einem bestimmten Warteschlangenmanager oder in einer bestimmten Reihenfolge verarbeitet werden müssen. Solche Anwendungen sollen Nachrichtenaffinitäten haben. Möglicherweise müssen Sie Ihre Anwendungen ändern, bevor Sie sie in komplexen Clustern verwenden können.

- Sie können die Option MQOO_BIND_ON_OPEN in einem MQOPEN verwenden, um das Senden von Nachrichten an ein bestimmtes Ziel zu erzwingen. Wenn der Zielwarteschlangenmanager nicht verfügbar ist, werden die Nachrichten erst zugestellt, wenn der WS-Manager wieder verfügbar ist. Nachrichten werden aufgrund des Risikos der Duplizierung nicht an einen anderen WS-Manager weitergeleitet.
- Wenn ein WS-Manager ein Cluster-Repository hosten soll, müssen Sie seinen Hostnamen oder seine IP-Adresse kennen. Sie müssen diese Informationen im Parameter CONNAME angeben, wenn Sie die Definition CLUSSDR auf anderen Warteschlangenmanagern, die den Cluster verbinden, definieren. Wenn Sie DHCP verwenden, kann sich die IP-Adresse ändern, da DHCP bei jedem Neustart eines Systems eine neue IP-Adresse zuordnen kann. Daher dürfen Sie die IP-Adresse in den CLUSSDR -Definitionen nicht angeben. Selbst wenn alle CLUSSDR -Definitionen den Hostnamen und nicht die IP-Adresse angeben, sind die Definitionen immer noch nicht zuverlässig. DHCP aktualisiert nicht notwendigerweise den DNS-Verzeichniseintrag für den Host mit der neuen Adresse. Wenn Sie WS-Manager als vollständige Repositorys auf Systemen benennen müssen, die DHCP verwenden, installieren Sie die Software, die garantiert, dass Ihr DNS-Verzeichnis auf dem neuesten Stand ist.
- Verwenden Sie keine generischen Namen, z. B. generische VTAM-Ressourcen oder generische DDNS-Namen (Dynamic Domain Name Server) als Verbindungsnamen für Ihre Kanäle. Wenn dies der Fall ist, stellen die Kanäle möglicherweise eine Verbindung zu einem anderen Warteschlangenmanager her als erwartet.
- Sie können eine Nachricht nur aus einer lokalen Clusterwarteschlange abrufen, aber Sie können eine Nachricht in eine beliebige Warteschlange in einem Cluster stellen. Wenn Sie eine Warteschlange zur Verwendung des Befehls MQGET öffnen, öffnet der Warteschlangenmanager die lokale Warteschlange.
- Sie müssen keine Ihrer Anwendungen ändern, wenn Sie einen einfachen IBM MQ-Cluster einrichten. Die Anwendung kann die Zielwarteschlange im MQOPEN -Aufruf benennen und muss die Position des Warteschlangenmanagers nicht kennen. Wenn Sie einen Cluster für das Workload-Management einrichten, müssen Sie Ihre Anwendungen überprüfen und sie bei Bedarf ändern.
- Sie können die aktuellen Überwachungs-und Statusdaten für einen Kanal oder eine Warteschlange mit den Befehlen DISPLAY CHSTATUS und DISPLAY QSTATUS **runmqsc** anzeigen. Die Überwachungsdaten können verwendet werden, um die Leistung und den Status des Systems zu messen. Die Überwachung wird über WS-Manager-, Warteschlangen-und Kanalattribute gesteuert. Die Überwachung automatisch definierter Clustersenderkanäle ist mit dem WS-Manager-Attribut MONACLS möglich.

Zugehörige Konzepte

Cluster

„Vergleich von Clustering und verteilter Steuerung von Warteschlangen” auf Seite 32
Vergleichen Sie die Komponenten, die für die Verbindung von WS-Managern mit verteilter Steuerung von Warteschlangen und Clustering definiert werden müssen.

Komponenten eines Clusters

Zugehörige Tasks

WS-Manager-Cluster konfigurieren

Neuen Cluster einrichten

Wie lange werden die Informationen in den Warteschlangenmanager-Repositorys aufbewahrt?

WS-Manager-Repositorys behalten Informationen für 30 Tage bei. Ein automatischer Prozess aktualisiert die Informationen, die gerade verwendet werden, effizient.

Wenn ein Warteschlangenmanager einige Informationen über sich selbst sendet, speichern die vollständigen und partiellen Repository-WS-Manager die Informationen für 30 Tage. Informationen werden beispielsweise gesendet, wenn ein WS-Manager die Erstellung einer neuen Warteschlange bewirbt. Damit diese Informationen nicht auslaufen, werden die Warteschlangenmanager nach 27 Tagen automatisch alle Informationen über sich selbst erneut senden. Wenn ein Teilrepository eine neue Anforderung zum Teil über die 30-Tage-Lebensdauer sendet, bleibt die Ablaufzeit die ursprünglichen 30 Tage.

Wenn Informationen verfallen, wird sie nicht sofort aus dem Repository entfernt. Stattdessen wird sie für eine Karenzzeit von 60 Tagen gehalten. Wenn innerhalb der Karenzzeit keine Aktualisierung empfangen wird, werden die Informationen entfernt. Die Karenzzeit ermöglicht es, dass ein WS-Manager zum Ablauf-

datum vorübergehend außer Betrieb war. Wenn ein WS-Manager länger als 90 Tage von einem Cluster getrennt wird, wird er nicht mehr Teil des Clusters. Wenn er jedoch wieder eine Verbindung zum Netz herstellt, wird er wieder Teil des Clusters. Vollständige Repositorys verwenden keine Informationen, die abgelaufen sind, um neue Anforderungen von anderen Warteschlangenmanagern zu erfüllen.

Wenn ein Warteschlangenmanager eine Anforderung zum Sichern/Enddatum aus einem vollständigen Repository sendet, dauert die Anforderung ebenfalls 30 Tage. Nach 27 Tagen IBM MQ prüft die Anforderung. Wenn sie in den 27 Tagen referenziert wurde, wird sie automatisch aktualisiert. Ist dies nicht der Fall, bleibt sie verfallen und wird vom WS-Manager aktualisiert, wenn sie erneut benötigt wird. Das Ablaufen von Anforderungen verhindert eine Ansammlung von Anforderungen für Informationen von ruhenden WS-Managern.

Anmerkung: Sie sollten das PTF für APAR PH43191herunterladen und installieren, das Systemfehler bei der Berechnung der Ablaufzeit eines Abonnements behebt. Diese Fehler können dazu führen, dass die Subskription frühzeitig abläuft (was dazu führt, dass die Nachricht CSQX456I ausgegeben wird) oder nach Ablauf des Objekts abläuft (was zu Fehlern des Typs MQRC 2085 (MQRC_UNKNOWN_OBJECT) führt).

Bei großen Clustern kann es unterbrechend sein, wenn viele Warteschlangenmanager automatisch alle Informationen zu sich selbst erneut senden. Nähere Informationen hierzu erhalten Sie im Abschnitt Die Aktualisierung in einem großen Cluster kann sich auf die Leistung und Verfügbarkeit auswirken.

Zugehörige Konzepte

„Clustering: Best Practices für REFRESH CLUSTER verwenden” auf Seite 76
Sie verwenden den Befehl **REFRESH CLUSTER** , um alle lokal gespeicherten Informationen zu einem Cluster zu löschen und diese Informationen aus den vollständigen Repositorys im Cluster erneut zu erstellen. Sie sollten diesen Befehl nicht verwenden, außer in außergewöhnlichen Umständen. Wenn Sie es verwenden müssen, gibt es besondere Hinweise darauf, wie Sie es verwenden. Diese Informationen sind ein Leitfaden, der auf Tests und Feedback von Kunden basiert.

Beispielcluster

Das erste Beispiel zeigt den kleinsten möglichen Cluster von zwei Warteschlangenmanagern. Im zweiten und dritten Beispiel werden zwei Versionen eines drei WS-Manager-Clusters angezeigt.

Der kleinste mögliche Cluster enthält nur zwei WS-Manager. In diesem Fall enthalten beide WS-Manager vollständige Repositorys. Sie benötigen nur wenige Definitionen, um den Cluster zu konfigurieren, und dennoch gibt es bei jedem WS-Manager einen hohen Grad an Autonomie.

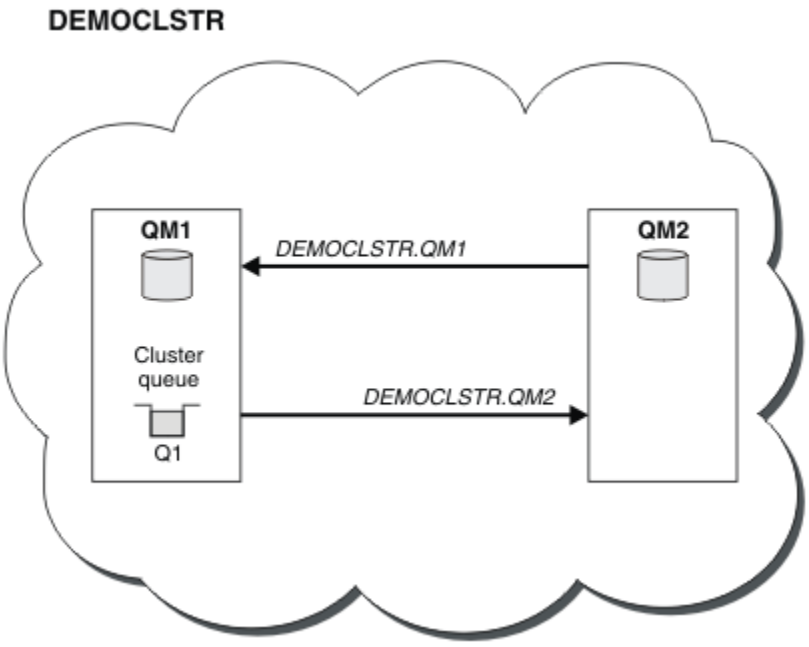


Abbildung 8. Kleiner Cluster mit zwei WS-Managern

- Die Warteschlangenmanager können lange Namen wie LONDON und NEWYORK aufweisen. z/OS In IBM MQ for z/OS dürfen Warteschlangenmanagernamen nur vier Zeichen haben.
- Jeder WS-Manager ist in der Regel auf einer separaten Maschine konfiguriert. Sie können jedoch mehrere WS-Manager auf derselben Maschine haben.

Anweisungen zum Konfigurieren eines ähnlichen Beispielclusters finden Sie im Abschnitt Neuen Cluster einrichten .

Abbildung 9 auf Seite 43 zeigt die Komponenten eines Clusters mit dem Namen CLSTR1.

- In diesem Cluster gibt es drei Warteschlangenmanager: QM1, QM2 und QM3.
- QM1 und QM2 Host-Repositorys mit Informationen zu allen Warteschlangenmanagern und clusterbezogenen Objekten im Cluster. Sie werden als *vollständige WS-Manager-Repository-Warteschlangenmanager* bezeichnet. Die Repositorys werden in dem Diagramm durch die schattierten Zylinder dargestellt.
- QM2 und QM3 enthalten einige Warteschlangen, auf die alle anderen Warteschlangenmanager im Cluster zugreifen können. Warteschlangen, die für alle anderen WS-Manager im Cluster zugänglich sind, werden als *Clusterwarteschlangen* bezeichnet. Die Clusterwarteschlangen werden in dem Diagramm durch die schraffierten Warteschlangen dargestellt. Auf Clusterwarteschlangen kann von einer beliebigen Position im Cluster aus zugegriffen werden. Mit dem IBM MQ-Clustering-Code wird sichergestellt, dass für Clusterwarteschlangen auf jedem Warteschlangenmanager, der auf sie verweist, entsprechende Definitionen für ferne Warteschlangen erstellt werden.

  Wie bei der verteilten Steuerung von Warteschlangen verwendet eine Anwendung den Aufruf MQPUT , um eine Nachricht in eine Clusterwarteschlange auf einem beliebigen Warteschlangenmanager im Cluster einzureihen. Eine Anwendung verwendet den Aufruf MQGET , um Nachrichten aus einer Clusterwarteschlange nur auf dem Warteschlangenmanager abzurufen, auf dem sich die Warteschlange befindet.
- Jeder Warteschlangenmanager verfügt über eine manuell erstellte Definition für das Empfangsende eines Kanals mit dem Namen *cluster_name. queue_manager_name*, auf dem Nachrichten empfangen werden können. Auf dem Empfangswarteschlangenmanager ist *cluster_name. queue_manager_name* ein Cluster-Empfängerkanal. Ein Clusterempfängerkanal ist wie ein Empfängerkanal, der in der verteilten Warteschlangensteuerung verwendet wird; er empfängt Nachrichten für den Warteschlangenmanager. Darüber hinaus erhält er auch Informationen über den Cluster.
-

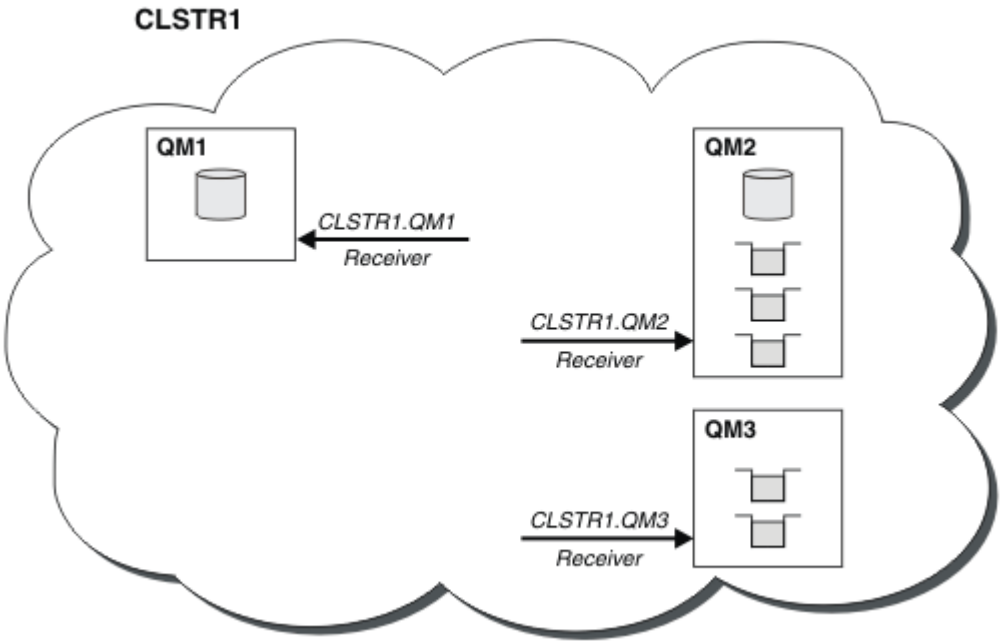


Abbildung 9. Warteschlangenmanagercluster

- In Abbildung 10 auf Seite 44 verfügt jeder Warteschlangenmanager auch über eine Definition für die Sendeseite des Kanals. Es stellt eine Verbindung zum Clusterempfängerkanal eines der vollständi-

gen WS-Manager-Repositorys her. Auf dem sendenden Warteschlangenmanager ist *cluster_name.queue_manager_name* ein Clustersenderkanal. QM1 und QM3 verfügen über Clustersenderkanäle, die eine Verbindung zu CLSTR1.QM2 herstellen, siehe gepunktete Linie "2".

QM2 verfügt über einen Clustersenderkanal, der mit CLSTR1.QM1 verbunden ist (siehe gepunktete Linie "3"). Ein Clustersenderkanal ist vergleichbar mit einem Senderkanal, wie er bei der verteilten Steuerung von Warteschlangen verwendet wird. Über ihn werden Nachrichten an den empfangenden Warteschlangenmanager gesendet. Darüber hinaus sendet er auch Informationen zum Cluster.

Wenn sowohl das Clusterempfängerende als auch das Clustersenderende eines Kanals definiert sind, wird der Kanal automatisch gestartet.

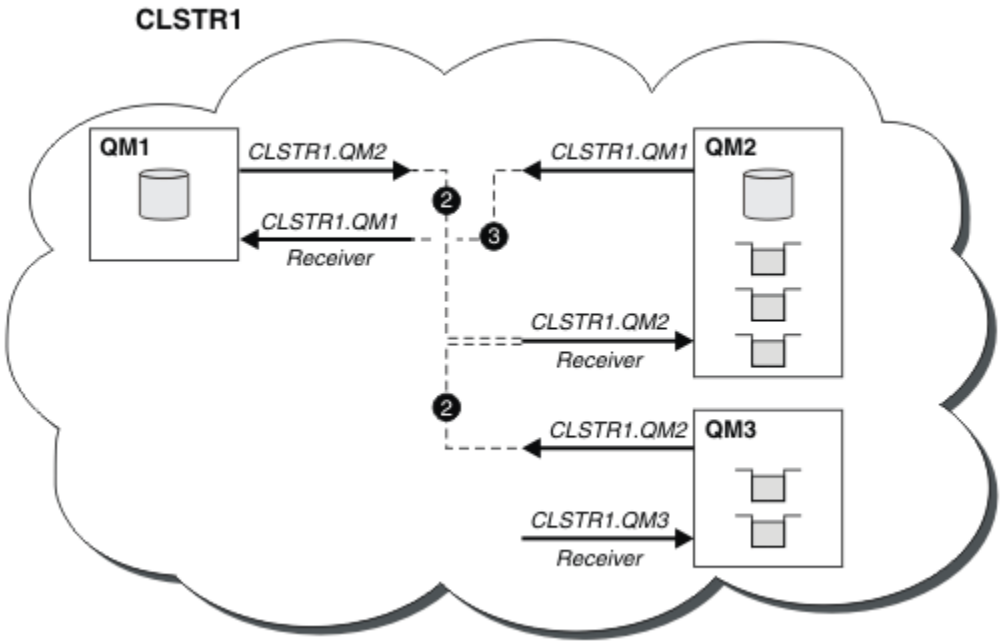


Abbildung 10. Ein Cluster von WS-Managern mit Senderkanälen

Wenn Sie einen Clustersenderkanal auf dem lokalen Warteschlangenmanager definieren, wird dieser Warteschlangenmanager zu einem der vollständigen WS-Manager-Repositorys eingeführt. Der vollständige Repository-WS-Manager aktualisiert die Informationen in seinem vollständigen Repository entsprechend. Anschließend erstellt es automatisch einen Clustersenderkanal zurück zum ursprünglichen Warteschlangenmanager und sendet diese WS-Manager-Informationen über den Cluster. Daher lernt ein WS-Manager über einen Cluster und ein Cluster lernt einen Warteschlangenmanager.

Sehen Sie sich Abbildung 9 auf Seite 43 noch einmal an. Angenommen, eine Anwendung, die mit dem Warteschlangenmanager QM3 verbunden ist, möchte einige Nachrichten an die Warteschlangen von QM2 senden. Wenn QM3 zum ersten Mal auf diese Warteschlangen zugreifen muss, erkennt es sie anhand eines vollständigen Repositorys. Das vollständige Repository ist in diesem Fall QM2, auf das über den Senderkanal CLSTR1.QM2 zugegriffen wird. Mit den Informationen aus dem Repository kann es automatisch ferne Definitionen für diese Warteschlangen erstellen. Wenn sich die Warteschlangen unter QM1 befinden, funktioniert dieser Mechanismus weiterhin, da QM2 ein vollständiges Repository ist. Ein vollständiges Repository verfügt über einen vollständigen Datensatz aller Objekte im Cluster. In diesem Fall würde QM3 auch automatisch einen Clustersenderkanal erstellen, der dem Clusterempfängerkanal unter QM1 entspricht, wodurch eine direkte Kommunikation zwischen den beiden Kanälen ermöglicht wird.

Abbildung 11 auf Seite 45 zeigt den gleichen Cluster mit den beiden automatisch erstellten Clustersenderkanälen. Die Clustersenderkanäle werden durch die beiden gestrichelten Linien dargestellt, die mit dem Clusterempfängerkanal CLSTR1.QM3verbunden sind. Außerdem wird die Clusterübertragungswarteschlange, SYSTEM.CLUSTER.TRANSMIT.QUEUE, angezeigt, die von QM1 zum Senden der Nachrichten verwendet wird. Alle WS-Manager im Cluster verfügen über eine Clusterübertragungswarteschlange, von

der aus sie Nachrichten an einen beliebigen anderen Warteschlangenmanager in demselben Cluster senden können.

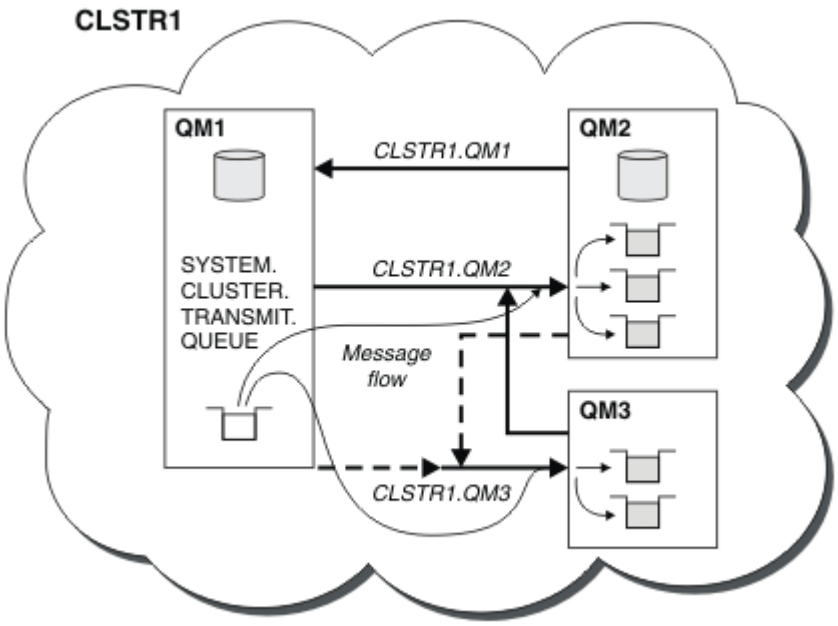


Abbildung 11. Ein Cluster von WS-Managern mit automatisch definierten Kanälen

Anmerkung: Andere Diagramme zeigen nur die Empfangsenden von Kanälen an, für die Sie manuelle Definitionen vornehmen. Die sendenden Enden werden weggelassen, da sie meist automatisch bei Bedarf definiert werden. Die automatische Definition der meisten Clustersenderkanäle ist entscheidend für die Funktion und die Effizienz von Clustern.

Zugehörige Konzepte

„Vergleich von Clustering und verteilter Steuerung von Warteschlangen” auf Seite 32
Vergleichen Sie die Komponenten, die für die Verbindung von WS-Managern mit verteilter Steuerung von Warteschlangen und Clustering definiert werden müssen.

Komponenten eines Clusters

Zugehörige Tasks

WS-Manager-Cluster konfigurieren

Neuen Cluster einrichten

Clustering: Bewährte Verfahren

Cluster stellen einen Mechanismus für die Verbindung von Warteschlangenmanagern bereit. Die in diesem Abschnitt beschriebenen bewährten Verfahren basieren auf Tests und Feedback von Kunden.

Für eine erfolgreiche Clusterkonfiguration sind eine gute Planung und umfassende Kenntnisse der Grundlagen von IBM MQ (z. B. ein gutes Anwendungsmanagement und ein durchdachter Netzentwurf) erforderlich. Stellen Sie sicher, dass Sie mit den Informationen in den zugehörigen Themen vertraut sind, bevor Sie fortfahren.

Zugehörige Konzepte

Verteilte Warteschlangen und Cluster

Cluster

Zugehörige Tasks

„Cluster entwerfen” auf Seite 25
Cluster bieten einen Mechanismus für die Verbindung von Warteschlangenmanagern in einer Weise, die sowohl die Erstkonfiguration als auch die laufende Verwaltung vereinfacht. Cluster müssen sorgfältig ent-

worfen werden, um sicherzustellen, dass sie ordnungsgemäß funktionieren, und dass sie die erforderliche Verfügbarkeit und Reaktionsfähigkeit erreichen.

Cluster überwachen

Clustering: Besondere Hinweise zu überlappenden Clustern
Dieser Abschnitt enthält eine Anleitung zur Planung und Verwaltung von IBM MQ-Clustern. Diese Informationen sind ein Leitfaden, der auf Tests und Feedback von Kunden basiert.

Clustereigentumsrecht

Machen Sie sich mit überlappenden Clustern vertraut, bevor Sie die folgenden Informationen lesen. Informationen zu den erforderlichen Informationen finden Sie in „Überlappende Cluster” auf Seite 39 und Nachrichtenpfade zwischen Clustern konfigurieren .

Wenn Sie ein System konfigurieren und verwalten, das sich aus überlappenden Clustern zusammensetzt, ist es am besten, die folgenden Schritte zu befolgen:

- Obwohl IBM MQ-Cluster wie oben beschrieben nur 'lose verbunden' sind, ist es sinnvoll, einen Cluster als eine einzige Verwaltungseinheit zu betrachten. Dieses Konzept wird verwendet, da die Interaktion zwischen Definitionen auf einzelnen Warteschlangenmanagern für das reibungslose Funktionieren des Clusters von entscheidender Bedeutung ist. Beispiel: Bei der Verwendung von auslastungsabhängigen Clusterwarteschlangen ist es wichtig, dass ein einzelner Administrator oder ein Team die vollständige Gruppe möglicher Destinations für Nachrichten versteht, die von den im Cluster verteilten Definitionen abhängig sind. Weitere triviale, Cluster-Sender-/Empfänger-Kanal-Paare müssen in der gesamten Konfiguration kompatibel sein.
- In Anbetracht dieses früheren Konzeptes, bei dem mehrere Cluster (die von separaten Teams/Einzelpersonen verwaltet werden sollen), ist es wichtig, klare Richtlinien für die Verwaltung der Gateway-Warteschlangenmanager zu haben.
- Es ist sinnvoll, überlappende Cluster als einen einzigen Namensbereich zu behandeln: Kanalnamen und WS-Manager-Namen müssen in einem einzigen Cluster eindeutig sein. Die Verwaltung ist viel einfacher, wenn sie in der gesamten Topologie eindeutig ist. Es empfiehlt sich, eine geeignete Namenskonvention zu verwenden. Mögliche Konventionen werden im Abschnitt „Namenskonventionen für Cluster” auf Seite 37beschrieben.
- Manchmal ist eine Zusammenarbeit zwischen Verwaltung und Systemmanagement unumgänglich: zum Beispiel die Zusammenarbeit zwischen Organisationen, die eigene Cluster besitzen, die sich überschneiden müssen. Ein klares Verständnis davon, wer welche besitzt, und durchsetzbare Regeln/Konventionen unterstützt das Clustering beim Zusammenfassen von Clustern.

Überlappende Cluster: Gateways

Im Allgemeinen ist ein einzelner Cluster einfacher zu verwalten als mehrere Cluster. Daher ist die Erstellung einer großen Anzahl von kleinen Clustern (eine für jede Anwendung zum Beispiel) etwas zu vermeiden, die im Allgemeinen.

Sie können jedoch überlappende Cluster implementieren, um Serviceklassen zur Verfügung zu stellen. For example:

- Wenn Sie konzentrische Cluster haben, bei denen der kleinere für Publish/Subscribe vorgesehen ist. Weitere Informationen hierzu finden Sie im Abschnitt Vorgehensweise bei der Größe von Systemen .
- Wenn einige Warteschlangenmanager von verschiedenen Teams verwaltet werden sollen. Weitere Informationen finden Sie im vorherigen Abschnitt „Clustereigentumsrecht” auf Seite 46.
- Wenn es aus organisatorischer oder geographischer Sicht sinnvoll ist.
- If equivalent clusters work with name resolution, for example when implementing TLS in an existing cluster.

Es gibt keine Sicherheitsleistung von überlappenden Clustern; die Möglichkeit, dass Cluster, die von zwei verschiedenen Teams verwaltet werden, sich überschneiden, verbindet sich effektiv mit den Teams und der Topologie. Beliebig:

- Der Name, der in einem solchen Cluster zugänglich gemacht wird, ist für den anderen Cluster zugänglich.
- Name, der in einem Cluster bekannt gemacht wird, kann in der anderen ausgeschrieben werden, um auswählbare Nachrichten abzuzeichnen.
- Nicht beworbenes Objekt in einem WS-Manager neben dem Gateway kann aus allen Clustern aufgelöst werden, in denen das Gateway ein Mitglied ist.

Der Namespace ist die Union der beiden Cluster und muss als einzelner Namensbereich behandelt werden. Daher wird das Eigentumsrecht an einem überlappenden Cluster von allen Administratoren beider Cluster gemeinsam genutzt.

Wenn ein System mehrere Cluster enthält, kann es erforderlich sein, Nachrichten von Warteschlangenmanagern in einem Cluster an Warteschlangen von Warteschlangenmanagern in einem anderen Cluster weiterzuleiten. In dieser Situation müssen die mehreren Cluster in irgendeiner Weise miteinander verbunden sein: Ein gutes Muster, das zu folgen ist, ist die Verwendung von Gateway-WS-Managern zwischen Clustern. Diese Anordnung verhindert die Erstellung eines schwer zu verwaltenden Netzes aus Punkt-zu-Punkt-Kanälen und stellt einen guten Platz bereit, um solche Probleme als Sicherheitsrichtlinien zu verwalten. Es gibt zwei verschiedene Möglichkeiten, diese Anordnung zu erreichen:

1. Platzieren Sie einen (oder mehrere) Warteschlangenmanager in beiden Clustern unter Verwendung einer zweiten Clusterempfängerdefinition. Diese Anordnung umfasst weniger Verwaltungsdefinitionen, bedeutet aber, wie bereits erwähnt, bedeutet, dass das Eigentumsrecht an einem überlappenden Cluster von allen Administratoren beider Cluster gemeinsam genutzt wird.
2. Verbinden Sie einen Warteschlangenmanager in Cluster eins mit einem Warteschlangenmanager in Cluster zwei mithilfe von konventionellen Punkt-zu-Punkt-Kanälen.

In einem dieser Fälle können verschiedene Tools verwendet werden, um den Datenverkehr entsprechend weiterzuleiten. Insbesondere können Aliasnamen von Warteschlangen oder Warteschlangenmanagern verwendet werden, um in den anderen Cluster zu steuern. Ein Alias eines Warteschlangenmanagers mit leerer **RQMNAME**-Eigenschaft sorgt für einen erneuten Lastausgleich, wo er gewünscht ist.

Namenskonventionen für Cluster

Diese Informationen enthalten die vorherigen Anleitungen zu Namenskonventionen und die aktuelle Anleitung. Da die IBM MQ-Technologie laufend verbessert wird und Kunden Technologie in immer neuen Kontexten oder auf andere Art und Weise verwenden, müssen für diese Situationen neue Empfehlungen und Informationen bereitgestellt werden.

Namenskonventionen für Cluster: Vorherige Anleitung

Wenn Sie einen neuen Cluster einrichten, sollten Sie eine Namenskonvention für die WS-Manager in Betracht ziehen. Jeder WS-Manager muss einen anderen Namen haben, aber er kann Ihnen dabei helfen, sich daran zu erinnern, wo die Warteschlangenmanager gruppiert sind, wenn Sie ihnen eine Gruppe ähnlicher Namen geben.

Jeder Clusterempfängerkanal muss ebenfalls einen eindeutigen Namen haben.

Wenn Sie mehrere Kanäle zum selben Warteschlangenmanager haben, die jeweils unterschiedliche Prioritäten aufweisen oder unterschiedliche Protokolle verwenden, können Sie die Namen erweitern, um die verschiedenen Protokolle einzuschließen, z. B. `QM1.S1`, `QM1.N3` und `QM1.T4`. In diesem Beispiel könnte `S1` der erste SNA-Kanal und `N3` der NetBIOS-Kanal mit der Netzpriorität 3 sein.

Das abschließende Qualifikationsmerkmal kann die Serviceklasse beschreiben, die vom Kanal bereitgestellt wird. Weitere Informationen hierzu finden Sie im Abschnitt Serviceklassen definieren .

Denken Sie daran, dass alle Clustersenderkanäle denselben Namen wie der entsprechende Clusterempfängerkanal haben.

Verwenden Sie keine generischen Verbindungsnamen in Ihren Clusterempfängerdefinitionen. In IBM MQ for z/OS können Sie generische VTAM-Ressourcen oder generische DDNS-Namen (*Dynamic Domain Name Server*) definieren. Doch wenn Sie Cluster verwenden, sollten Sie dies nicht tun. Wenn Sie einen

CLUSRCVR mit einem generischen **CONNAME** definieren, besteht keine Garantie, dass Ihre CLUSSDR-Kanäle auf die von Ihnen beabsichtigten Warteschlangenmanager zeigen. Ihr anfänglicher CLUSSDR kann auf jeden Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange verweisen, nicht notwendigerweise auf einen Warteschlangenmanager, der ein vollständiges Repository enthält. Wenn ein Kanal in den Wiederholungsstatus wechselt, kann er außerdem eine Verbindung zu einem anderen WS-Manager mit demselben generischen Namen herstellen und der Nachrichtenfluss wird unterbrochen.

Namenskonventionen für Cluster: Aktuelle Anleitung

Die vorherige Anleitung im Abschnitt „Namenskonventionen für Cluster: Vorherige Anleitung" auf Seite 47 ist noch gültig. Die folgende Anleitung ist jedoch als Aktualisierung beim Entwurf neuer Cluster gedacht. Dieser aktualisierte Vorschlag stellt die Eindeutigkeit der Kanäle in mehreren Clustern sicher, so dass mehrere Cluster erfolgreich überlappt werden können. Da Warteschlangenmanager und Cluster Namen mit bis zu 48 Zeichen haben können und ein Kanalname auf 20 Zeichen begrenzt ist, muss beim Benennen von Objekten von Anfang an Sorgfalt verwendet werden, um zu vermeiden, dass die Namenskonvention in der Mitte eines Projekts geändert werden muss.

Wenn Sie einen neuen Cluster einrichten, sollten Sie eine Namenskonvention für die WS-Manager in Betracht ziehen. Jeder WS-Manager muss einen anderen Namen haben. Wenn Sie Warteschlangenmanagern in einem Cluster eine Gruppe ähnlicher Namen geben, kann es hilfreich sein, sich daran zu erinnern, wo die WS-Manager gruppiert sind.

Wenn Sie Kanäle definieren, müssen Sie daran denken, dass alle automatisch erstellten Clustersenderkanäle auf jedem WS-Manager im Cluster denselben Namen wie der entsprechende Clusterempfängerkanal haben, der auf dem empfangenden Warteschlangenmanager im Cluster konfiguriert ist, und muss daher eindeutig sein und im Cluster für die Administratoren dieses Clusters sinnvoll sein. Die Kanalnamen sind auf maximal 20 Zeichen begrenzt.

Eine Möglichkeit besteht darin, den Namen des WS-Managers zu verwenden, dem der Clustername vorangestellt ist. Beispiel: Wenn der Clustername CLUSTER1 lautet und die Warteschlangenmanager QM1, QM2 und dann Clusterempfängerkanäle sind, sind die Clusterempfängerkanäle CLUSTER1 .QM1, CLUSTER1 .QM2.

Sie können diese Konvention erweitern, wenn Kanäle unterschiedliche Prioritäten haben oder unterschiedliche Protokolle verwenden, beispielsweise `CLUSTER1.QM1.S1`, `CLUSTER1.QM1.N3` und `CLUSTER1.QM1.T4`. In diesem Beispiel könnte S1 der erste SNA-Kanal und N3 der NetBIOS-Kanal mit einer Netzpriorität von drei sein.

Ein finales Qualifikationsmerkmal kann die Serviceklasse beschreiben, die vom Kanal bereitgestellt wird.

Überlegungen zu IBM MQ for z/OS

z/OS

In IBM MQ for z/OS können Sie generische VTAM-Ressourcen oder generische DDNS-Namen (*Dynamic Domain Name Server*) definieren. Sie können Verbindungsnamen mit generischen Namen definieren. Wenn Sie jedoch eine Clusterempfängerdefinition erstellen, verwenden Sie keinen generischen Verbindungsnamen.

Das Problem bei der Verwendung generischer Verbindungsnamen für Clusterempfängerdefinitionen lautet wie folgt. Wenn Sie einen `CLUSRCVR` mit einem generischen `CONNAME` definieren, gibt es keine Garantie dafür, dass Ihre `CLUSSDR` -Kanäle auf die Warteschlangenmanager verweisen, die Sie beabsichtigen. Der ursprüngliche CLUSSDR-Kanal kann auf jeden Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange verweisen, nicht notwendigerweise auf einen Warteschlangenmanager, der ein vollständiges Repository enthält. Wenn ein Kanal erneut versucht, eine Verbindung herzustellen, kann er die Verbindung zu einem anderen WS-Manager mit demselben generischen Namen erneut herstellen, der den Nachrichtenfluss stört.

Clustering: Aspekte des Topologiedesigns
Dieser Abschnitt enthält eine Anleitung zur Planung und Verwaltung von IBM MQ-Clustern. Diese Informationen sind ein Leitfaden, der auf Tests und Feedback von Kunden basiert.

Wenn Sie darüber nachdenken, wo Benutzeranwendungen und interne Verwaltungsprozesse im Voraus lokalisiert werden sollen, können viele Probleme entweder vermieden oder zu einem späteren Zeitpunkt minimiert werden. Dieses Thema enthält Informationen zu Designentscheidungen, die die Leistung verbessern können, und vereinfachen die Verwaltungstasks als Clusterskalierungen.

- „Leistung der Clustering-Infrastruktur" auf Seite 49
- „Vollständige Repositorys" auf Seite 50
- „Sollen Anwendungen Warteschlangen in vollständigen Repositorys verwenden?" auf Seite 51
- „Kanaldefinitionen verwalten" auf Seite 51
- „Lastausgleich über mehrere Kanäle" auf Seite 52

Leistung der Clustering-Infrastruktur

Wenn eine Anwendung versucht, eine Warteschlange auf einem Warteschlangenmanager in einem Cluster zu öffnen, registriert der Warteschlangenmanager sein Interesse an den vollständigen Repositorys für diese Warteschlange, so dass er lernen kann, wo sich die Warteschlange im Cluster befindet. Alle Aktualisierungen an der Warteschlangenposition oder -konfiguration werden automatisch von den vollständigen Repositorys an den interessierten WS-Manager gesendet. Diese Registrierung von Interesse wird intern als Subskription bezeichnet (diese Subskriptionen sind nicht mit den IBM MQ-Subskriptionen identisch, die für Publish/Subscribe-Messaging in IBM MQ verwendet werden).

Alle Informationen zu einem Cluster durchlaufen jedes vollständige Repository. Vollständige Repositorys werden daher immer in einem Cluster für den Verwaltungsnachrichtenverkehr verwendet. Die hohe Auslastung der Systemressourcen bei der Verwaltung dieser Subskriptionen und die Übertragung dieser Nachrichten und die daraus resultierenden Konfigurationsnachrichten können zu einer erheblichen Auslastung der Clustering-Infrastruktur führen. Es gibt eine Reihe von Faktoren, die zu berücksichtigen sind, wenn sichergestellt wird, dass diese Last wo immer möglich verstanden und minimiert wird:

- Je mehr einzelne WS-Manager eine Clusterwarteschlange verwenden, umso mehr Subskriptionen sind im System vorhanden, wodurch der Verwaltungsaufwand bei Änderungen größer ist und interessierte Subskribenten benachrichtigt werden müssen, insbesondere auf den vollständigen WS-Managern des Repositorys. Eine Möglichkeit, den unnötigen Datenverkehr und die Auslastung des gesamten Repositorys zu minimieren, besteht darin, ähnliche Anwendungen (d. a. die Anwendungen, die mit denselben Warteschlangen arbeiten) mit einer kleineren Anzahl von Warteschlangenmanagern zu verbinden.
- Neben der Anzahl der Subskriptionen im System, die sich auf die Leistung auswirken, kann sich die Änderungsrate in der Konfiguration von Clusterobjekten auf die Leistung auswirken, z. B. die häufige Änderung einer Clusterwarteschlangenkonfiguration.
- Wenn ein Warteschlangenmanager Mitglied mehrerer Cluster ist (d. B. er Teil eines überlappenden Clustersystems ist), wird jedes Interesse, das in einer Warteschlange erstellt wird, zu einer Subskription für jeden Cluster, zu dem er gehört, auch dann, wenn dieselben Warteschlangenmanager die vollständigen Repositorys für mehr als einen der Cluster sind. Diese Anordnung erhöht die Belastung des Systems und ist ein Grund, zu überlegen, ob mehrere überlappende Cluster erforderlich sind, und nicht nur ein einzelner Cluster.
- Anwendungsnachrichtenverkehr (d. h. Nachrichten, die von IBM MQ-Anwendungen an die Clusterwarteschlangen gesendet werden), gehen nicht über die vollständigen Repositorys, um die Zielwarteschlangenmanager zu erreichen. Dieser Nachrichtenverkehr wird direkt zwischen dem Warteschlangenmanager, in dem die Nachricht in den Cluster eintritt, und dem Warteschlangenmanager, in dem die Clusterwarteschlange vorhanden ist, gesendet. Daher ist es nicht erforderlich, hohe Aufwandmengen an Anwendungsnachrichtenverkehr in Bezug auf die vollständigen WS-Manager-Repositorys zu berücksichtigen, es sei denn, die vollständigen WS-Manager-WS-Manager sind einer der beiden genannten WS-Manager. Aus diesem Grund wird empfohlen, vollständige WS-Manager-Repositorys nicht für Anwendungsnachrichtenverkehr in Clustern zu verwenden, in denen die Clustering-Infrastrukturbelastung von Bedeutung ist.

Vollständige Repositorys

Ein Repository ist eine Zusammenstellung von Informationen über die Warteschlangenmanager, die zu einem Cluster gehören. Ein Warteschlangenmanager, der über einen vollständigen Satz von Informationen über jeden Warteschlangenmanager im Cluster verfügt, besitzt ein vollständiges Repository. Weitere Informationen zu vollständigen Repositorys und Teilrepositorys finden Sie unter Cluster-Repository.

Vollständige Repositorys müssen auf Servern eingesetzt werden, die zuverlässig und so hoch wie möglich verfügbar sind und Single Points of Failure vermieden werden müssen. Das Clusterdesign muss immer über zwei vollständige Repositorys verfügen. Wenn ein vollständiges Repository nicht vorhanden ist, kann der Cluster trotzdem ausgeführt werden.

Details zu Aktualisierungen für Clusterressourcen, die von einem Warteschlangenmanager in einem Cluster erstellt werden, z. B. Clusterwarteschlangen, werden von diesem Warteschlangenmanager an die meisten in diesem Cluster an zwei vollständige Repositorys gesendet (oder zu einem Cluster, wenn nur ein vollständiger Warteschlangenmanager im Cluster vorhanden ist). Diese vollständigen Repositorys enthalten die Informationen und geben sie an alle WS-Manager im Cluster weiter, die ein Interesse daran haben (d. a. sie subskribieren). Um sicherzustellen, dass jedes Member des Clusters über eine Up-to-Data-Ansicht der Clusterressourcen verfügt, muss jeder WS-Manager in der Lage sein, mit mindestens einem vollständigen WS-Manager-Repository gleichzeitig zu kommunizieren.

Wenn ein Warteschlangenmanager aus irgendeinem Grund nicht mit vollständigen Repositorys kommunizieren kann, kann er im Cluster abhängig von seiner bereits zwischengespeicherten Informationsstufe für einen Zeitraum weiter funktionieren, aber es sind keine neuen Aktualisierungen oder der Zugriff auf zuvor nicht verwendete Clusterressourcen verfügbar.

Aus diesem Grund müssen Sie das Ziel haben, die beiden vollständigen Repositorys immer verfügbar zu halten. Diese Anordnung bedeutet jedoch nicht, dass extreme Maßnahmen ergriffen werden müssen, da der Cluster für eine kurze Zeit ohne vollständiges Repository ausreichend funktioniert.

Es gibt einen weiteren Grund, dass ein Cluster über zwei vollständige WS-Manager-Repository-WS-Manager verfügen muss, die nicht die Verfügbarkeit von Clusterinformationen sind: Dieser Grund besteht darin, sicherzustellen, dass die Clusterinformationen, die im vollständigen Repository-Cache gespeichert sind, an zwei Stellen zu Wiederherstellungszwecken vorhanden sind. Wenn nur ein vollständiges Repository vorhanden ist und seine Informationen zum Cluster verloren gehen, ist ein manueller Eingriff auf alle WS-Manager im Cluster erforderlich, damit der Cluster wieder funktionieren kann. Wenn jedoch zwei vollständige Repositorys vorhanden sind, weil die Informationen immer in zwei vollständigen Repositorys veröffentlicht und subskribiert werden, kann das Repository für fehlgeschlagene vollständige Repositorys mit dem Minimum an Aufwand wiederhergestellt werden.

- Es ist möglich, die Verwaltung von WS-Managern mit vollem Repository in einem zwei vollständigen Repository-Cluster-Design auszuführen, ohne die Benutzer des Clusters zu beeinträchtigen: Der Cluster funktioniert weiterhin mit nur einem Repository, so dass die Repositorys nach unten gebracht, die Wartung angewendet und ein weiteres Mal wieder gesichert werden kann. Selbst wenn ein Ausfall im zweiten vollständigen Repository vorhanden ist, wird die Ausführung von Anwendungen für mindestens drei Tage nicht beeinträchtigt.
- Es sei denn, es gibt einen guten Grund für die Verwendung eines dritten Repositorys, wie z. B. die Verwendung eines geographisch lokalen vollständigen Repositorys aus geographischen Gründen, die Verwendung der beiden Repository-Designs. Die Verwendung von drei vollständigen Repositorys bedeutet, dass Sie nie wissen, welche beiden derzeit verwendet werden, und es kann zu Verwaltungsproblemen kommen, die durch die Interaktionen zwischen mehreren Workload-Management-Parametern verursacht werden. Es wird nicht empfohlen, mehr als zwei vollständige Repositorys zu verwenden.
- Wenn Sie nach wie vor eine bessere Verfügbarkeit benötigen, sollten Sie die vollständigen WS-Manager-Repositorys als Multi-Instanz-Warteschlangenmanager oder plattformspezifische Hochverfügbarkeitsunterstützung verwenden, um die Verfügbarkeit zu verbessern.
- Sie müssen alle vollständigen WS-Manager-Repository-Warteschlangenmanager vollständig mit manuell definierten Clustersenderkanälen verbinden. Es ist besonders darauf zu achten, dass der Cluster aus einem vertretbaren Grund mehr als zwei vollständige Repositorys hat. In dieser Situation ist es oft möglich, einen oder mehrere Kanäle zu verpassen und dafür nicht sofort erkennbar zu sein. Wenn keine

vollständige Verbindung auftritt, treten häufig Probleme bei der Diagnose von Problemen auf. Sie sind schwer zu diagnostizieren, da einige vollständige Repositorys nicht alle Repositorydaten enthalten und daher in Abhängigkeit von den vollständigen Repositorys, zu denen sie eine Verbindung herstellen, zu Warteschlangenmanagern im Cluster mit unterschiedlichen Sichten des Clusters führt.

Sollen Anwendungen Warteschlangen in vollständigen Repositorys verwenden?

Ein vollständiges Repository ist in der meisten Hinsicht genau wie jeder andere Warteschlangenmanager, und es ist daher möglich, Anwendungswarteschlangen im vollständigen Repository zu hosten und Anwendungen direkt mit diesen WS-Managern zu verbinden. Sollen Anwendungen Warteschlangen in vollständigen Repositorys verwenden?

Die allgemein akzeptierte Antwort lautet "Nein?". Obwohl diese Konfiguration möglich ist, bevorzugen viele Kunden, diese Warteschlangenmanager für die Verwaltung des gesamten Repository-Cluster-Caches zu halten. Punkte, die bei der Entscheidung für eine der beiden Optionen zu berücksichtigen sind, werden hier beschrieben, aber letztendlich muss die Clusterarchitektur den besonderen Anforderungen der Umgebung gerecht werden.

- Upgrades: Um neue Clusterfunktionen in neuen Releases von IBM MQ nutzen zu können, müssen normalerweise zuerst ein Upgrade der Warteschlangenmanager mit vollständigem Repository in diesem Cluster durchführen. Wenn eine Anwendung im Cluster neue Funktionen verwenden möchte, kann es nützlich sein, die vollständigen Repositorys (und eine Teilmenge von Teilrepositorys) zu aktualisieren, ohne eine Reihe von kolokationsfähigen Anwendungen testen zu müssen.
- Wartung: Auf ähnliche Weise, wenn Sie eine dringende Wartung auf die vollständigen Repositorys anwenden müssen, können sie mit dem Befehl **REFRESH** erneut gestartet oder aktualisiert werden, ohne Anwendungen zu berühren.
- Leistung: Wenn Cluster wachsen und die Anforderungen an die vollständige Repository-Cluster-Cache-Wartung größer werden, verringert sich die Gefahr, dass die Anwendungsleistung durch Konkurrenzsituationen getrennt wird, die die Anwendungsleistung beeinträchtigen, da die Systemressourcen in Konflikt stehen.
- Hardwarevoraussetzungen: Normalerweise müssen vollständige Repositorys nicht besonders leistungsfähig sein, z. B. ist ein einfacher UNIX-Server mit einer erwartungsgemäß guten Verfügbarkeit ausreichend. Alternativ dazu muss bei sehr großen oder sich ständig verändernden Clustern die Leistung des gesamten Repository-Computers berücksichtigt werden.
- Softwarevoraussetzungen: Anforderungen sind in der Regel der Hauptgrund für die Auswahl von Anwendungs-Warteschlangen in einem vollständigen Repository. In einem kleinen Cluster kann die Kollokation eine Voraussetzung für weniger WS-Manager/Server über alle bedeuten.

Kanaldefinitionen verwalten

Selbst in einem einzigen Cluster können mehrere Kanaldefinitionen vorhanden sein, die mehrere Routen zwischen zwei Warteschlangenmanagern enthalten.

Es gibt manchmal einen Vorteil, parallele Kanäle in einem einzigen Cluster zu haben, aber diese Designentscheidung muss gründlich durchdacht werden; abgesehen von der Komplexität der Komplexität kann dieses Design dazu führen, dass Kanäle untergenutzt werden, die die Leistung verringern. Diese Situation tritt auf, da beim Testen normalerweise viele Nachrichten mit einer konstanten Rate gesendet werden, so dass die parallelen Kanäle vollständig verwendet werden. Bei real-world-Bedingungen eines nicht konstanten Nachrichtenstroms bewirkt der Lastausgleichsalgorithmus jedoch, dass die Leistung sinkt, wenn der Nachrichtenfluss von Kanal zu Kanal umgeschaltet wird.

Wenn ein Warteschlangenmanager mehreren Clustern angehört, besteht die Möglichkeit, eine einzelne Kanaldefinition mit einer Clusternamensliste zu verwenden, anstatt einen separaten CLUSRCVR -Kanal für jeden Cluster zu definieren. Diese Konfiguration kann jedoch später zu Verwaltungsschwierigkeiten führen. Dies kann beispielsweise der Fall sein, wenn TLS auf einen Cluster, aber nicht auf einen zweiten Cluster angewendet werden soll. Es ist daher vorzuziehen, separate Definitionen zu erstellen, und die in „Namenskonventionen für Cluster” auf Seite 37 vorgeschlagene Namenskonvention unterstützt dies.

Lastausgleich über mehrere Kanäle

Diese Informationen sind als ein fortgeschrittenes Verständnis des Subjektes gedacht. Die grundlegende Erläuterung zu diesem Thema (die vor der Verwendung der Informationen hier zu verstehen ist) finden Sie im Abschnitt Cluster für das Workload-Management verwenden , Lastausgleich in Clustern und Algorithmus für Clusterauslastungsmanagement .

Der Algorithmus für die Clusterauslastungsverwaltung stellt eine große Gruppe von Tools zur Verfügung, aber sie dürfen nicht alle zusammen verwendet werden, ohne dass die Funktionsweise und die Interaktion vollständig verstanden werden müssen. Es ist möglicherweise nicht sofort ersichtlich, wie wichtig die Kanäle für den Lastausgleich sind: Der Algorithmus für die Verarbeitung des Workload-Managements verhält sich so, als ob mehrere Cluster-Kanäle zu einem Warteschlangenmanager, der Eigner einer Clusterwarteschlange ist, als mehrere Instanzen dieser Warteschlange behandelt werden. Dieser Prozess wird im folgenden Beispiel ausführlicher erläutert:

1. Es gibt zwei Warteschlangenmanager, die eine Warteschlange in einem Cluster hosten: `QM1` und `QM2`.
2. Es gibt fünf Clusterempfängerkanäle für `QM1`.
3. Es gibt nur einen Clusterempfängerkanal für `QM2`.
4. Wenn **MQPUT** oder **MQOPEN** on `QM3` eine Instanz auswählt, ist es fünf Mal wahrscheinlicher, dass der Algorithmus die Nachricht an `QM1` sendet als an `QM2`.
5. Die Situation in Schritt 4 tritt auf, weil der Algorithmus sechs Optionen zur Auswahl vorsieht (5 + 1) und Round-Robin über alle fünf Kanäle auf `QM1` und den einzelnen Kanal auf `QM2`.

Eine weitere kluge Funktion besteht darin, dass IBM MQ selbst beim Einreihen von Nachrichten in eine Clusterwarteschlange, für die auf dem lokalen Warteschlangenmanager zufällig eine Instanz konfiguriert ist, den Status des lokalen Clusterempfängerkanals verwendet, um zu entscheiden, ob Nachrichten in die lokale Instanz der Warteschlange oder in ferne Instanzen der Warteschlange gestellt werden sollen. In diesem Szenario gilt Folgendes:

1. Beim Einreihen von Nachrichten sieht der Algorithmus für die Auslastungsverwaltung nicht die einzelnen Clusterwarteschlangen an, sondern die Clusterkanäle, die diese Ziele erreichen können.
2. Um die lokalen Zieladressen zu erreichen, werden die lokalen Empfängerkanäle in diese Liste aufgenommen (obwohl sie nicht zum Senden der Nachricht verwendet werden).
3. Wenn ein lokaler Empfängerkanal gestoppt wird, bevorzugt der Workload-Management-Algorithmus eine alternative Instanz bevorzugt, wenn die CLUSRCVR nicht gestoppt ist. Wenn mehrere lokale CLUSRCVR-Instanzen für das Ziel vorhanden sind und mindestens eine Instanz nicht gestoppt ist, bleibt die lokale Instanz berechtigt.

Clustering: Anwendungsisolation mit mehreren Clusterübertragungswarteschlangen
Sie können die Nachrichtenflüsse zwischen Warteschlangenmanagern in einem Cluster isolieren. Sie können Nachrichten, die von verschiedenen Clustersenderkanälen transportiert werden, in verschiedene Clusterübertragungswarteschlangen stellen. Sie können den Ansatz in einem einzelnen Cluster oder mit überlappenden Clustern verwenden. Das Thema enthält Beispiele und einige bewährte Verfahren, die Sie bei der Auswahl eines zu verwendenden Ansatzes führen.

Bei der Bereitstellung einer Anwendung können Sie entscheiden, welche IBM MQ-Ressourcen die Anwendung mit anderen gemeinsam nutzen soll und welche nicht. Es gibt eine Reihe von Typen von Ressourcen, die gemeinsam genutzt werden können, wobei die Haupttypen der Server selbst, der Warteschlangenmanager, die Kanäle und die Warteschlangen sind. Sie können Anwendungen mit weniger gemeinsam genutzten Ressourcen konfigurieren. Sie können separate Warteschlangen, Kanäle, Warteschlangenmanager oder sogar Server für einzelne Anwendungen zuordnen. Wenn Sie dies tun, wird die Gesamtsystemkonfiguration größer und komplexer. Die Verwendung von IBM MQ-Clustern reduziert die Komplexität der Verwaltung von mehr Servern, Warteschlangenmanagern, Warteschlangen und Kanälen, führt aber eine weitere gemeinsam genutzte Ressource ein, die Cluster-Übertragungswarteschlange `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Abbildung 12 auf Seite 54 ist eine Schicht aus einer großen IBM MQ-Implementierung, die die Bedeutung der gemeinsamen Nutzung von `SYSTEM.CLUSTER.TRANSMIT.QUEUE`veranschaulicht. Im Diagramm ist die Anwendung `Client App` mit dem Warteschlangenmanager `QM2` im Cluster `CL1` verbun-

den. Eine Nachricht von `Client App` wird von der Anwendung `Server App` verarbeitet. Die Nachricht wird von `Server App` aus der Clusterwarteschlange `Q1` auf dem Warteschlangenmanager `QM3` in `CLUSTER2`abgerufen. Da sich die Client- und Serveranwendungen nicht in demselben Cluster befinden, wird die Nachricht vom Gateway-Warteschlangenmanager `QM1` übertragen.

Der normale Weg zur Konfiguration eines Cluster-Gateways besteht darin, den Gateway-Warteschlangenmanager zu einem Mitglied aller Cluster zu machen. Auf dem Gateway-WS-Manager werden Clusteraliasnamen für Clusterwarteschlangen in allen Clustern definiert. Die Aliasnamen für Clusterwarteschlangen sind in allen Clustern verfügbar. Nachrichten, die an die Clusterwarteschlangenaliasnamen gestellt werden, werden über den Gateway-Warteschlangenmanager an ihr korrektes Ziel weitergeleitet. Der Gateway-Warteschlangenmanager reiht Nachrichten, die an die Aliase der Clusterwarteschlangen gesendet werden, in die allgemeine `SYSTEM.CLUSTER.TRANSMIT.QUEUE` unter `QM1` ein.

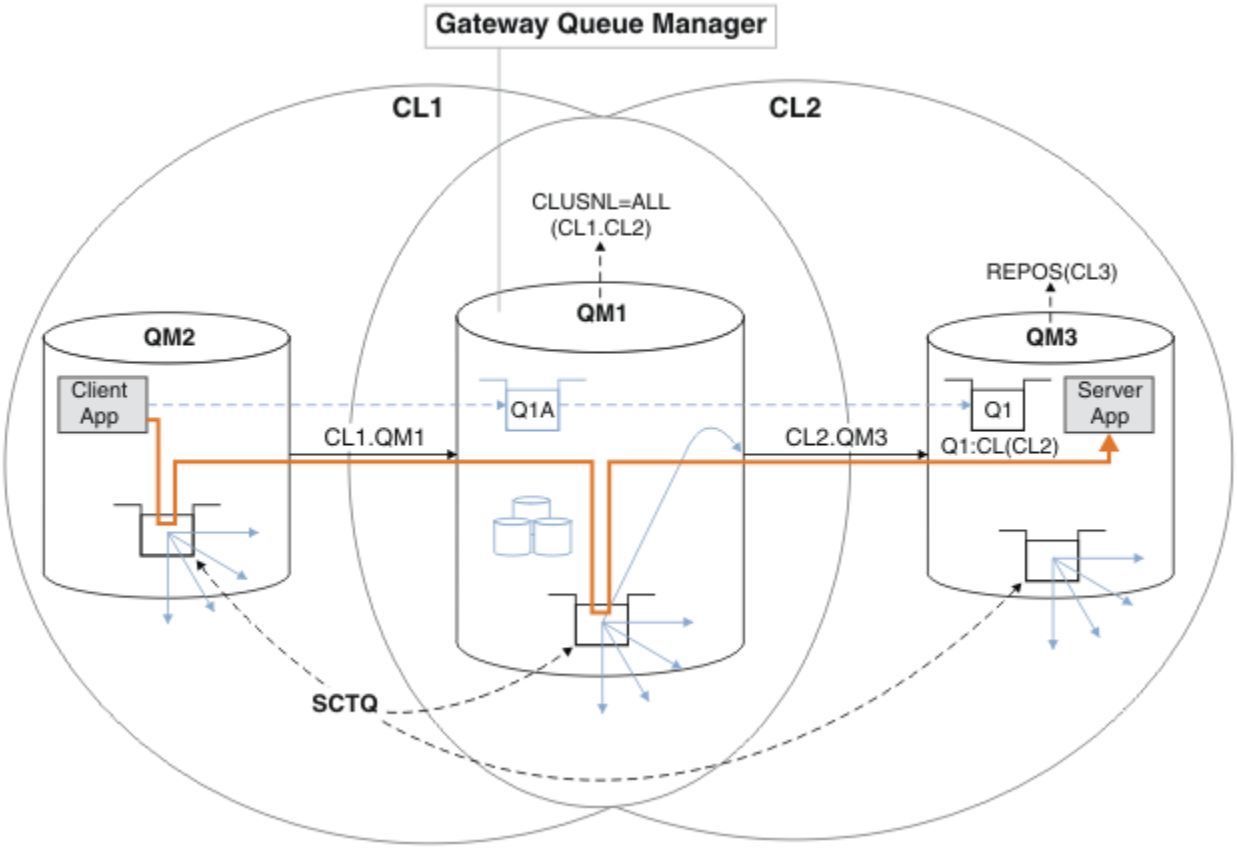
Die Hub-und Spoke-Architektur erfordert alle Nachrichten zwischen Clustern, die über den Gateway-Warteschlangenmanager übergeben werden. Das Ergebnis ist, dass alle Nachrichten durch die Warteschlange des einzelnen Clusters auf `QM1`, `SYSTEM.CLUSTER.TRANSMIT.QUEUE` fließen.

Aus einer Leistungsperspektive ist eine einzelne Warteschlange kein Problem. Eine allgemeine Übertragungswarteschlange stellt in der Regel keinen Leistungsengpass dar. Der Nachrichtendurchsatz auf dem Gateway wird weitgehend durch die Leistung der Kanäle bestimmt, die eine Verbindung zu ihm herstellen. Der Durchsatz wird in der Regel nicht von der Anzahl der Warteschlangen oder der Anzahl der Nachrichten in den Warteschlangen, die die Kanäle verwenden, beeinflusst.

Aus einigen anderen Perspektiven hat die Verwendung einer einzelnen Übertragungswarteschlange für mehrere Anwendungen Nachteile:

- Sie können den Fluss von Nachrichten nicht in ein Ziel vom Nachrichtenfluss zu einem anderen Ziel eingrenzen. Sie können die Speicherung von Nachrichten nicht trennen, bevor sie weitergeleitet werden, selbst wenn sich die Ziele in verschiedenen Clustern auf verschiedenen Warteschlangenmanagern befinden.

  Wenn eine Cluster-Destination nicht mehr verfügbar ist, werden Nachrichten für diese Zieladresse in der einzelnen Übertragungswarteschlange, und schließlich füllen sie die Nachrichten aus. Sobald die Übertragungswarteschlange voll ist, stoppt sie Nachrichten, die in die Übertragungswarteschlange für ein beliebtes Clusterziel gestellt werden.
- Es ist nicht einfach, die Übertragung von Nachrichten an verschiedene Cluster-Destinations zu überwachen. Alle Nachrichten befinden sich in der einzelnen Übertragungswarteschlange. Wenn Sie die Länge der Übertragungswarteschlange anzeigen, wird wenig darüber informiert, ob Nachrichten an alle Zieladressen übertragen werden.



Anmerkung: Die Pfeile in Abbildung 12 auf Seite 54 und die folgenden Abbildungen sind von unterschiedlichen Typen. Feste Pfeile stellen Nachrichtenflüsse dar. Bei den Beschriftungen auf festen Pfeilen handelt es sich um Nachrichtenkanalnamen. Die grauen ausgefüllten Pfeile sind potenzielle Nachrichtenflüsse von `SYSTEM.CLUSTER.TRANSMIT.QUEUE` auf Clustersenderkanälen. Schwarze gestrichelte Linien verbinden Beschriftungen mit ihren Zielen. Graue gestrichelte Pfeile sind Referenzen, z. B. von einem `MQOPEN` Aufruf von `Client` App an die Clusteraliaswarteschlangendefinition `Q1A`.

Abbildung 12. In Hub- und Spoke-Architektur mit IBM MQ-Clustern implementierte Client/Server-Anwendung

In Abbildung 12 auf Seite 54 öffnen Clients von `Server` App die Warteschlange `Q1A`. Nachrichten werden unter `QM2` in `SYSTEM.CLUSTER.TRANSMIT.QUEUE` eingereiht, unter `QM1` in `SYSTEM.CLUSTER.TRANSMIT.QUEUE` übertragen und anschließend unter `QM3` in `Q1` übertragen, wo sie von der Anwendung `Server` App empfangen werden.

Die Nachricht von `Client` App wird über die Clusterübertragungswarteschlangen des Systems durch `QM2` und `QM1`übergeben. In Abbildung 12 auf Seite 54 besteht das Ziel darin, den Nachrichtenfluss auf dem Gateway-Warteschlangenmanager von der Clientanwendung zu isolieren, damit seine Nachrichten nicht in `SYSTEM.CLUSTER.TRANSMIT.QUEUE` gespeichert werden. Sie können Flüsse auf einem der anderen Clusterwarteschlangenmanager isolieren. Sie können auch Flüsse in die andere Richtung isolieren, zurück an den Client. Um die Beschreibungen der Lösungen kurz zu halten, betrachten die Beschreibungen nur einen einzigen Nachrichtenfluss von der Clientanwendung.

Lösungen für die Isolierung des Clusternachrichtenverkehrs auf einem Cluster-Gateway-Warteschlangenmanager

Eine Möglichkeit, das Problem zu lösen, besteht darin, WS-Manager-Aliasnamen oder ferne Warteschlangendefinitionen zu verwenden, um eine Brücke zwischen Clustern zu schlagen. Erstellen Sie eine in Gruppen zusammengefasste ferne Warteschlangendefinition, eine Übertragungswarteschlange und einen Kanal, um die einzelnen Nachrichtenflüsse auf dem Gateway-Warteschlangenmanager zu trennen. Wei-

tere Informationen finden Sie im Abschnitt Definition einer fernen Warteschlange zum Isolieren von Nachrichten, die von einem Gateway-Warteschlangenmanager gesendet werden hinzufügen.

Ab IBM WebSphere MQ 7.5 sind Clusterwarteschlangenmanager nicht auf die Verwendung einer einzigen Clusterübertragungswarteschlange beschränkt. Sie haben zwei Möglichkeiten:

1. Definieren Sie zusätzliche Clusterübertragungswarteschlangen manuell, und definieren Sie, welche Clustersenderkanäle Nachrichten aus jeder Übertragungswarteschlange übertragen. Weitere Informationen finden Sie im Abschnitt Clustersendewarteschlange zum Isolieren des von einem Gateway-Warteschlangenmanager gesendeten Clusternachrichtenverkehrs hinzufügen .
2. Ermöglichen Sie dem WS-Manager, zusätzliche Clusterübertragungswarteschlangen automatisch zu erstellen und zu verwalten. Sie definiert eine andere Clusterübertragungswarteschlange für jeden Clustersenderkanal. Weitere Informationen finden Sie im Abschnitt Standardwert in separate Clusterübertragungswarteschlangen ändern, um den Nachrichtendatenverkehr zu isolieren .

Sie können manuell definierte Clusterübertragungswarteschlangen für einige Clustersenderkanäle kombinieren, wobei der Warteschlangenmanager den Rest verwaltet. Bei der Kombination von Übertragungswarteschlangen handelt es sich um den Ansatz, der im Abschnitt Clustersendungswarteschlange zum Isolieren des von einem Gateway-Warteschlangenmanager gesendeten Clusternachrichtenverkehrs hinzugefügt wird . In dieser Lösung verwenden die meisten Nachrichten zwischen Clustern `SYSTEM.CLUSTER.TRANSMIT.QUEUE` allgemein. Eine Anwendung ist kritisch, und alle ihre Nachrichtenflüsse werden von anderen Nachrichtenflüssen isoliert, indem eine manuell definierte Clusterübertragungswarteschlange verwendet wird.

Die Konfiguration im Abschnitt Clustersendungswarteschlange zum Isolieren von Clusternachrichtenverkehr, die von einem Gateway-Warteschlangenmanager gesendet werden, wird begrenzt hinzugefügt ist begrenzt. Der Nachrichtendatenverkehr, der in eine Clusterwarteschlange auf demselben WS-Manager in demselben Cluster wie eine andere Clusterwarteschlange läuft, wird nicht getrennt. Sie können den Nachrichtenverkehr mit Hilfe der Definitionen der fernen Warteschlange, die Teil der verteilten Steuerung von Warteschlangen sind, in einzelne Warteschlangen aufteilen. Bei Clustern, die mehrere Clusterübertragungswarteschlangen verwenden, können Sie den Nachrichtenverkehr trennen, der zu verschiedenen Clustersenderkanälen führt. Mehrere Clusterwarteschlangen im selben Cluster teilen sich auf demselben Warteschlangenmanager einen Clustersenderkanal gemeinsam. Nachrichten für diese Warteschlangen werden in derselben Übertragungswarteschlange gespeichert, bevor sie vom Gateway-WS-Manager weitergeleitet werden. In der Konfiguration unter Cluster-und Clustersendewarteschlange zum Isolieren des von einem Gateway-Warteschlangenmanager gesendeten Clusternachrichtenverkehrs hinzufügen wird die Einschränkung durch die Hinzufügung eines anderen Clusters und durch das Erstellen des WS-Managers und der Clusterwarteschlange zu einem Member des neuen Clusters abgestuft. Der neue Warteschlangenmanager kann der einzige WS-Manager im Cluster sein. Sie können dem Cluster weitere Warteschlangenmanager hinzufügen und denselben Cluster verwenden, um Clusterwarteschlangen auf diesen Warteschlangenmanagern zu isolieren.

Zugehörige Konzepte

„Zugriffssteuerung und mehrere Clusterübertragungswarteschlangen” auf Seite 31
Wählen Sie zwischen drei Prüfmodi aus, wenn eine Anwendung Nachrichten in ferne Clusterwarteschlangen einreiht. Die Modi sind: Prüfung über Fernzugriff gegen die Clusterwarteschlange, lokale Prüfung gegen `SYSTEM.CLUSTER.TRANSMIT.QUEUE` oder Prüfung gegen lokale Profile für die Clusterwarteschlange oder den Clusterwarteschlangenmanager.

Arbeiten mit Clusterübertragungswarteschlangen und Clustersenderkanälen

„Überlappende Cluster” auf Seite 39
Überlappende Cluster bieten zusätzliche Verwaltungsfunktionen. Verwenden Sie Namenslisten, um die Anzahl der Befehle zu reduzieren, die für die Verwaltung von überlappenden Clustern erforderlich sind.

Zugehörige Tasks

Berechtigung zum Einreihen von Nachrichten in ferne Clusterwarteschlangen berechtigen

Definition einer fernen Warteschlange hinzufügen, um Nachrichten zu isolieren, die von einem Gateway-Warteschlangenmanager gesendet wurden

Cluster-Übertragungswarteschlange zum Isolieren des Clusternachrichtenverkehrs hinzufügen, der von einem Gateway-Warteschlangenmanager gesendet wurde

Cluster und Cluster-Übertragungswarteschlange hinzufügen, um den Datenverkehr der Clusternachrichten zu isolieren, die von einem Gateway-Warteschlangenmanager gesendet werden

Ändern der Standardeinstellung in separate Clusterübertragungswarteschlangen, um den Nachrichtendatenverkehr zu isolieren

Erstellen von zwei überlappenden Clustern mit einem Gateway-Warteschlangenmanager

Nachrichtenpfade zwischen Clustern konfigurieren

Sicherung

Zugehörige Verweise

setmqaut

Clustering: Planung der Konfiguration von Clusterübertragungswarteschlangen
Sie werden durch die Auswahl von Clusterübertragungswarteschlangen geführt. Sie können eine gemeinsame Standardwarteschlange, separate Standardwarteschlangen oder manuell definierte Warteschlangen konfigurieren.

Vorbereitende Schritte

Lesen Sie den Abschnitt „Art der zu verwendenden Clusterübertragungswarteschlange auswählen” auf Seite 59.

Informationen zu diesem Vorgang

Wenn Sie planen, wie ein Warteschlangenmanager für die Auswahl einer Clusterübertragungswarteschlange konfiguriert werden soll, können Sie einige Optionen auswählen.

1. Was ist die Standard-Cluster-Übertragungswarteschlange für die Übertragung von Clusternachrichten?
   a. Eine allgemeine Clusterübertragungswarteschlange, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.
   b. Trennen Sie die Clusterübertragungswarteschlangen voneinander. Der WS-Manager verwaltet die separaten Clusterübertragungswarteschlangen. Sie werden als permanent dynamische Warteschlangen aus der Modellwarteschlange `SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE` erstellt. Er erstellt für jeden Clustersenderkanal, den er verwendet, eine Clusterübertragungswarteschlange.
2. Für die Clusterübertragungswarteschlangen, die Sie manuell erstellen möchten, haben Sie die folgenden beiden Möglichkeiten:
   a. Definieren Sie eine separate Übertragungswarteschlange für jeden Clustersenderkanal, den Sie manuell konfigurieren möchten. Setzen Sie in diesem Fall das Warteschlangenattribut **CLCHNAME** der Übertragungswarteschlange auf den Namen eines Clustersenderkanals. Wählen Sie den Clustersenderkanal aus, der Nachrichten aus dieser Übertragungswarteschlange übertragen soll.
   b. Kombinieren Sie den Nachrichtenverkehr für eine Gruppe von Clustersenderkanälen in derselben Clusterübertragungswarteschlange (siehe Abbildung 13 auf Seite 57). In diesem Fall setzen Sie das Warteschlangenattribut **CLCHNAME** jeder allgemeinen Übertragungswarteschlange auf den Namen eines generischen Clustersenderkanals. Ein generischer Clustersenderkanalname ist ein Filter zum Gruppieren von Namen von Clustersenderkanälen. Beispiel: `SALES.*` gruppiert alle Clustersenderkanäle, deren Namen mit `SALES.` beginnen. Sie können mehrere Platzhalterzeichen an einer beliebigen Position in der Filterzeichenfolge platzieren. Das Platzhalterzeichen ist ein Stern ("*"). Er steht für eine Zahl von null bis zu einer beliebigen Anzahl von Zeichen.

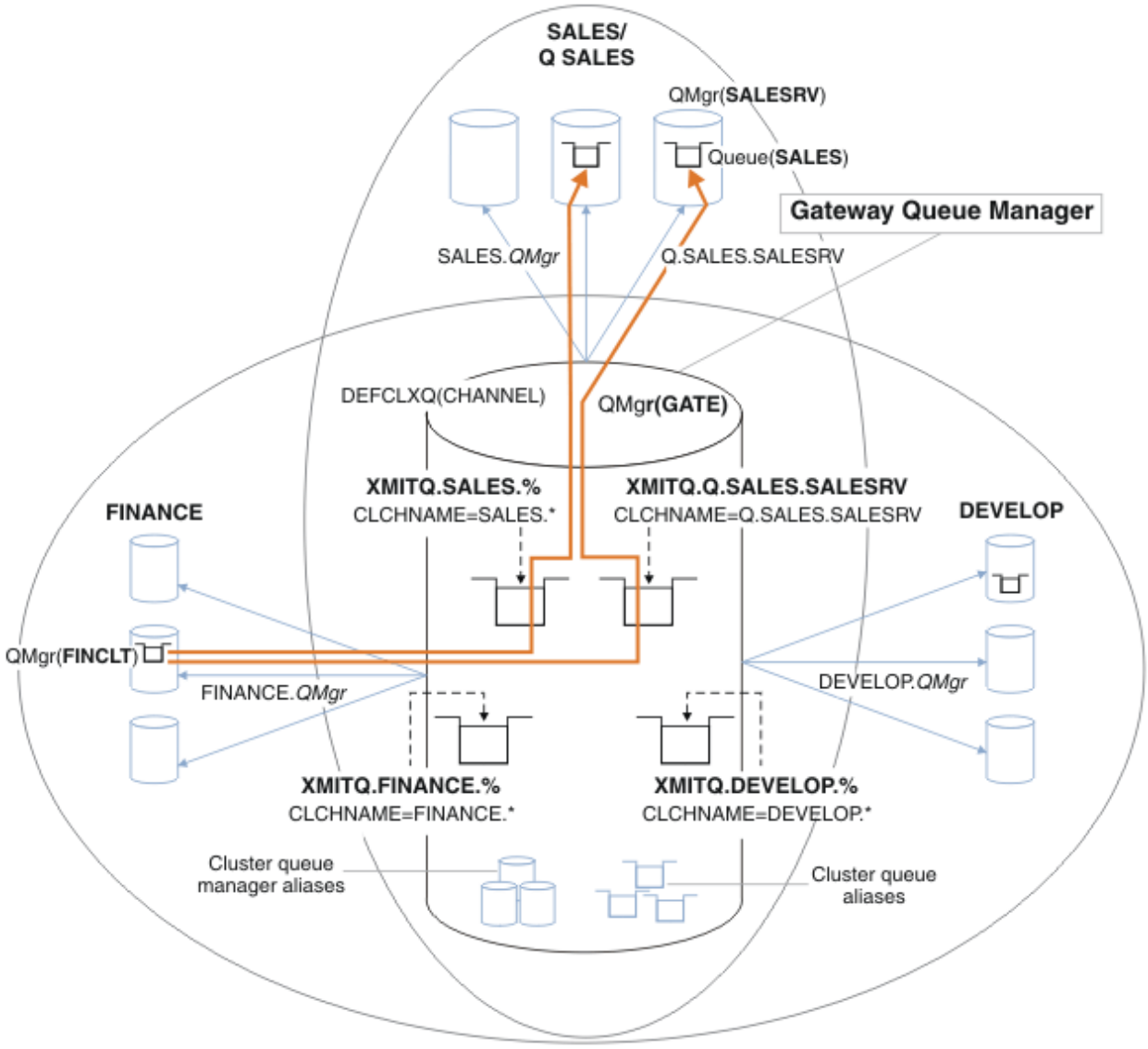


Abbildung 13. Beispiel für eigene Übertragungswarteschlangen für die verschiedenen IBM MQ-Abteilungscluster

Vorgehensweise

1. Wählen Sie den Typ der Standardübertragungswarteschlange für Cluster aus, die verwendet werden soll .
   - Wählen Sie eine einzelne Clusterübertragungswarteschlange oder separate Warteschlangen für jede Clusterverbindung aus.

   Übernehmen Sie die Standardeinstellung oder führen Sie den Befehl **MQSC** aus:

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

2. Isolieren Sie alle Nachrichtenflüsse, die keine Cluster-Übertragungswarteschlange mit anderen Flows gemeinsam nutzen dürfen .
   - Siehe „Clustering: Beispielkonfiguration mehrerer Clusterübertragungswarteschlangen” auf Seite 61. Im Beispiel ist die SALES-Warteschlange, die isoliert werden muss, ein Mitglied des SALES-Clusters unter SALESRV. Erstellen Sie zum Isolieren der SALES-Warteschlange einen neuen `Q.SA-`

LES-Cluster. Machen Sie den SALESRV-Warteschlangenmanager zu einem Mitglied und ändern die SALES-Warteschlange so, dass sie zu `Q.SALES` gehört.

- Warteschlangenmanager, die Nachrichten an SALES senden, müssen ebenfalls Mitglieder des neuen Clusters sein. Wenn Sie einen Clusterwarteschlangenaliasnamen und einen Gateway-Warteschlangenmanager verwenden, wie im Beispiel in vielen Fällen, können Sie die Änderungen begrenzen, um den Gateway-Warteschlangenmanager zu einem Mitglied des neuen Clusters zu machen.
- Durch die Trennung der Flüsse vom Gateway zum Ziel werden jedoch keine Flüsse in das Gateway vom Quellenwarteschlangenmanager getrennt. Aber es erweist sich manchmal als ausreichend, um die Abläufe vom Gateway zu trennen und nicht zum Gateway zu fließen. Wenn dies nicht ausreichend ist, fügen Sie den Quellenwarteschlangenmanager in den neuen Cluster ein. Wenn Nachrichten über das Gateway übertragen werden sollen, versetzen Sie den Clusteralias in den neuen Cluster, und senden Sie weiterhin Nachrichten an den Clusteralias auf dem Gateway und nicht direkt an den Ziel-WS-Manager.

Führen Sie die folgenden Schritte aus, um Nachrichtenflüsse zu isolieren:

a) Konfigurieren Sie die Ziele der Flows so, dass jede Zielwarteschlange die einzige Warteschlange in einem bestimmten Cluster ist, auf diesem Warteschlangenmanager .

b) Erstellen Sie die Cluster-Sender- und Clusterempfängerkanäle für alle neuen Cluster, die Sie nach einer systematischen Namenskonvention erstellt haben .

- Siehe „Clustering: Besondere Hinweise zu überlappenden Clustern” auf Seite 46.

c) Definieren Sie eine Clusterübertragungswarteschlange für jedes isolierte Ziel auf jedem Warteschlangenmanager, der Nachrichten an die Zielwarteschlange sendet.

- Eine Namenskonvention für Clusterübertragungswarteschlangen besteht darin, den Attributwert des Clusterkanalnamens `CLCHNAME` mit dem Präfix `XMITQ.` zu verwenden

3. Erstellen Sie Clusterübertragungswarteschlangen, um die Governance- oder Monitoring-Voraussetzungen zu erfüllen .

- Typische Governance-und Überwachungsanforderungen führen zu einer Übertragungswarteschlange pro Cluster oder einer Übertragungswarteschlange pro Warteschlangenmanager. Wenn Sie die Namenskonvention für Clusterkanäle (*`ClusterName.  QueueManagerName`*) befolgen, ist es einfach, generische Kanalnamen zu erstellen, die einen Cluster von Warteschlangenmanagern oder alle Cluster auswählen, zu denen ein Warteschlangenmanager gehört. (Siehe „Clustering: Beispielkonfiguration mehrerer Clusterübertragungswarteschlangen” auf Seite 61.)
- Erweitern Sie die Namenskonvention für Clusterübertragungswarteschlangen, um generische Kanalnamen zu verwenden, indem Sie das Sternsymbol durch ein Prozentzeichen ersetzen. Zum Beispiel:

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

Zugehörige Konzepte

Arbeiten mit Clusterübertragungswarteschlangen und Clustersenderkanälen

„Zugriffssteuerung und mehrere Clusterübertragungswarteschlangen” auf Seite 31
Wählen Sie zwischen drei Prüfmodi aus, wenn eine Anwendung Nachrichten in ferne Clusterwarteschlangen einreiht. Die Modi sind: Prüfung über Fernzugriff gegen die Clusterwarteschlange, lokale Prüfung gegen `SYSTEM.CLUSTER.TRANSMIT.QUEUE` oder Prüfung gegen lokale Profile für die Clusterwarteschlange oder den Clusterwarteschlangenmanager.

„Überlappende Cluster” auf Seite 39
Überlappende Cluster bieten zusätzliche Verwaltungsfunktionen. Verwenden Sie Namenslisten, um die Anzahl der Befehle zu reduzieren, die für die Verwaltung von überlappenden Clustern erforderlich sind.

Zugehörige Tasks

Definition einer fernen Warteschlange hinzufügen, um Nachrichten zu isolieren, die von einem Gateway-Warteschlangenmanager gesendet wurden

Cluster-Übertragungswarteschlange zum Isolieren des Clusternachrichtenverkehrs hinzufügen, der von einem Gateway-Warteschlangenmanager gesendet wurde

Cluster und Cluster-Übertragungswarteschlange hinzufügen, um den Datenverkehr der Clusternachrichten zu isolieren, die von einem Gateway-Warteschlangenmanager gesendet werden

Ändern der Standardeinstellung in separate Clusterübertragungswarteschlangen, um den Nachrichtendatenverkehr zu isolieren

Erstellen von zwei überlappenden Clustern mit einem Gateway-Warteschlangenmanager

Nachrichtenpfade zwischen Clustern konfigurieren

Art der zu verwendenden Clusterübertragungswarteschlange auswählen
Vorgehensweise zur Auswahl zwischen verschiedenen Konfigurationsoptionen für die Clusterübertragungswarteschlange.

Ab IBM WebSphere MQ 7.5 können Sie auswählen, welche Clusterübertragungswarteschlange einem Clustersenderkanal zugeordnet werden soll.

1. Sie können alle Clustersenderkanäle der einzigen standardmäßigen Clustersendewarteschlange SYSTEM.CLUSTER.TRANSMIT.QUEUE zuordnen. Diese Option ist die Standardeinstellung und ist die einzige Option für Warteschlangenmanager, die IBM WebSphere MQ 7.1 oder früher ausführen.
2. Sie können alle Clustersenderkanäle so festlegen, dass sie automatisch einer separaten Clusterübertragungswarteschlange zugeordnet werden. Die Warteschlangen werden vom Warteschlangenmanager aus der Modellwarteschlange SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE mit dem Namen SYSTEM.CLUSTER.TRANSMIT. *ChannelName* erstellt. Kanäle verwenden ihre eindeutig benannte Clusterübertragungswarteschlange, wenn das Warteschlangenmanagerattribut **DEFCLXQ** auf CHANNEL gesetzt ist.

   Achtung: Wenn Sie eine dedizierte SYSTEM.CLUSTER.TRANSMIT.QUEUES -Instanz mit einem Warteschlangenmanager verwenden, für den ein Upgrade von einer früheren Produktversion als IBM WebSphere MQ 7.5durchgeführt wurde, müssen Sie sicherstellen, dass für SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE die Option SHARE/NOSHARE auf **SHARE** gesetzt ist.
3. Sie können bestimmte Clustersenderkanäle festlegen, die von einer einzelnen Clusterübertragungswarteschlange bedient werden sollen. Wählen Sie diese Option aus, indem Sie eine Übertragungswarteschlange erstellen und ihr Attribut **CLCHNAME** auf den Namen des Clustersenderkanals einstellen.
4. Sie können Gruppen von Clustersenderkanälen auswählen, die von einer einzelnen Clusterübertragungswarteschlange bedient werden sollen. Wählen Sie diese Option aus, indem Sie eine Übertragungswarteschlange erstellen und ihr Attribut **CLCHNAME** auf einen generischen Kanalnamen wie *ClusterName*.* einstellen. Wenn Sie Clusterkanäle nach den Namenskonventionen in „Clustering: Besondere Hinweise zu überlappenden Clustern” auf Seite 46 benennen, wählt dieser Name alle Clusterkanäle aus, die mit Warteschlangenmanagern im Cluster *ClusterName* verbunden sind.

Sie können eine der Standardoptionen für die Clusterübertragungswarteschlange für einige Clustersenderkanäle mit einer beliebigen Anzahl spezifischer und generischer Cluster-Übertragungswarteschlangen-Konfigurationen kombinieren.

Bewährte Verfahren

In den meisten Fällen ist bei vorhandenen IBM MQ-Installationen die Standardkonfiguration die beste Wahl. Ein Clusterwarteschlangenmanager speichert Clusternachrichten in einer einzelnen Clusterübertragungswarteschlange, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Sie haben die Möglichkeit, den Standardwert zum Speichern von Nachrichten für verschiedene Warteschlangenmanager und verschiedene Cluster in separaten Übertragungswarteschlangen oder für die Definition eigener Übertragungswarteschlangen zu ändern.

In den meisten Fällen ist bei neuen IBM MQ-Installationen die Standardkonfiguration auch die beste Wahl. Der Prozess der Umschaltung von der Standardkonfiguration auf die alternative Standardkonfiguration mit einer Übertragungswarteschlange für jeden Clustersenderkanal erfolgt automatisch. Die Umschaltung erfolgt ebenfalls automatisch. Die Auswahl der einen oder der anderen ist nicht kritisch, Sie können sie umkehren.

Der Grund für die Auswahl einer anderen Konfiguration ist eher mit Governance und Management zu tun, als mit Funktionalität oder Leistung. Bei einigen Ausnahmebedingungen wird das Verhalten des

WS-Managers nicht von der Konfiguration mehrerer Clusterübertragungswarteschlangen unterstützt. Sie führt zu mehr Warteschlangen und erfordert, dass Sie die Überwachungs-und Managementprozeduren, die Sie bereits konfiguriert haben, ändern müssen, die sich auf die einzelne Übertragungswarteschlange beziehen. Aus diesem Grund ist der Rest der Standardkonfiguration die beste Wahl, es sei denn, Sie verfügen über starke Governance-oder Verwaltungsgründe für eine andere Auswahl.

Die Ausnahmen beziehen sich beide darauf, was passiert, wenn die Anzahl der in SYSTEM.CLUSTER.TRANSMIT.QUEUE gespeicherten Nachrichten zunimmt. Wenn Sie alle Schritte zum Trennen der Nachrichten für ein Ziel von den Nachrichten für ein anderes Ziel verwenden, sollten Kanal-und Zustellungsprobleme mit einem Ziel die Zustellung an ein anderes Ziel nicht beeinträchtigen. Die Anzahl der in SYSTEM.CLUSTER.TRANSMIT.QUEUE gespeicherten Nachrichten kann sich jedoch erhöhen, da Nachrichten nicht schnell genug an ein Ziel zugestellt werden. Die Anzahl der Nachrichten in SYSTEM.CLUSTER.TRANSMIT.QUEUE für ein Ziel kann sich auf die Zustellung von Nachrichten an andere Ziele auswirken.

Um Probleme zu vermeiden, die sich aus der Befüllung einer einzelnen Übertragungswarteschlange ergeben, sollten Sie genügend Kapazität in Ihrer Konfiguration aufbauen. Wenn dann ein Ziel fehlschlägt und ein Nachrichtenrückstand zu erstellen beginnt, haben Sie die Zeit, das Problem zu beheben.

Wenn Nachrichten über einen Hub-Warteschlangenmanager, z. B. ein Cluster-Gateway, weitergeleitet werden, nutzen sie eine gemeinsame Übertragungswarteschlange, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Wenn die Anzahl der in SYSTEM.CLUSTER.TRANSMIT.QUEUE auf dem Gateway-Warteschlangenmanager gespeicherten Nachrichten die maximale Länge erreicht, beginnt der Warteschlangenmanager, neue Nachrichten für die Übertragungswarteschlange zurückzuweisen, bis die Länge abnimmt. Die Überlastung wirkt sich auf Nachrichten für alle Ziele aus, die über das Gateway weitergeleitet werden. Nachrichten sichern die Übertragungswarteschlangen von anderen Warteschlangenmanagern, die Nachrichten an das Gateway senden. Das Problem manifestiert sich in Nachrichten, die in die Fehlerprotokolle des Warteschlangenmanagers geschrieben werden, den Nachrichtendurchsatz und die abgelaufenen Zeiten zwischen dem Senden einer Nachricht und dem Zeitpunkt, zu dem eine Nachricht an ihrem Zielort ankommt, länger verstrichen sind.

Die Auswirkungen von Überlastung auf eine einzelne Übertragungswarteschlange können sichtbar werden, auch bevor sie voll sind. Wenn Sie einen Mischnachrichtenverkehr mit einigen großen nicht persistenten Nachrichten und einigen kleinen Nachrichten haben, wird die Zeit, in der kleine Nachrichten gesendet werden, mit der Größe der Übertragungswarteschlange erhöht. Die Verzögerung ist darauf zurückzuführen, dass große nicht persistente Nachrichten auf Platte geschrieben werden, die normalerweise nicht auf Platte geschrieben werden. Wenn Sie zeitkritische Nachrichtenflüsse haben, die eine Cluster-Übertragungswarteschlange mit anderen gemischten Nachrichtenflüssen gemeinsam nutzen, könnte es sinnvoll sein, einen speziellen Nachrichtenpfad zu konfigurieren, um ihn von anderen Nachrichtenflüssen zu isolieren. Weitere Informationen finden Sie im Abschnitt Cluster-und Clustersendungswarteschlange zum Isolieren des Clusternachrichtenverkehrs, der von einem Gateway-Warteschlangenmanager gesendet wird , hinzufügen.

Die anderen Gründe für die Konfiguration getrennter Clusterübertragungswarteschlangen sind die Erfüllung der Governance-Anforderungen oder die Vereinfachung der Überwachung von Nachrichten, die an verschiedene Clusterziele gesendet werden. Möglicherweise müssen Sie beispielsweise nachweisen, dass Nachrichten für ein Ziel nie eine Übertragungswarteschlange mit Nachrichten für ein anderes Ziel gemeinsam nutzen.

Ändern Sie das Warteschlangenmanagerattribut **DEFCLXQ**, das die Standardclusterübertragungswarteschlange steuert, um für jeden Clustersenderkanal unterschiedliche Clusterübertragungswarteschlangen zu erstellen. Mehrere Ziele können einen Clustersenderkanal gemeinsam nutzen, sodass Sie Ihre Cluster so planen müssen, dass sie dieses Ziel vollständig erfüllen. Wenden Sie die Methode Cluster-und Clusterübertragungswarteschlange hinzufügen an, um den Clusternachrichtenverkehr, der von einem Gateway-Warteschlangenmanager gesendet wird, systematisch auf alle Ihre Clusterwarteschlangen zu isolieren. Das Ergebnis, das Sie anstreben, ist es, dass keine Cluster-Destination einen Clustersenderkanal mit einem anderen Clusterziel gemeinsam nutzen kann. Dies hat zur Folge, dass keine Nachricht für eine Cluster-Destination ihre Clusterübertragungswarteschlange mit einer Nachricht für ein anderes Ziel gemeinsam nutzt.

Wenn Sie eine separate Clusterübertragungswarteschlange für einen bestimmten Nachrichtenfluss erstellen, ist es einfach, den Nachrichtenfluss zu diesem Ziel zu überwachen. Wenn Sie eine neue Clusterübertragungswarteschlange verwenden möchten, definieren Sie die Warteschlange, ordnen Sie sie einem Clustersenderkanal zu, und stoppen Sie den Kanal und starten Sie ihn. Die Änderung muss nicht permanent sein. Sie können einen Nachrichtenfluss für eine Weile isolieren, die Übertragungswarteschlange überwachen und anschließend die Standardübertragungswarteschlange erneut verwenden.

Zugehörige Tasks

Clustering: Beispielkonfiguration mehrerer Clusterübertragungswarteschlangen
In dieser Task wenden Sie die Schritte zum Planen mehrerer Clusterübertragungswarteschlangen auf drei sich überlappende Cluster an. Die Anforderungen bestehen darin, Nachrichten von allen anderen Nachrichtenflüssen in eine Clusterwarteschlange zu trennen und Nachrichten für verschiedene Cluster in verschiedenen Clusterübertragungswarteschlangen zu speichern.

Clustering: Clusterübertragungswarteschlangen wechseln
Planen Sie, wie die Änderungen an den Clusterübertragungswarteschlangen eines vorhandenen Produktionswarteschlangenmanagers in Kraft gebracht werden.

Clustering: Beispielkonfiguration mehrerer Clusterübertragungswarteschlangen
In dieser Task wenden Sie die Schritte zum Planen mehrerer Clusterübertragungswarteschlangen auf drei sich überlappende Cluster an. Die Anforderungen bestehen darin, Nachrichten von allen anderen Nachrichtenflüssen in eine Clusterwarteschlange zu trennen und Nachrichten für verschiedene Cluster in verschiedenen Clusterübertragungswarteschlangen zu speichern.

Informationen zu diesem Vorgang

Die Schritte in dieser Übung zeigen, wie die Prozedur in „Clustering: Planung der Konfiguration von Clusterübertragungswarteschlangen” auf Seite 56 angewendet wird und die in Abbildung 14 auf Seite 62 gezeigte Konfiguration erreicht wird. Es ist ein Beispiel für drei sich überlappende Cluster mit einem Gateway-WS-Manager, der mit separaten Clusterübertragungswarteschlangen konfiguriert ist. Die MQSC-Befehle zum Definieren der Cluster werden in „Beispielcluster erstellen” auf Seite 64 beschrieben.

Für das Beispiel gibt es zwei Anforderungen. Eine davon ist die Trennung des Nachrichtenflusses vom Gateway-Warteschlangenmanager zu der Verkaufsanwendung, die die Verkäufe protokolliert. Der zweite Punkt ist die Abfrage, wie viele Nachrichten zu einem beliebigen Zeitpunkt darauf warten, an verschiedene Abteilbereiche gesendet zu werden. Die Cluster `SALES`, `FINANCE` und `DEVELOP` sind bereits definiert. Clusternachrichten werden derzeit von `SYSTEM.CLUSTER.TRANSMIT.QUEUE` weitergeleitet.

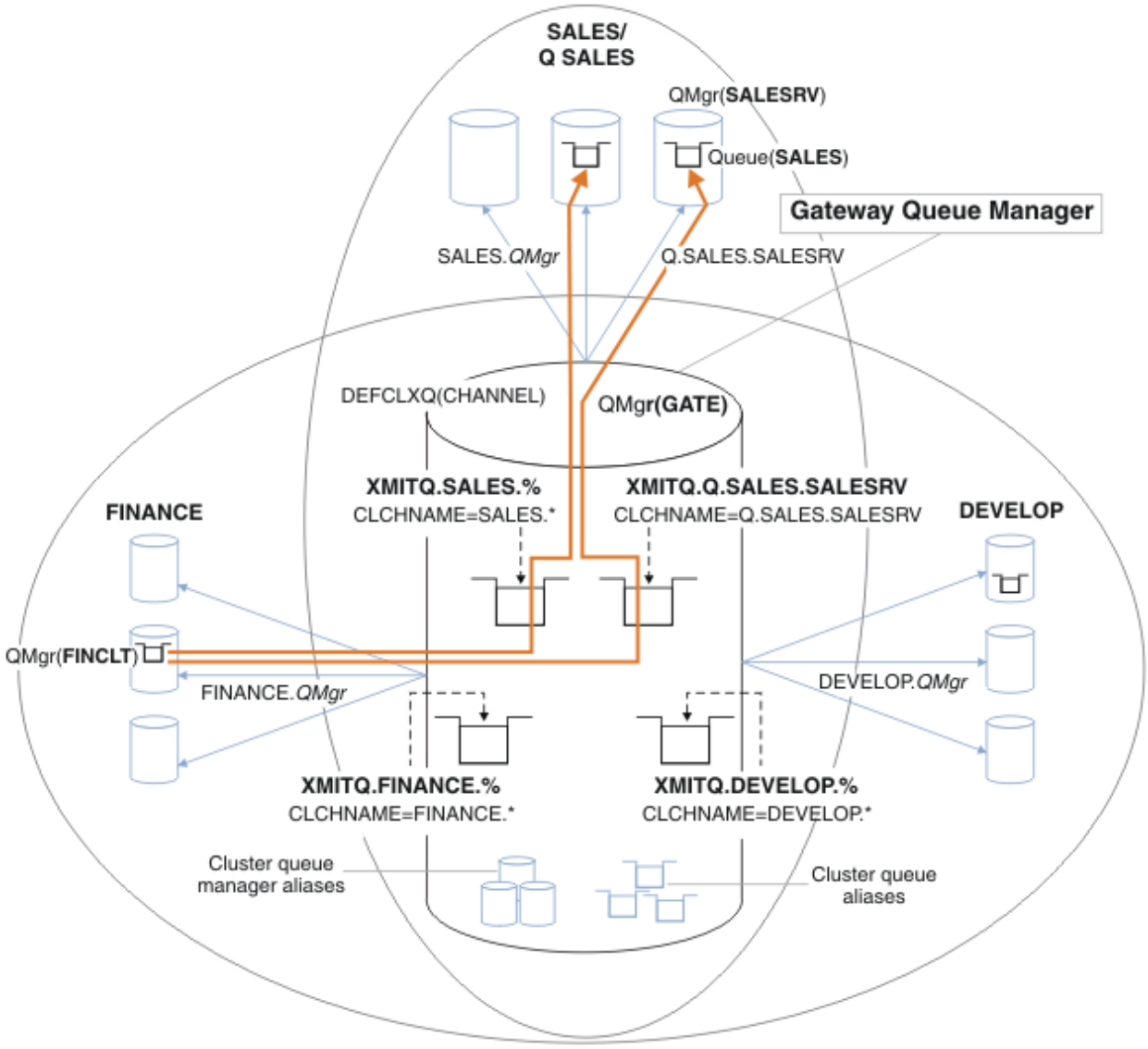


Abbildung 14. Beispiel für eigene Übertragungswarteschlangen für die verschiedenen IBM MQ-Abteilungscluster

Die Schritte zum Ändern der Cluster sind wie folgt: Informationen zu den Definitionen finden Sie unter Änderungen zum Isolieren der Vertriebswarteschlange in einem neuen Cluster und Trennen der Gateway-Clusterübertragungswarteschlangen .

Vorgehensweise

1. Der erste Konfigurationsschritt ist in " Wählen Sie den Typ der Standardübertragungswarteschlange für Cluster aus, die verwendet werden soll ".

   Die Entscheidung besteht darin, separate Standardclusterübertragungswarteschlangen zu erstellen, indem der folgende **MQSC** -Befehl auf dem GATE -Warteschlangenmanager ausgeführt wird.

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

   Es gibt keinen starken Grund für die Auswahl dieser Standardeinstellung, da die Clusterübertragungswarteschlangen manuell definiert werden sollen. Die Auswahl weist einen schwachen Diagnosewert auf. Wenn eine manuelle Definition falsch ausgeführt wird und eine Nachricht eine Standard-Cluster-Übertragungswarteschlange abfließt, wird sie in der Erstellung einer permanentdynamischen Clusterübertragungswarteschlange angezeigt.

2. Der zweite Konfigurationsschritt befindet sich in " Isolieren Sie alle Nachrichtenflüsse, die keine Cluster-Übertragungswarteschlange mit anderen Flows gemeinsam nutzen dürfen ".

   In diesem Fall muss die Vertriebsanwendung, die Nachrichten aus der Warteschlange SALES unter SALESRV empfängt, isoliert werden. Es ist nur die Isolation von Nachrichten vom Gateway-WS-Manager erforderlich. Die drei Unterschritte sind:

   a) " Konfigurieren Sie die Ziele der Flows so, dass jede Zielwarteschlange die einzige Warteschlange in einem bestimmten Cluster ist, auf diesem Warteschlangenmanager ".

      In diesem Beispiel muss der Warteschlangenmanager SALESRV einem neuen Cluster innerhalb der Vertriebsabteilung hinzugefügt werden. Wenn Sie nur wenige Warteschlangen haben, die isoliert werden müssen, können Sie entscheiden, einen bestimmten Cluster für die SALES-Warteschlange zu erstellen. Eine mögliche Namenskonvention für den Clusternamen ist es, solche `Q.` *`QueueName`*-Cluster beispielsweise mit `Q.SALES` zu benennen. Ein alternativer Ansatz, der praktischer ist, wenn Sie eine große Anzahl von Warteschlangen zu isolieren haben, besteht darin, Cluster von isolierten Warteschlangen zu erstellen, in denen und wann dies erforderlich ist. Die Clusternamen können `QUEUES.` *`n`* lauten.

      In diesem Beispiel heißt der neue Cluster `Q.SALES`. Informationen zum Hinzufügen des neuen Clusters finden Sie in den Definitionen unter Änderungen zum Isolieren der Vertriebswarteschlange in einem neuen Cluster und Trennen der Gateway-Clusterübertragungswarteschlangen. Die Zusammenfassung der Definitionsänderungen lautet wie folgt:

      i) Fügen Sie `Q.SALES` zur Namensliste der Cluster auf den Repository-Warteschlangenmanagern hinzu. Auf die Namensliste wird im Parameter **REPOSNL** des Warteschlangenmanagers verwiesen.

      ii) Fügen Sie `Q.SALES` zur Namensliste der Cluster auf dem Gateway-Warteschlangenmanager hinzu. Die Namensliste wird in allen Aliasnamendefinitionen der Clusterwarteschlange und des Cluster-WS-Managers auf dem Gateway-WS-Manager bezeichnet.

      iii) Erstellen Sie eine Namensliste auf dem Warteschlangenmanager SALESRV für beide Cluster, zu denen er gehört, und ändern Sie die Clusterzugehörigkeit der SALES-Warteschlange:

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

      Die SALES-Warteschlange ist ein Mitglied beider Cluster, aber nur für den Übergang. Sobald die neue Konfiguration ausgeführt wird, entfernen Sie die SALES-Warteschlange aus dem SALES-Cluster (siehe Abbildung 15 auf Seite 67).

   b) " Erstellen Sie die Cluster-Sender- und Clusterempfängerkanäle für alle neuen Cluster, die Sie nach einer systematischen Namenskonvention erstellt haben ".

      i) Fügen Sie den Clusterempfängerkanal `Q.SALES.` *`RepositoryQMgr`* zu jedem der Repository-Warteschlangenmanager hinzu

      ii) Fügen Sie den Clustersenderkanal `Q.SALES.` *`OtherRepositoryQMgr`* zu jedem der Repository-Warteschlangenmanager hinzu, um eine Verbindung zum anderen Repository-Manager herzustellen. Starten Sie diese Kanäle.

      iii) Fügen Sie die Clusterempfängerkanäle `Q.SALES.SALESRV` und `Q.SALES.GATE` einem der aktiven Repository-Warteschlangenmanager hinzu.

      iv) Fügen Sie die Clustersenderkanäle `Q.SALES.SALESRV` und `Q.SALES.GATE` den Warteschlangenmanagern SALESRV und GATE hinzu. Verbinden Sie den Clustersenderkanal mit dem Repository-WS-Manager, auf dem Sie die Clusterempfängerkanäle erstellt haben.

   c) " Definieren Sie eine Clusterübertragungswarteschlange für jedes isolierte Ziel auf jedem Warteschlangenmanager, der Nachrichten an die Zielwarteschlange sendet ".

Definieren Sie auf dem Gateway-Warteschlangenmanager die Clusterübertragungswarteschlange XMITQ.Q.SALES.SALESRV für den Q.SALES.SALESRV-Clustersenderkanal:

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

3. Der dritte Konfigurationsschritt ist in " Erstellen Sie Clusterübertragungswarteschlangen, um die Governance- oder Monitoring-Voraussetzungen zu erfüllen " enthalten.

   Definieren Sie auf dem Gateway-WS-Manager die Clusterübertragungswarteschlangen:

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

Nächste Schritte

Wechseln Sie in die neue Konfiguration auf dem Gateway-Warteschlangenmanager.

Der Switch wird ausgelöst, indem die neuen Kanäle gestartet werden, und die Kanäle, die jetzt verschiedenen Übertragungswarteschlangen zugeordnet sind, erneut gestartet werden. Alternativ können Sie den Gateway-WS-Manager stoppen und starten.

1. Stoppen Sie die folgenden Kanäle auf dem Gateway-WS-Manager:

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

2. Starten Sie die folgenden Kanäle auf dem Gateway-WS-Manager:

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

Wenn der Wechsel abgeschlossen ist, entfernen Sie die SALES-Warteschlange aus dem SALES-Cluster (siehe Abbildung 15 auf Seite 67).

Zugehörige Konzepte

Art der zu verwendenden Clusterübertragungswarteschlange auswählen
Vorgehensweise zur Auswahl zwischen verschiedenen Konfigurationsoptionen für die Clusterübertragungswarteschlange.

Zugehörige Tasks

Clustering: Clusterübertragungswarteschlangen wechseln
Planen Sie, wie die Änderungen an den Clusterübertragungswarteschlangen eines vorhandenen Produktionswarteschlangenmanagers in Kraft gebracht werden.

Beispielcluster erstellen
Die Definitionen und Anweisungen zum Erstellen des Beispielclusters und zum Ändern des Clusters, um die SALES-Warteschlange und separate Nachrichten auf dem Gateway-Warteschlangenmanager zu isolieren.

Informationen zu diesem Vorgang

Die vollständigen **MQSC** -Befehle zum Erstellen der FINANCE-, SALES-und Q.SALES -Cluster werden in Definitionen für die Basiscluster, Änderungen zum Isolieren der Vertriebswarteschlange in einem neuen Cluster und zum Trennen der Gateway-Clusterübertragungswarteschlangenund Entfernen der Vertriebswarteschlange auf dem Warteschlangenmanager SALESRV aus dem Vertriebsclusterbereitgestellt. Der DEVELOP -Cluster wird in den Definitionen nicht angegeben, um die Definitionen kürzer zu halten.

Vorgehensweise

1. Erstellen Sie die Cluster SALES und FINANCE und den Gateway-Warteschlangenmanager.
   a) Erstellen Sie die Warteschlangenmanager.

      Führen Sie den Befehl `crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE` *QmgrName* für jeden Warteschlangenmanagernamen in Tabelle 4 auf Seite 65 aus.

Tabelle 4. Namen und Portnummern des Warteschlangenmanagers		
Beschreibung	**Name des Warteschlangenmanagers**	**Portnummer**
Finanzrepository	FINR1	1414
Finanzrepository	FINR2	1415
Finanzclient	FINCLT	1418
Verkaufsrepository	SALER1	1416
Verkaufsrepository	SALER2	1417
Verkaufsserver	SALESRV	1419
Gateway	GATE	1420

   b) Alle WS-Manager starten

      Führen Sie den Befehl `strmqm` *QmgrName* für jeden Warteschlangenmanagernamen in Tabelle 4 auf Seite 65 aus.

   c) Erstellen Sie die Definitionen für jeden der Warteschlangenmanager.

      Führen Sie den Befehl `runmqsc` *QmgrName* < *filename* aus, wobei die Dateien in Definitionen für die Basisclusteraufgelistet sind und der Dateiname mit dem Namen des Warteschlangenmanagers übereinstimmt.

      Definitionen für die Basiscluster
      finr1.txt

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

      finr2.txt

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

      finclt.txt

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

saler1.txt

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

saler2.txt

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

salesrv.txt

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

gate.txt

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

2. Testen Sie die Konfiguration, indem Sie das Beispielanforderungsprogramm ausführen.
   a) Starten Sie das Auslösemonitorprogramm auf dem SALESRV-Warteschlangenmanager

      Öffnen Sie unter Windows ein Befehlsfenster und führen Sie den Befehl `runmqtrm -m SALESRV` aus

   b) Führen Sie das Beispielanforderungsprogramm aus, und senden Sie eine Anforderung.

      Öffnen Sie unter Windows ein Befehlsfenster und führen Sie den Befehl `amqsreq A.SALES FINCLT` aus

      Die Anforderungsnachricht wird zurückgemeldet, und nach 15 Sekunden wird das Beispielprogramm beendet.
3. Erstellen Sie die Definitionen, um die SALES-Warteschlange im `Q.SALES`-Cluster und separate Clusternachrichten für den SALES- und `FINANCE`-Cluster im Gateway-Warteschlangenmanager zu isolieren.

   Führen Sie den Befehl `runmqsc` *QmgrName* < *filename* aus, wobei die Dateien in der folgenden Liste aufgeführt sind und der Dateiname fast mit dem Namen des Warteschlangenmanagers übereinstimmt.

Änderungen zum Isolieren der Verkaufswarteschlange in einem neuen Cluster und Trennen der Gateway-Cluster-Übertragungswarteschlangen
chgsaler1.txt

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

chgsaler2.txt

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

chgsalesrv.txt

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

chggate.txt

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

4. Entfernen Sie die Warteschlange SALES aus dem SALES-Cluster.

   Führen Sie den Befehl **MQSC** in Abbildung 15 auf Seite 67 aus:

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

   Abbildung 15. Entfernen Sie die Verkaufswarteschlange auf dem WS-Manager SALESRV aus dem Vertriebscluster.

5. Schalten Sie die Kanäle in die neuen Übertragungswarteschlangen ein.

   Voraussetzung ist, dass alle Kanäle, die vom GATE-Warteschlangenmanager verwendet werden, gestoppt und gestartet werden. Stoppen und starten Sie den WS-Manager mit der geringsten Anzahl an Befehlen.

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

Nächste Schritte

1. Das Beispielanforderungsprogramm erneut ausführen, um die neue Konfiguration zu überprüfen. Siehe Schritt „2” auf Seite 66

2. Überwachen Sie die Nachrichten, die durch alle Clusterübertragungswarteschlangen auf dem GATE-Warteschlangenmanager fließen:
   a. Ändern Sie die Definition der einzelnen Clusterübertragungswarteschlangen, um die Warteschlangenüberwachung zu aktivieren.

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

   b. Überprüfen Sie, ob die Statistiküberwachung des Warteschlangenmanagers OFF ist, um die Ausgabe zu minimieren. Setzen Sie das Überwachungsintervall auf einen niedrigeren Wert, um mehrere Tests bequem auszuführen.

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

   c. Starten Sie den Warteschlangenmanager GATE erneut.
   d. Führen Sie das Beispielanforderungsprogramm einige Male aus, um sicherzustellen, dass eine gleiche Anzahl von Nachrichten durch SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SALESRV und SYSTEM.CLUSTER.TRANSMIT.QUEUE fließt. Anforderungen durchlaufen SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SALESRV und antworten über SYSTEM.CLUSTER.TRANSMIT.QUEUE.

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

   e. Die Ergebnisse in einigen Intervallen lauten wie folgt:

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

```
GetBytes: [435, 0]
...
MonitoringType: QueueStatistics
QueueManager: 'GATE'
IntervalStartDate: '2012-02-27'
IntervalStartTime: '15.00.20'
IntervalEndDate: '2012-02-27'
IntervalEndTime: '15.01.20'
CommandLevel: 700
ObjectCount: 2
QueueStatistics: 0
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.QUEUE'
CreateDate: '2012-02-24'
CreateTime: '15.58.15'
...
PutCount: [2, 0]
PutFailCount: 0
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [863, 0]
GetCount: [2, 0]
GetBytes: [863, 0]
...
QueueStatistics: 1
QueueName: 'SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV'
CreateDate: '2012-02-24'
CreateTime: '16.37.43'
...
PutCount: [2, 0]
PutFailCount: 0
Put1Count: [0, 0]
Put1FailCount: 0
PutBytes: [863, 0]
GetCount: [2, 0]
GetBytes: [863, 0]
...
2 Records Processed.
```

Eine Anforderungs-und Antwortnachricht wurde im ersten Intervall und zwei in der zweiten Nachricht gesendet. Sie können daraus schließen, dass die Anforderungsnachrichten auf SYSTEM.CLUSTER.TRANSMIT.Q.SALES.SAVESRV und die Antwortnachrichten auf SYSTEM.CLUSTER.TRANSMIT.QUEUE platziert wurden.

Clustering: Clusterübertragungswarteschlangen wechseln
Planen Sie, wie die Änderungen an den Clusterübertragungswarteschlangen eines vorhandenen Produktionswarteschlangenmanagers in Kraft gebracht werden.

Vorbereitende Schritte

Wenn Sie die Anzahl der Nachrichten reduzieren, die der Switching-Prozess in die neue Übertragungswarteschlange übertragen muss, wird der Wechsel schneller abgeschlossen. Lesen Sie den Abschnitt Wie der Prozess zum Umschalten des Clustersenderkanals in eine andere Übertragungswarteschlange funktioniert aus den Gründen, die versucht haben, die Übertragungswarteschlange zu leeren, bevor Sie fortfahren.

Informationen zu diesem Vorgang

Sie haben die Wahl zwischen zwei Möglichkeiten, die Änderungen an Clusterübertragungswarteschlangen wirksam zu machen.

1. Lassen Sie den WS-Manager die Änderungen automatisch vornehmen. Dies ist die Standardeinstellung. Der Warteschlangenmanager wechselt die Clustersenderkanäle mit anstehender Übertragungswarteschlange, wenn ein Clustersenderkanal als Nächstes gestartet wird.
2. Nehmen Sie die Änderungen manuell vor. Sie können die Änderungen an einem Clustersenderkanal vornehmen, wenn er gestoppt wird. Sie können sie von einer Clusterübertragungswarteschlange in eine andere übertragen, bevor der Clustersenderkanal gestartet wird.

Welche Faktoren berücksichtigen Sie bei der Entscheidung, welche der beiden Optionen Sie auswählen können, und wie verwalten Sie den Switch?

Prozedur

- Option 1: Lassen Sie den Warteschlangenmanager die Änderungen automatisch vornehmen (siehe „Aktive Clustersenderkanäle zu einer anderen Gruppe von Clusterübertragungswarteschlangen wechseln" auf Seite 71).

  Wählen Sie diese Option aus, wenn der WS-Manager den Switch für Sie herstellen soll.

  Eine alternative Möglichkeit, diese Option zu beschreiben, besteht darin, dass der Warteschlangenmanager einen Clustersenderkanal umschaltet, ohne dass der Kanal gestoppt werden muss. Sie haben die Möglichkeit, den Kanal zu zwingen, den Kanal zu stoppen und dann den Kanal zu starten, damit der Schalter früher passiert. Die Umschaltung wird gestartet, wenn der Kanal gestartet wird und er wird ausgeführt, während der Kanal aktiv ist, was sich von Option 2 unterscheidet. In Option 2 erfolgt die Umschaltung, wenn der Kanal gestoppt wird.

  Wenn Sie diese Option auswählen, indem Sie den Switch automatisch passieren lassen, wird der Umschaltvorgang gestartet, wenn ein Clustersenderkanal gestartet wird. Wenn der Kanal nicht gestoppt wird, wird er gestartet, wenn er inaktiv wird, wenn eine Nachricht zum Verarbeiten vorhanden ist. Wenn der Kanal gestoppt ist, starten Sie ihn mit dem Befehl `START CHANNEL`.
  Der Switchprozess wird beendet, sobald keine Nachrichten mehr für den Clustersenderkanal in der Übertragungswarteschlange übrig sind, die der Kanal bedient hat. Sobald dies der Fall ist, werden neu eingetrohtes Nachrichten für den Clustersenderkanal direkt in der neuen Übertragungswarteschlange gespeichert. Bis dahin werden Nachrichten in der alten Übertragungswarteschlange gespeichert, und der Switching-Prozess überträgt Nachrichten aus der alten Übertragungswarteschlange in die neue Übertragungswarteschlange. Der Clustersenderkanal leitet Nachrichten aus der neuen Clusterübertragungswarteschlange während des gesamten Switching-Prozesses weiter.
  Wenn der Switchprozess abgeschlossen ist, hängt vom Status des Systems ab. Wenn Sie die Änderungen in einem Wartungsfenster vornehmen, müssen Sie vorher prüfen, ob der Switching-Prozess in der Zeit abgeschlossen ist. Ob die Zeit vollständig abgeschlossen wird, hängt davon ab, ob die Anzahl der Nachrichten, die auf die Übertragung aus der alten Übertragungswarteschlange warten, null erreicht.

  Der Vorteil der ersten Methode ist, dass sie automatisch ist. Ein Nachteil besteht darin, dass Sie sicher sein müssen, dass Sie das System steuern können, um den Switchprozess im Wartungsfenster zu beenden, wenn die Konfigurationsänderungen auf ein Verwaltungsfenster beschränkt sind. Wenn Sie sich nicht sicher sein können, ist Option 2 möglicherweise eine bessere Wahl.
- Option 2: Nehmen Sie die Änderungen manuell vor („Gestoppten Clustersenderkanal in eine andere Clusterübertragungswarteschlange wechseln" auf Seite 72).

  Wählen Sie diese Option aus, wenn Sie den gesamten Switching-Prozess manuell steuern möchten oder ob Sie einen gestoppten oder inaktiven Kanal umschalten wollen. Es ist eine gute Wahl, wenn Sie einige Clustersenderkanäle umschalten und während eines Wartungsfensters den Switch ausführen möchten.

  Eine alternative Beschreibung dieser Option ist die Angabe, dass Sie den Clustersenderkanal umschalten, während der Clustersenderkanal gestoppt ist.

Wenn Sie diese Option auswählen, haben Sie die vollständige Kontrolle über den Zeitpunkt, an dem der Switch ausgeführt wird.

Sie können sicher sein, dass Sie den Switching-Prozess in einem festen Zeitraum in einem Wartungsfenster abschließen können. Der Zeitpunkt, zu dem der Switch ausgeführt wird, hängt davon ab, wie viele Nachrichten von einer Übertragungswarteschlange an die andere übertragen werden müssen. Wenn Nachrichten weiterhin ankommen, kann es zu einer Zeit dauern, bis der Prozess alle Nachrichten übertragen hat.

Sie haben die Möglichkeit, den Kanal zu wechseln, ohne Nachrichten aus der alten Übertragungswarteschlange zu übertragen. Der Switch ist " instant ".

Wenn Sie den Clustersenderkanal erneut starten, beginnt er mit der Verarbeitung von Nachrichten in der Übertragungswarteschlange, die Sie neu zugeordnet haben.

Der Vorteil der zweiten Methode besteht darin, dass Sie die Kontrolle über den Schaltvorgang haben. Der Nachteil besteht darin, dass Sie die zu vermittelnden Clustersenderkanäle identifizieren müssen, die erforderlichen Befehle ausführen und alle unbestäuben Kanäle auflösen müssen, die möglicherweise verhindern, dass der Clustersenderkanal gestoppt wird.

Zugehörige Konzepte

Art der zu verwendenden Clusterübertragungswarteschlange auswählen
Vorgehensweise zur Auswahl zwischen verschiedenen Konfigurationsoptionen für die Clusterübertragungswarteschlange.

Funktionsweise des Prozesses zum Wechseln des Clustersenderkanals in eine andere Übertragungswarteschlange

Zugehörige Tasks

Clustering: Beispielkonfiguration mehrerer Clusterübertragungswarteschlangen
In dieser Task wenden Sie die Schritte zum Planen mehrerer Clusterübertragungswarteschlangen auf drei sich überlappende Cluster an. Die Anforderungen bestehen darin, Nachrichten von allen anderen Nachrichtenflüssen in eine Clusterwarteschlange zu trennen und Nachrichten für verschiedene Cluster in verschiedenen Clusterübertragungswarteschlangen zu speichern.

Aktive Clustersenderkanäle zu einer anderen Gruppe von Clusterübertragungswarteschlangen wechseln
Mit dieser Task erhalten Sie drei Optionen zum Wechseln der aktiven Clustersenderkanäle. Eine Möglichkeit besteht darin, dass der WS-Manager den Switch automatisch macht, was die Ausführung von Anwendungen nicht beeinträchtigt. Die anderen Optionen sind zum manuellen Stoppen und Starten von Kanälen oder zum erneuten Starten des Warteschlangenmanagers.

Vorbereitende Schritte

Ändern Sie die Konfiguration der Clusterübertragungswarteschlange. Sie können das WS-Manager-Attribut **DEFCLXQ** ändern oder das Attribut **CLCHNAME** von Übertragungswarteschlangen hinzufügen oder ändern.

Wenn Sie die Anzahl der Nachrichten reduzieren, die der Switching-Prozess in die neue Übertragungswarteschlange übertragen muss, wird der Wechsel schneller abgeschlossen. Lesen Sie den Abschnitt Wie der Prozess zum Umschalten des Clustersenderkanals in eine andere Übertragungswarteschlange funktioniert aus den Gründen, die versucht haben, die Übertragungswarteschlange zu leeren, bevor Sie fortfahren.

Informationen zu diesem Vorgang

Verwenden Sie die Schritte in der Task als Basis für die Bearbeitung eines eigenen Plans für die Änderung der Konfiguration der Clusterübertragungswarteschlange.

Vorgehensweise

1. Optional: Aktualisieren Sie den aktuellen Kanalstatus

Erstellen Sie einen Datensatz mit dem Status der aktuellen und gespeicherten Kanäle, die Clusterübertragungswarteschlangen bedienen. Mit den folgenden Befehlen wird der Status angezeigt, der den Systemclusterübertragungswarteschlangen zugeordnet ist. Fügen Sie eigene Befehle hinzu, um den Status anzuzeigen, der den von Ihnen definierten Clusterübertragungswarteschlangen zugeordnet ist. Verwenden Sie eine Konvention, z. B. `XMITQ.` *`ChannelName`* verwendet werden, um Clusterübertragungswarteschlangen zu benennen, die Sie definieren, um die Anzeige des Kanalstatus für diese Übertragungswarteschlangen zu erleichtern.

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

2. Übertragungswarteschlangen wechseln.
   - Tun Sie nichts. Der Warteschlangenmanager wechselt beim Neustart die Clustersenderkanäle, wenn er nach dem Stoppen oder Inaktiv erneut gestartet wird.

     Wählen Sie diese Option aus, wenn Sie keine Regeln oder Bedenken zum Ändern einer Warteschlangenmanagerkonfiguration haben. Aktive Anwendungen sind von den Änderungen nicht betroffen.
   - Starten Sie den Warteschlangenmanager erneut. Alle Clustersenderkanäle werden bei Bedarf automatisch gestoppt und erneut gestartet.

     Wählen Sie diese Option aus, um alle Änderungen sofort einzuleiten. Aktive Anwendungen werden durch den Warteschlangenmanager unterbrochen, da er heruntergefahren und erneut gestartet wird.
   - Stoppen Sie einzelne Clustersenderkanäle, und starten Sie sie erneut.

     Wählen Sie diese Option aus, um ein paar Kanäle sofort zu ändern. Beim Ausführen von Anwendungen wird eine kurze Verzögerung bei der Nachrichtenübertragung zwischen dem Stoppen und dem erneuten Starten des Nachrichtenkanals angezeigt. Der Clustersenderkanal bleibt aktiv, außer während der Zeit, in der Sie ihn gestoppt haben. Während der Vermittlung werden Nachrichten an die alte Übertragungswarteschlange zugestellt, durch den Vermittlungsvorgang in die neue Übertragungswarteschlange übertragen und vom Clustersenderkanal aus der neuen Übertragungswarteschlange weitergeleitet.
3. Optional: Kanäle überwachen, während sie umschalten

   Zeigen Sie den Kanalstatus und die Übertragungswarteschlangentiefe während des Switchs an. Im folgenden Beispiel wird der Status der Übertragungswarteschlangen des Systemclusters angezeigt.

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

4. Optional: Überwachen Sie die Nachrichten AMQ7341 `Die Übertragungswarteschlange für den Kanal` *`ChannelName`*`, die von der Warteschlange` *`QueueName`* `in` *`QueueName`* umgeschaltet wurde, die in das Fehlerprotokoll des Warteschlangenmanagers geschrieben werden.

Gestoppten Clustersenderkanal in eine andere Clusterübertragungswarteschlange wechseln
Wenn Sie die Änderungen manuell vornehmen möchten, nehmen Sie die Änderungen an einem Clustersenderkanal vor, wenn er gestoppt ist, und übertragen ihn von einer Clusterübertragungswarteschlange in eine andere, bevor der Clustersenderkanal gestartet wird.

Vorbereitende Schritte

Sie können einige Konfigurationsänderungen vornehmen und sie jetzt wirksam werden lassen, ohne die betroffenen Clustersenderkanäle zu starten. Alternativ können Sie die Konfigurationsänderungen vornehmen, die Sie als einen der Schritte in der Task benötigen.

Wenn Sie die Anzahl der Nachrichten reduzieren, die der Switching-Prozess in die neue Übertragungswarteschlange übertragen muss, wird der Wechsel schneller abgeschlossen. Lesen Sie den Abschnitt Wie der Prozess zum Umschalten des Clustersenderkanals in eine andere Übertragungswarteschlange

funktioniert aus den Gründen, die versucht haben, die Übertragungswarteschlange zu leeren, bevor Sie fortfahren.

Informationen zu diesem Vorgang

Diese Task schaltet die Übertragungswarteschlangen, die von gestoppten oder inaktiven Clustersenderkanälen bereitgestellt werden. Sie können diese Task ausführen, da ein Clustersenderkanal gestoppt ist und Sie die Übertragungswarteschlange sofort umschalten möchten. Dies ist beispielsweise der Fall, wenn ein Clustersenderkanal nicht gestartet wird oder ein anderes Konfigurationsproblem vorliegt. Um das Problem zu beheben, müssen Sie einen Clustersenderkanal erstellen und die Übertragungswarteschlange für den alten Clustersenderkanal mit dem neuen Clustersenderkanal verknüpfen, den Sie definiert haben.

Ein wahrscheinlicher Fall ist, dass Sie die Steuerung steuern wollen, wenn die Neukonfiguration von Clusterübertragungswarteschlangen ausgeführt wird. Um die Rekonfiguration vollständig zu steuern, stoppen Sie die Kanäle, ändern die Konfiguration und wechseln dann die Übertragungswarteschlangen.

Vorgehensweise

1. Stoppen Sie die Kanäle, die Sie wechseln möchten.
   a) Stoppen Sie alle aktiven oder inaktiven Kanäle, die Sie wechseln möchten. Wenn Sie einen inaktiven Clustersenderkanal stoppen, wird dieser verhindert, während Sie Konfigurationsänderungen vornehmen.

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

2. Optional: Nehmen Sie die Konfigurationsänderungen vor.

   Informationen zum Beispiel finden Sie unter „Clustering: Beispielkonfiguration mehrerer Clusterübertragungswarteschlangen” auf Seite 61.
3. Schalten Sie die Clustersenderkanäle in die neuen Clusterübertragungswarteschlangen um.

   Multi Geben Sie unter Multiplatforms folgenden Befehl aus:

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

   z/OS Verwenden Sie unter z/OS die Funktion SWITCH des Befehls CSQUTIL, um die Nachrichten zu Wechseln oder die Vorgänge zu überwachen. Verwenden Sie den folgenden Befehl.

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

   Weitere Informationen finden Sie im Abschnitt SWITCH-Funktion .

   Der Befehl **runswchl**oder CSQUTIL SWITCH überträgt alle Nachrichten in der alten Übertragungswarteschlange an die neue Übertragungswarteschlange. Wenn die Anzahl der Nachrichten in der alten Übertragungswarteschlange für diesen Kanal den Wert null erreicht, wird der Switch abgeschlossen. Der Befehl ist synchron. Der Befehl schreibt während des Umschaltvorgangs Statusnachrichten in das Fenster.

   Während der Übertragungsphase werden vorhandene und neue Nachrichten, die für den Clustersenderkanal bestimmt sind, in die neue Übertragungswarteschlange übertragen.

   Da der Clustersenderkanal gestoppt ist, werden die Nachrichten in der neuen Übertragungswarteschlange erstellt. Vergleichen Sie den gestoppten Clustersenderkanal mit dem Schritt „2” auf Seite 72 in „Aktive Clustersenderkanäle zu einer anderen Gruppe von Clusterübertragungswarteschlangen wechseln” auf Seite 71. In diesem Schritt wird der Clustersenderkanal ausgeführt, sodass Nachrichten nicht notwendigerweise in der neuen Übertragungswarteschlange erstellt werden müssen.
4. Optional: Kanäle überwachen, während sie umschalten

Zeigen Sie in einem anderen Befehlsfenster die Länge der Übertragungswarteschlange während des Switchs an. Im folgenden Beispiel wird der Status der Übertragungswarteschlangen des Systemclusters angezeigt.

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

5. Optional: Überwachen Sie die Nachrichten AMQ7341 `Die Übertragungswarteschlange für den Kanal` *`ChannelName`*`, die von der Warteschlange` *`QueueName`* `in` *`QueueName`* umgeschaltet wurde, die in das Fehlerprotokoll des Warteschlangenmanagers geschrieben werden.
6. Starten Sie die Clustersenderkanäle erneut, die Sie gestoppt haben.

   Die Kanäle werden nicht automatisch gestartet, wenn Sie sie gestoppt haben, indem Sie sie in den Status STOPPED stellen.

   ```
   START CHANNEL(ChannelName)
   ```

Zugehörige Verweise
runswchl
GELÖST-CHANNEL
STOP CHANNEL

Clustering: Best Practices für Migration und Änderung
Dieser Abschnitt enthält eine Anleitung zur Planung und Verwaltung von IBM MQ-Clustern. Diese Informationen sind ein Leitfaden, der auf Tests und Feedback von Kunden basiert.

1. „Objekte in einem Cluster verschieben" auf Seite 74 (Bewährte Verfahren für das Verschieben von Objekten innerhalb eines Clusters ohne Installation von Fixpacks oder neuen Versionen von IBM MQ).
2. „Upgrades und Wartungsinstallationen" auf Seite 76 (Bewährte Verfahren für die Aufrechterhaltung einer betriebsweisen Clusterarchitektur und die Ausführung von Wartungs-oder Upgrades und Tests der neuen Architektur).

Objekte in einem Cluster verschieben

Anwendungen und ihre Warteschlangen

Wenn Sie eine Warteschlangeninstanz, die auf einem WS-Manager gehostet wird, in einem anderen Warteschlangenmanager verschieben müssen, können Sie mit den Parametern für die Lastverteilung arbeiten, um einen reibungslosen Übergang zu gewährleisten.

Erstellen Sie eine Instanz der Warteschlange, in der sie neu gehostet werden soll, verwenden Sie jedoch die Einstellungen für die Lastverteilung im Cluster, um das Senden von Nachrichten an die ursprüngliche Instanz fortzusetzen, bis Ihre Anwendung bereit ist, zu wechseln. Dies wird mit den folgenden Schritten erreicht:

1. Setzen Sie die **CLWLRANK**-Eigenschaft der vorhandenen Warteschlange auf einen hohen Wert, z. B. auf 5.
2. Erstellen Sie die neue Instanz der Warteschlange und setzen Sie die **CLWLRANK**-Eigenschaft auf 0.
3. Führen Sie eine beliebige weitere Konfiguration des neuen Systems aus, z. B. die Implementierung und das Starten von Anwendungen für die neue Instanz der Warteschlange.
4. Setzen Sie die **CLWLRANK**-Eigenschaft der neuen Warteschlangeninstanz auf einen höheren Wert als die ursprüngliche Instanz, z. B. auf 9.
5. Zulassen, dass die ursprüngliche Warteschlangeninstanz alle in der Warteschlange befindlichen Nachrichten im System verarbeitet und dann die Warteschlange löscht.

Verschieben ganzer WS-Manager

Wenn sich der WS-Manager auf demselben Host befindet, die IP-Adresse jedoch geändert wird, lautet der Prozess wie folgt:

- DNS, wenn es korrekt verwendet wird, kann die Vereinfachung des Prozesses vereinfachen. Informationen zur Verwendung von DNS durch Festlegen des Kanalattributs Verbindungsname (CONNAME) finden Sie unter ALTER CHANNEL.
- Wenn Sie ein vollständiges Repository verschieben, müssen Sie sicherstellen, dass Sie mindestens ein anderes vollständiges Repository haben, das problemlos ausgeführt wird (z. B. keine Probleme mit dem Kanalstatus), bevor Sie Änderungen vornehmen.
- Setzen Sie den Warteschlangenmanager mit dem Befehl SUSPEND QMGR aus, um die Datenverkehrsaufbauung zu vermeiden.
- Ändern Sie die IP-Adresse des Computers. Wenn Ihre CLUSRCVR-Kanaldefinition im Feld CONNAME eine IP-Adresse verwendet, ändern Sie diesen IP-Adresseneintrag. Der DNS-Cache muss möglicherweise durchgebürstet werden, um sicherzustellen, dass Aktualisierungen überall verfügbar sind.
- Wenn der Warteschlangenmanager die Verbindung zu den vollständigen Repositorys wiederherstellt, lösen sich automatisch die Kanalautodefinitionen selbst auf.
- Wenn der Warteschlangenmanager ein vollständiges Repository und die Änderungen an der IP-Adresse befindet, muss sichergestellt werden, dass die Teilpartien so bald wie möglich umgestellt werden, um manuell definierte CLUSSDR-Kanäle an die neue Position zu verweisen. Solange dieser Schalter nicht ausgeführt wird, können diese WS-Manager möglicherweise nur die verbleibenden (unveränderten) vollständigen Repositorys in Verbindung setzen, und es werden Warnungen angezeigt, die sich auf die falsche Kanaldefinition richten.
- Den WS-Manager mit dem Befehl RESUME QMGR wiederaufnehmen.

Wenn der Warteschlangenmanager auf einen neuen Host verschoben werden muss, ist es möglich, die Daten des Warteschlangenmanagers zu kopieren und aus einer Sicherung zurückzuschreiben. Dieser Prozess wird jedoch nicht empfohlen, es sei denn, es gibt keine anderen Optionen; es kann jedoch besser sein, einen Warteschlangenmanager auf einer neuen Maschine zu erstellen und Warteschlangen und Anwendungen zu replizieren, wie im vorherigen Abschnitt beschrieben. Diese Situation bietet einen reibungslosen Rollover/Rollback-Mechanismus.

Wenn Sie entschlossen sind, einen vollständigen Warteschlangenmanager unter Verwendung der Sicherung zu verschieben, befolgen Sie die folgenden bewährten Verfahren:

- Behandeln Sie den gesamten Prozess als Restore des Warteschlangenmanagers von der Sicherung, wobei Sie alle Prozesse anwenden, die Sie in der Regel für die Systemwiederherstellung verwenden, die für Ihre Betriebssystemumgebung geeignet sind.
- Verwenden Sie den Befehl **REFRESH CLUSTER** nach der Migration, um alle lokal gespeicherten Clusterinformationen (einschließlich aller unbestätigten, automatisch definierten Kanäle) zu löschen und die erneute Erstellung zu erzwingen.

  Anmerkung: Bei großen Clustern kann der Befehl **REFRESH CLUSTER** während seiner Ausführung und danach in 27-Tage-Intervallen, wenn die Clusterobjekte ihre Statusaktualisierungen automatisch an alle interessierten Warteschlangenmanager senden, zu Unterbrechungen führen. Nähere Informationen hierzu erhalten Sie im Abschnitt Die Aktualisierung in einem großen Cluster kann sich auf die Leistung und Verfügbarkeit auswirken.

Wenn Sie einen Warteschlangenmanager erstellen und die Konfiguration von einem vorhandenen WS-Manager im Cluster replizieren (wie in diesem Abschnitt beschrieben), behandeln Sie die beiden verschiedenen Warteschlangenmanager niemals so, wie sie eigentlich identisch sind. Geben Sie insbesondere keinen neuen Warteschlangenmanager denselben Warteschlangenmanagernamen und die gleiche IP-Adresse an. Der Versuch, auf diese Weise schnell zu einem Ersatz-Warteschlangenmanager zu wechseln, ist eine häufige Ursache für Probleme in IBM MQ-Clustern. Der Cache erwartet Aktualisierungen, einschließlich des Attributs **QMID**, und der Status kann beschädigt sein.

Wenn versehentlich zwei verschiedene Warteschlangenmanager mit demselben Namen erstellt werden, wird empfohlen, den Befehl RESET CLUSTER **QMID** zu verwenden, um den falschen Eintrag aus dem Cluster zu entfernen.

Upgrades und Wartungsinstallationen

Vermeiden Sie das so genannte Big-Bang-Szenario (z. B. das Stoppen aller Cluster-und WS-Manageraktivitäten, das Anwenden aller Upgrades und Wartungsarbeiten auf alle WS-Manager und das anschließende Starten aller Aktivitäten). Cluster sind so konzipiert, dass sie immer noch mit mehreren Versionen des Warteschlangenmanagers zusammenarbeiten, so dass ein gut geplanter, gestaffter Wartungsansatz empfohlen wird.

Haben Sie einen Backup-Plan:

- Haben Sie Sicherungen erstellt?
- Vermeiden Sie sofort die Verwendung der neuen Clusterfunktionalität: Warten Sie, bis Sie sicher sind, dass alle WS-Manager auf die neue Version aufgerüstet sind, und sind sicher, dass Sie keinen Rollback rückgängig machen werden. Die Verwendung einer neuen Clusterfunktion in einem Cluster, in dem einige WS-Manager noch auf einer früheren Version stehen, kann zu undefiniertem Verhalten führen. Wenn ein Warteschlangenmanager beispielsweise bei der Verschiebung von IBM WebSphere MQ 6.0nach IBM WebSphere MQ 7.1 ein Clusterthema definiert, werden IBM WebSphere MQ 6.0 -Warteschlangenmanager die Definition nicht verstehen oder nicht in der Lage sein, zu diesem Thema zu veröffentlichen.

Migrieren Sie zuerst die vollständigen Repositorys. Obwohl sie Informationen weiterleiten können, die sie nicht verstehen, können sie sie nicht fortbestehen, so dass es nicht der empfohlene Ansatz ist, es sei denn, es ist absolut notwendig. Weitere Informationen finden Sie im Abschnitt Migration des WS-Managers-Clusters .

Clustering: Best Practices für REFRESH CLUSTER verwenden
Sie verwenden den Befehl **REFRESH CLUSTER** , um alle lokal gespeicherten Informationen zu einem Cluster zu löschen und diese Informationen aus den vollständigen Repositorys im Cluster erneut zu erstellen. Sie sollten diesen Befehl nicht verwenden, außer in außergewöhnlichen Umständen. Wenn Sie es verwenden müssen, gibt es besondere Hinweise darauf, wie Sie es verwenden. Diese Informationen sind ein Leitfaden, der auf Tests und Feedback von Kunden basiert.

Führen Sie nur den Befehl REFRESH CLUSTER aus, wenn Sie dies wirklich tun müssen.

Die IBM MQ-Clustertechnologie stellt sicher, dass jede Änderung an der Clusterkonfiguration, z. B. die Änderung an einer Clusterwarteschlange, automatisch allen Mitgliedern des Clusters bekannt gegeben wird, die diese Information benötigen. Es ist nicht notwendig, weitere administrative Schritte zu unternehmen, um diese Weitergabe von Informationen zu erreichen.

Wenn solche Informationen nicht zu den Warteschlangenmanagern im Cluster gelangen, in denen sie erforderlich sind, z. B. eine Clusterwarteschlange, die von einem anderen Warteschlangenmanager im Cluster nicht bekannt ist, wenn eine Anwendung versucht, sie zum ersten Mal zu öffnen, bedeutet dies ein Problem in der Clusterinfrastruktur. Es ist beispielsweise möglich, dass ein Kanal nicht zwischen einem WS-Manager und einem vollständigen WS-Manager-Repository gestartet werden kann. Daher müssen alle Situationen, in denen Inkonsistenzen beobachtet werden, untersucht werden. Lösen Sie die Situation nach Möglichkeit ohne Verwendung des Befehls **REFRESH CLUSTER** auf.

In seltenen Fällen, die an anderer Stelle in dieser Produktdokumentation oder auf Anforderung des IBM Support dokumentiert sind, können Sie den Befehl **REFRESH CLUSTER** verwenden, um alle lokal gespeicherten Informationen zu einem Cluster zu löschen und diese Informationen aus den vollständigen Repositorys im Cluster erneut zu erstellen.

Die Neuerung in einem großen Cluster kann die Leistung und Verfügbarkeit des Clusters beeinträchtigen.

Die Verwendung des Befehls **REFRESH CLUSTER** kann während der Ausführung des Clusters zu Unterbrechungen führen, z. B. durch eine plötzliche Zunahme der Arbeit für die vollständigen Repositorys, wenn sie die erneute Weitergabe von Clusterressourcen des Warteschlangenmanagers verarbeiten. Wenn Sie in einem großen Cluster (d. h. viele Hunderte von Warteschlangenmanagern) aktualisieren, sollten Sie die Verwendung des Befehls in der täglichen Arbeit vermeiden, wenn möglich, und alternative Metho-

den verwenden, um spezifische Inkonsistenzen zu korrigieren. Wenn beispielsweise eine Clusterwarteschlange im Cluster nicht ordnungsgemäß weitergegeben wird, wird die Warteschlangenkonfiguration im gesamten Cluster von einem ersten Untersuchungsverfahren aktualisiert, das die Clusterwarteschlangendefinition aktualisiert, z. B. die Beschreibung der Clusterwarteschlange, die die Warteschlangenkonfiguration ändert. Dieser Prozess kann dazu beitragen, das Problem zu identifizieren und möglicherweise eine temporäre Inkonsistenz zu beheben.

Wenn alternative Methoden nicht verwendet werden können und Sie **REFRESH CLUSTER** in einem großen Cluster ausführen müssen, sollten Sie dies zu Zeiten geringer Systemauslastung oder während eines Wartungsfensters tun, um Auswirkungen auf Benutzerworkloads zu vermeiden. Sie sollten auch vermeiden, einen großen Cluster in einem einzigen Stapel zu aktualisieren und stattdessen die Aktivität wie in „Leistungs-und Verfügbarkeitsprobleme vermeiden, wenn Clusterobjekte automatische Aktualisierungen senden" auf Seite 77 erläutert zu stagnihen.

Leistungs-und Verfügbarkeitsprobleme vermeiden, wenn Clusterobjekte automatische Aktualisierungen senden

Nachdem ein neues Clusterobjekt in einem Warteschlangenmanager definiert ist, wird eine Aktualisierung für dieses Objekt alle 27 Tage ab der Definitionierungszeit generiert und an alle vollständigen Repositorys im Cluster und an alle anderen interessierten Warteschlangenmanager gesendet. Wenn Sie den Befehl **REFRESH CLUSTER** an einen Warteschlangenmanager ausgeben, setzen Sie die Systemzeit für diese automatische Aktualisierung für alle Objekte zurück, die lokal im angegebenen Cluster definiert sind.

Wenn Sie einen großen Cluster (d. a. viele Hunderte von Warteschlangenmanagern) in einem einzigen Stapel oder unter anderen Umständen aktualisieren, z. B. ein System aus der Konfigurationssicherung erneut erstellen, werden alle diese Warteschlangenmanager nach 27 Tagen alle ihre Objektdefinitionen erneut für die vollständigen Repositorys bekannt machen. Dies könnte wiederum dazu führen, dass das System erheblich langsamer oder gar nicht mehr verfügbar ist, bis alle Aktualisierungen abgeschlossen sind. Wenn Sie also mehrere Warteschlangenmanager in einem großen Cluster aktualisieren oder erneut erstellen müssen, sollten Sie die Aktivität über mehrere Stunden oder mehrere Tage stagniern, sodass nachfolgende automatische Aktualisierungen die Systemleistung nicht regelmäßig beeinträchtigen.

Die Systemclusterprotokollwarteschlange

Wenn eine **REFRESH CLUSTER** ausgeführt wird, erstellt der WS-Manager eine Momentaufnahme des Clusterstatus vor der Aktualisierung und speichert sie in `SYSTEM.CLUSTER.HISTORY.QUEUE` (SCHQ), wenn sie auf dem Warteschlangenmanager definiert ist. Diese Momentaufnahme dient ausschließlich zu Servicezwecken für IBM im Falle von späteren Problemen mit dem System.

Der SCHQ wird standardmäßig auf verteilten WS-Managern beim Start definiert. Bei der Migration von z/OS muss SCHQ manuell definiert werden.

Die Nachrichten in der SCHQ laufen nach drei Monaten ab.

Zugehörige Konzepte

„Hinweise zu REFRESH CLUSTER für Publish/Subscribe-Cluster" auf Seite 115
Die Ausgabe des Befehls **REFRESH CLUSTER** führt dazu, dass der Warteschlangenmanager vorübergehend lokal gehaltene Informationen zu einem Cluster löscht, einschließlich aller Clusterthemen und der zugehörigen Proxy-Subskriptionen.

Anwendungsprobleme bei der Ausführung von REFRESH CLUSTER

Zugehörige Verweise

MQSC-Befehlsreferenz: REFRESH CLUSTER

Clustering: Verfügbarkeit, Multi-Instanz und Wiederherstellung nach einem Katastrophenfall
Dieser Abschnitt enthält eine Anleitung zur Planung und Verwaltung von IBM MQ-Clustern. Diese Informationen sind ein Leitfaden, der auf Tests und Feedback von Kunden basiert.

IBM MQ-Clustering ist eigentlich keine Hochverfügbarkeitslösung, aber unter bestimmten Umständen kann sie verwendet werden, um die Verfügbarkeit von Services unter Verwendung von IBM MQ zu verbessern, z. B. wenn mehrere Instanzen einer Warteschlange auf verschiedenen Warteschlangenmanagern

vorhanden sind. Dieser Abschnitt enthält Anleitungen um sicherzustellen, dass die IBM MQ-Infrastruktur eine möglichst hohe Verfügbarkeit aufweist, damit sie in einer solchen Architektur verwendet werden kann.

Anmerkung: Weitere Hochverfügbarkeits-und Disaster-Recovery-Lösungen sind für IBM MQverfügbar (siehe Hochverfügbarkeit, Wiederherstellung und Neustart konfigurieren).

Verfügbarkeit von Clusterressourcen
Der Grund für die übliche Empfehlung, zwei vollständige Repositorys zu verwalten, besteht darin, dass der Verlust von einem nicht kritisch für die reibungslose Ausführung des Clusters ist. Selbst wenn beide nicht mehr verfügbar sind, gibt es eine 60-Tage-Karenzzeit für vorhandene Kenntnisse, die von Teilrepositorys gehalten werden, obwohl neue oder nicht zuvor aufgerufene Ressourcen (z. B. Warteschlangen) in diesem Ereignis nicht verfügbar sind.

Verwenden von Clustern zur Verbesserung der Anwendungsverfügbarkeit
Ein Cluster kann Ihnen bei der Entwicklung hoch verfügbarer Anwendungen (z. B. einer Serveranwendung für Anforderungen/Antworttyp) helfen, indem Sie mehrere Instanzen der Warteschlange und der Anwendung verwenden. Falls erforderlich, können Prioritätsattribute die Anwendung "live" bevorzugen, es sei denn, ein WS-Manager oder Kanal ist beispielsweise nicht verfügbar. Dies ist leistungsfähig, um schnell umschalten zu können, um die Verarbeitung neuer Nachrichten fortzusetzen, wenn ein Problem auftritt.

Nachrichten, die einem bestimmten Warteschlangenmanager in einem Cluster zugestellt wurden, werden jedoch nur in dieser Warteschlangeninstanz gehalten und stehen erst dann zur Verarbeitung zur Verfügung, wenn dieser WS-Manager wiederhergestellt wird. Aus diesem Grund sollten Sie für die hohe Verfügbarkeit von Daten möglicherweise andere Technologien, wie z. B. Warteschlangenmanager mit mehreren Instanzen, berücksichtigen.

Warteschlangenmanager mit mehreren Instanzen
Software mit hoher Verfügbarkeit (mehrere Instanzen) ist ein integriertes Angebot, damit Ihre vorhandenen Nachrichten verfügbar bleiben. Weitere Informationen finden Sie unter IBM MQ mit Konfigurationen mit hoher Verfügbarkeit verwenden, Erstellen eines Multi-Instanz-Warteschlangenmanagers und im folgenden Abschnitt. Für jeden Warteschlangenmanager in einem Cluster kann mit diesem Verfahren eine hohe Verfügbarkeit erreicht werden, sofern auf allen Warteschlangenmanagern im Cluster mindestens IBM WebSphere MQ 7.0.1 ausgeführt wird. Wenn sich die WS-Manager im Cluster auf früheren Ebenen befinden, verlieren sie möglicherweise die Verbindung zu den Multi-Instanz-WS-Managern, wenn sie zu einem sekundären IP-System umschlagen.

Wie bereits in diesem Artikel beschrieben, solange zwei vollständige Repositorys konfiguriert sind, sind sie fast von ihrer Natur hoch verfügbar. Falls IBM MQ mit hoher Verfügbarkeit benötigt wird, können Multi-Instanz-Warteschlangenmanager für vollständige Repositorys verwendet werden. Es gibt keinen Grund, diese Methoden zu verwenden, und in der Tat für temporäre Ausfälle können diese Methoden während des Failover zusätzliche Leistungskosten verursachen. Wenn Sie die Software HA verwenden, anstatt zwei vollständige Repositorys auszuführen, wird davon abgeraten, weil z. B. bei einem einzelnen Kanalausfall nicht notwendigerweise ein Fehler fehlschlagen würde, aber es kann vorkommen, dass Teilrepositorys nicht in der Lage sind, Clusterressourcen abzufragen.

Wiederherstellung nach einem Katastrophenfall
Eine Disaster-Recovery, z. B. die Wiederherstellung nach einer Beschädigung der Platten, auf denen die Daten eines Warteschlangenmanagers gespeichert waren, ist zwar schwierig, wird von IBM MQ aber unterstützt, obwohl der Vorgang nicht automatisch ausgeführt werden kann. Die einzige "wahre" Disaster-Revovery-Option in IBM MQ (abgesehen von den durch das Betriebssystem bereitgestellten oder sonstigen grundlegenden Replikationstechnologien) ist die Wiederherstellung aus einer Sicherung. Es gibt einige Cluster-spezifische Punkte, die in diesen Situationen zu berücksichtigen sind:

- Gehen Sie beim Testen von Szenarios zur Notfallwiederherstellung sorgfältig vor. Wenn Sie beispielsweise den Betrieb von Sicherungswarteschlangenmanagern testen, müssen Sie darauf achten, dass sie in demselben Netz online sind, da es möglich ist, versehentlich den Live-Cluster zu verbinden und die 'Stealing' -Nachrichten zu starten, indem sie dieselben benannten Warteschlangen wie in den Live-Cluster-WS-Managern enthalten.
- Der Test zur Wiederherstellung nach einem Katastrophenfall darf nicht in einen aktiven Live-Cluster eingreifen. Zu den Techniken zur Vermeidung von Kollisionen gehören:

  - Vollständige Netztrennung oder Trennung auf Firewall-Ebene.
  - z/OS Kanalinitialisierung oder z/OS **chinit** -Adressraum wird nicht gestartet.
  - Es wird kein Live-TLS-Zertifikat für das System zur Wiederherstellung nach einem Katastrophenfall ausgegeben, oder es sei denn, es tritt ein tatsächliches Fehlerbehebungsszenario
- Wenn Sie eine Sicherung eines Warteschlangenmanagers im Cluster wiederherstellen, ist es möglich, dass die Sicherung nicht mehr mit dem Rest des Clusters synchronisiert ist. Der Befehl **REFRESH CLUSTER** kann Aktualisierungen auflösen und mit dem Cluster synchronisieren, aber der Befehl **REFRESH CLUSTER** muss als letzte Möglichkeit verwendet werden. Siehe „Clustering: Best Practices für REFRESH CLUSTER verwenden" auf Seite 76. Bevor Sie den Befehl verwenden, überprüfen Sie in der unternehmensinternen Dokumentation und der IBM MQ-Dokumentation, ob irgendein einfacher Schritt versäumt wurde.
- Wie bei jeder Wiederherstellung müssen die Anwendungen mit der Wiedergabe und dem Verlust von Daten umgehen. Es muss entschieden werden, ob die Warteschlangen in einem bekannten Status gelöscht werden sollen oder ob genügend Informationen vorhanden sind, um die Replays zu verwalten.

Verteiltes Publish/Subscribe-Netz planen

Sie können ein Netz von Warteschlangenmanagern erstellen, in denen Subskriptionen, die auf einem Warteschlangenmanager erstellt wurden, übereinstimmende Nachrichten empfangen, die von einer Anwendung veröffentlicht werden, die mit einem anderen Warteschlangenmanager im Netz verbunden ist. Um eine geeignete Topologie auszuwählen, müssen Sie Ihre Anforderungen für die manuelle Steuerung, die Netzgröße, die Häufigkeit von Änderungen, die Verfügbarkeit und die Skalierbarkeit in Betracht ziehen.

Vorbereitende Schritte

Diese Task setzt voraus, dass Sie wissen, was verteilte Publish/Subscribe-Netze sind und wie sie funktionieren. Eine technische Übersicht finden Sie unter Verteilte Publish/Subscribe-Netzwerke.

Informationen zu diesem Vorgang

Es gibt drei grundlegende Topologien für ein Publish/Subscribe-Netzwerk:

- Direkt geroutete Cluster
- Topic-Host-Routing-Cluster
- Hierarchie

Bei den ersten beiden Topologien ist der Ausgangspunkt eine IBM MQ-Clusterkonfiguration. Die dritte Topologie kann mit oder ohne Cluster erstellt werden. Weitere Informationen zur Planung des zugrundeliegenden Warteschlangenmanagernetzes finden Sie unter „Verteilte Warteschlangen und Cluster planen" auf Seite 21.

Ein *Direkt-Routing-Cluster* ist die einfachste Topologie, die konfiguriert werden soll, wenn ein Cluster bereits vorhanden ist. Jedes Thema, das Sie in jedem WS-Manager definieren, wird automatisch auf jedem WS-Manager im Cluster zur Verfügung gestellt, und die Veröffentlichungen werden direkt von jedem Warteschlangenmanager weitergeleitet, auf dem eine Veröffentlichungsanwendung eine Verbindung herstellt, zu jedem der Warteschlangenmanager, für die übereinstimmende Subskriptionen vorhanden sind. Voraussetzung für eine solch einfache Konfiguration ist das hohe Maß an gemeinsamer Nutzung von Informationen und an Konnektivität zwischen den Warteschlangenmanagern eines Cluster, das IBM MQ ermöglicht. Für kleine und einfache Netze (d. a. eine kleine Anzahl von Warteschlangenmanagern und eine relativ statische Gruppe von Publishern und Subskribenten) ist dies akzeptabel. Wenn der Systemaufwand jedoch in größeren oder dynamischeren Umgebungen verwendet wird, ist dies möglicherweise untragbar. Siehe„Direktes Routing in Publish/Subscribe-Clustern" auf Seite 85.

Ein *Topic-Host-Routing-Cluster* bietet denselben Vorteil wie ein direkter weitergeleitete Cluster, indem Sie jedes Thema, das Sie in jedem WS-Manager im Cluster definieren, automatisch auf jedem WS-Manager im Cluster verfügbar machen. Bei den Host-Routing-Clustern müssen Sie jedoch die Warteschlangenmanager, die die einzelnen Themen enthalten, sorgfältig auswählen, da alle Informationen und Veröffentlich-

ungen zu diesem Thema diese Topic-Host-WS-Manager durchlaufen. Dies bedeutet, dass das System die Kanäle und Informationsflüsse nicht zwischen allen Warteschlangenmanagern verwalten muss. Dies bedeutet jedoch auch, dass Veröffentlichungen möglicherweise nicht mehr direkt an Subskribenten gesendet werden, sondern möglicherweise über einen Topic-Host-Warteschlangenmanager weitergeleitet werden. Aus diesen Gründen kann es zu einer zusätzlichen Belastung des Systems kommen, insbesondere auf den Warteschlangenmanagern, die die Themen hosten, so dass eine sorgfältige Planung der Topologie erforderlich ist. Diese Topologie ist besonders effektiv für Netze, die viele Warteschlangenmanager enthalten, oder die eine dynamische Gruppe von Publishern und Subskribenten (d. a. veröffentlichende Stellen oder Subskribenten, die häufig hinzugefügt oder entfernt werden) enthalten. Es können zusätzliche Themenhosts definiert werden, um die Verfügbarkeit von Routen zu verbessern und die Publikationsworkload horizontal skalieren zu lassen. Siehe„Thema Host-Routing in Publish/Subscribe-Clustern” auf Seite 90.

Eine *Hierarchie* erfordert die Konfiguration der meisten manuellen Konfigurationen und ist die schwierigste Topologie, die geändert werden soll. Sie müssen die Beziehungen zwischen den einzelnen Warteschlangenmanagern in der Hierarchie und ihren direkten Beziehungen manuell konfigurieren. Nach der Konfiguration von Beziehungen werden die Veröffentlichungen (wie bei den vorherigen beiden Topologien) an Subskriptionen auf anderen Warteschlangenmanagern in der Hierarchie weitergeleitet. Veröffentlichungen werden unter Verwendung der Hierarchiebeziehungen weitergeleitet. Dadurch können sehr spezifische Topologien so konfiguriert werden, dass sie unterschiedlichen Anforderungen entsprechen, aber es kann auch dazu führen, dass Veröffentlichungen, die viele " Hops " erfordern, über temporäre Warteschlangenmanager die Subskriptionen erreichen. Es gibt immer nur eine Route durch eine Hierarchie für eine Veröffentlichung, so dass die Verfügbarkeit jedes Warteschlangenmanagers kritisch ist. Hierarchien sind in der Regel nur dann vorzuziehen, wenn ein einzelner Cluster nicht konfiguriert werden kann, z. B. wenn er mehrere Organisationen umfasst. Siehe„Routing in Publish/Subscribe-Hierarchien” auf Seite 116.

Bei Bedarf können die oben genannten drei Topologien kombiniert werden, um spezifische topographische Anforderungen zu lösen. Ein Beispiel finden Sie unter Kombinieren der Topic-Bereiche mehrerer Cluster .

Wenn Sie eine geeignete Topologie für Ihr verteiltes Publish/Subscribe-Netz auswählen möchten, müssen Sie die folgenden allgemeinen Fragen berücksichtigen:

- Wie groß wird Ihr Netzwerk sein?
- Wie viel manuelle Steuerung benötigen Sie über die Konfiguration?
- Wie dynamisch wird das System sowohl in Bezug auf Themen als auch in Bezug auf die Subskriptionen und in Bezug auf die Warteschlangenmanager sein?
- Was sind Ihre Verfügbarkeits-und Skalierbarkeitsanforderungen?
- Können alle WS-Manager direkt miteinander verbunden werden?

Prozedur

- Schätzen Sie, wie groß Ihr Netzwerk sein muss.
  a) Schätzen Sie, wie viele Themen Sie benötigen.
  b) Schätzen Sie, wie viele Publisher und Abonnenten Sie erwarten.
  c) Schätzen Sie, wie viele WS-Manager an Publish/Subscribe-Aktivitäten beteiligt sein werden.

  Weitere Informationen finden Sie unter „Publish/Subscribe-Clustering: Bewährte Verfahren” auf Seite 100, insbesondere in folgenden Abschnitten:

  – Vorgehensweise zum Anpassen der Größe Ihres Systems
  – Gründe für die Begrenzung der Anzahl von an Publish/Subscribe-Aktivitäten beteiligten Clusterwarteschlangenmanagern
  – Vorgehensweise bei der Entscheidung, welche Themen zu einem Cluster gehören sollen

  Wenn Ihr Netz über viele Warteschlangenmanager verfügt und viele Publisher und Subskribenten verarbeiten kann, müssen Sie wahrscheinlich einen Topic-Host-Routing-Cluster oder eine Hierarchie

verwenden. Direkt verlegte Cluster erfordern fast keine manuelle Konfiguration und können eine gute Lösung für kleine oder statische Netzwerke sein.

- Überlegen Sie, wie viel manuelle Steuerung Sie benötigen, über welchen Warteschlangenmanager die einzelnen Themen, Bereitsteller oder Subskribenten gehostet werden.
  a) Überlegen Sie, ob einige Ihrer WS-Manager weniger fähig sind als andere.
  b) Überlegen Sie, ob die Kommunikationsverbindungen zu einigen Ihrer WS-Manager empfindlicher als andere sind.
  c) Geben Sie Fälle an, in denen Sie ein Thema mit vielen Veröffentlichungen und nur wenigen Subskribenten erwarten.
  d) Geben Sie Fälle an, in denen Sie ein Thema erwarten, das viele Subskribenten und nur wenige Veröffentlichungen enthält.

  In allen Topologien werden Veröffentlichungen an Subskriptionen auf anderen Warteschlangenmanagern zugestellt. In einem direkt weitergeleiteten Cluster nehmen diese Veröffentlichungen den kürzesten Pfad zu den Subskriptionen an. In einem Topic-Host-Routing-Cluster oder einer Hierarchie steuern Sie die Route, die von den Veröffentlichungen ausgeführt wird. Wenn sich Ihre Warteschlangenmanager in ihrer Funktionalität unterscheiden oder unterschiedliche Verfügbarkeits-und Konnektivitätsstufen aufweisen, möchten Sie bestimmte Workloads bestimmten Warteschlangenmanagern zuordnen. Sie können dies entweder mit einem Topic-Host-Routing-Cluster oder mit einer Hierarchie ausführen.

  In allen Topologien ist es möglich, die Veröffentlichungsanwendungen auf demselben Warteschlangenmanager wie die Subskriptionen zu lokalisieren, wenn dies möglich ist, um die Leistung zu minimieren und die Leistung zu maximieren. Für Topic-Host-Routing-Cluster können Sie Publisher oder Subskribenten in den Warteschlangenmanagern, die das Thema hosten, in Betracht ziehen. Dadurch werden alle zusätzlichen " Hops " zwischen WS-Managern entfernt, um eine Veröffentlichung an einen Subskribenten zu übergeben. Dieser Ansatz ist besonders effektiv in Fällen, in denen ein Thema viele veröffentlichende Stellen und wenige Abonnenten hat, oder viele Abonnenten und nur wenige Verlage. Siehe z. B. Topic-Host-Routing mit zentralisierten Publishern oder Subskribenten .

  Weitere Informationen finden Sie unter „Publish/Subscribe-Clustering: Bewährte Verfahren” auf Seite 100, insbesondere in folgenden Abschnitten:

  – Vorgehensweise bei der Entscheidung, welche Themen zu einem Cluster gehören sollen
  – Publisher- und Subskriptionspositionen

- Überlegen Sie, wie dynamisch die Netzaktivität sein wird.
  a) Schätzen Sie, wie häufig Subskribenten zu verschiedenen Themen hinzugefügt und entfernt werden.

     Immer wenn eine Subskription aus einem Warteschlangenmanager hinzugefügt oder aus einem Warteschlangenmanager entfernt wird und die erste oder letzte Subskription für diese bestimmte Themenzeichenfolge ist, werden diese Informationen anderen Warteschlangenmanagern in der Topologie mitgeteilt. In einem direkt weitergeleiteten Cluster und einer Hierarchie werden diese Subskriptionsinformationen an alle Warteschlangenmanager in der Topologie weitergegeben, unabhängig davon, ob sie über Publisher für das Thema verfügen. Wenn die Topologie aus vielen Warteschlangenmanagern besteht, kann dies zu einem erheblichen Leistungsaufwand führen. In einem Host-Routing-Cluster werden diese Informationen nur an die WS-Manager weitergegeben, die ein Clusterthema enthalten, das der Themenzeichenfolge der Subskription zugeordnet ist.

     Weitere Informationen finden Sie unter „Publish/Subscribe-Clustering: Bewährte Verfahren” auf Seite 100 im Abschnitt Subskriptionsänderung und dynamische Themenzeichenfolgen.

     Anmerkung: In sehr dynamischen Systemen, bei denen die Gruppe vieler eindeutiger Themenzeichenfolgen schnell und ständig geändert wird, kann es am besten sein, das Modell in den Modus " publish überall " umzuschalten. Weitere Informationen finden Sie im Abschnitt Subskriptionsleistung in Publish/Subscribe-Netzen.
  b) Überlegen Sie, wie dynamisch die WS-Manager in der Topologie sind.

     Eine Hierarchie erfordert jede Änderung des Warteschlangenmanagers in der Topologie, die manuell in die Hierarchie eingefügt oder aus der Hierarchie entfernt werden muss, wobei die Änderungen

beim Ändern von Warteschlangenmanagern auf höheren Ebenen in der Hierarchie berücksichtigt werden müssen. WS-Manager in einer Hierarchie verwenden normalerweise auch manuell konfigurierte Kanalverbindungen. Sie müssen diese Verbindungen verwalten, Kanäle hinzufügen und entfernen, da Warteschlangenmanager hinzugefügt und aus der Hierarchie entfernt werden.

In einem Publish/Subscribe-Cluster werden WS-Manager automatisch mit jedem anderen Warteschlangenmanager verbunden, der erforderlich ist, wenn er zum ersten Mitglied des Clusters ist, und wird automatisch über Themen und Subskriptionen informiert.

- Berücksichtigen Sie die Anforderungen an die Verfügbarkeit und die Skalierbarkeit des Veröffentlichungsverkehrs.
  a) Entscheiden Sie, ob Sie immer eine verfügbare Route von einem Veröffentlichungswarteschlangenmanager zu einem subskribierenden Warteschlangenmanager haben müssen, selbst wenn ein Warteschlangenmanager nicht verfügbar ist.
  b) Berücksichtigen Sie, wie skalierbar Sie das Netz benötigen. Entscheiden Sie, ob die Ebene des Veröffentlichungsdatenverkehrs zu hoch ist, um durch einen einzelnen Warteschlangenmanager oder Kanal weitergeleitet zu werden, und ob diese Ebene des Veröffentlichungsdatenverkehrs von einem einzelnen Topic-Zweig bearbeitet werden muss oder sich über mehrere Topic-Verzweigungen verteilen kann.
  c) Überlegen Sie, ob die Nachrichtenreihenfolge beibehalten werden muss.

  Da ein direkter Routing-Cluster Nachrichten direkt von Veröffentlichungswarteschlangenmanagern zum Subskribieren von Warteschlangenmanagern sendet, müssen Sie die Verfügbarkeit von temporären Warteschlangenmanagern entlang der Route nicht berücksichtigen. Ebenso wird die Skalierung auf die temporären WS-Manager nicht berücksichtigt. Wie bereits erwähnt, kann der Aufwand für die automatische Verwaltung von Kanälen und Informationsflüssen zwischen allen Warteschlangenmanagern im Cluster jedoch erhebliche Auswirkungen auf die Leistung haben, insbesondere in einer großen oder dynamischen Umgebung.

  Ein Topic-Host-Routing-Cluster kann für einzelne Themen optimiert werden. Sie können sicherstellen, dass jede Verzweigung der Themenstruktur, die über eine beachtliche Veröffentlichungsworkload verfügt, auf einem anderen Warteschlangenmanager definiert ist und dass jeder Warteschlangenmanager ausreichend performant ist und für die erwartete Auslastung für diese Verzweigung der Themenstruktur verfügbar ist. Sie können die Verfügbarkeit und die horizontale Skalierung auch verbessern, indem Sie die einzelnen Themen auf mehreren Warteschlangenmanagern definieren. Auf diese Weise kann das System den Host-WS-Managern des Topics nicht mehr verfügbar machen und die Auslastung des Publikationsdatenverkehrs in der Lastverteilung auf sie Wenn Sie jedoch ein bestimmtes Thema auf mehreren Warteschlangenmanagern definieren, führen Sie außerdem die folgenden Einschränkungen durch:

  – Sie verlieren die Nachrichtenreihenfolge in allen Veröffentlichungen.
  – Es ist nicht möglich, ständige Veröffentlichungen zu verwenden. Siehe„Designüberlegungen zu ständigen Veröffentlichungen in Publish/Subscribe-Clustern” auf Seite 113.

  Sie können keine hohe Verfügbarkeit oder Skalierbarkeit von Routing in einer Hierarchie über mehrere Routen konfigurieren.

  Weitere Informationen finden Sie unter „Publish/Subscribe-Clustering: Bewährte Verfahren” auf Seite 100 im Abschnitt Veröffentlichungsdatenverkehr.
- Basierend auf diesen Berechnungen verwenden Sie die Links, die Ihnen bei der Entscheidung helfen, ob ein Topic-Host-Routing-Cluster, ein direkter Routing-Cluster, eine Hierarchie oder eine Mischung dieser Topologien verwendet werden soll.

Nächste Schritte

Sie können jetzt Ihr verteiltes Publish/Subscribe-Netz konfigurieren.

Zugehörige Tasks

WS-Manager-Cluster konfigurieren

Verteilte Warteschlangensteuerung konfigurieren

Publish/Subscribe-Cluster konfigurieren

WS-Manager mit einer Publish/Subscribe-Hierarchie verbinden

Publish/Subscribe-Cluster entwerfen

Es gibt zwei grundlegende Publish/Subscribe-Clustertopologien: *direktes Routing* und *Topic-Host-Routing* . Jeder hat unterschiedliche Vorteile. Wenn Sie Ihren Publish/Subscribe-Cluster entwerfen, wählen Sie die Topologie aus, die am besten zu den erwarteten Netzanforderungen passt.

Eine Übersicht über die beiden Publish/Subscribe-Clustertopologien finden Sie unter Publish/Subscribe-Cluster. Informationen zum Auswerten der Netzanforderungen finden Sie in „Verteiltes Publish/Subscribe-Netz planen” auf Seite 79 und „Publish/Subscribe-Clustering: Bewährte Verfahren” auf Seite 100.

Im Allgemeinen bieten beide Clustertopologien die folgenden Vorteile:

- Einfache Konfiguration über eine Punkt-zu-Punkt-Clustertopologie.
- Automatischer Umgang mit Warteschlangenmanagern, die den Cluster verbinden und verlassen.
- Skalieren Sie die Skalierung für zusätzliche Subskriptionen und Publisher, indem Sie zusätzliche Warteschlangenmanager hinzufügen und die zusätzlichen Subskriptionen und Publisher auf diese verteilen.

Allerdings weisen die beiden Topologien unterschiedliche Vorteile auf, da die Anforderungen spezifischer werden.

Direkt weitergeleitete Publish/Subscribe-Cluster

Bei einem direkten Routing sendet jeder WS-Manager im Cluster Veröffentlichungen von verbundenen Anwendungen direkt an jeden anderen Warteschlangenmanager im Cluster mit einer übereinstimmenden Subskription.

Ein Publish/Subscribe-Cluster mit direkter Weiterleitung bietet die folgenden Vorteile:

- Nachrichten, die für eine Subskription auf einem bestimmten Warteschlangenmanager im selben Cluster bestimmt sind, werden direkt zu diesem Warteschlangenmanager transportiert und müssen keinen temporären Warteschlangenmanager durchlaufen. Dies kann die Leistung im Vergleich zu einer Topologie mit Topic-Host oder einer hierarchischen Topologie verbessern.
- Da alle WS-Manager direkt miteinander verbunden sind, gibt es in der Routing-Infrastruktur dieser Topologie keinen Single Point of Failure. Wenn ein Warteschlangenmanager nicht verfügbar ist, können Subskriptionen auf anderen WS-Managern im Cluster weiterhin Nachrichten von Publishern auf verfügbaren Warteschlangenmanagern empfangen.
- Es ist sehr einfach zu konfigurieren, insbesondere auf einem vorhandenen Cluster.

Bei Verwendung eines direkt weitergeleiteten Publish/Subscribe-Clusters ist Folgendes zu beachten:

- Alle WS-Manager im Cluster werden von allen anderen Warteschlangenmanagern im Cluster informiert.
- Warteschlangenmanager in einem Cluster, die eine oder mehrere Subskriptionen für ein Clusterthema hosten, erstellen automatisch Clustersenderkanäle zu allen anderen WS-Managern im Cluster, auch wenn diese Warteschlangenmanager keine Nachrichten in einem Clusterthema veröffentlichen.
- Die erste Subskription auf einem WS-Manager in einer Themenzeichenfolge unter einem Clusterthema führt dazu, dass eine Nachricht an alle anderen Warteschlangenmanager im Cluster gesendet wird. In ähnlicher Weise wird auch die letzte Subskription für eine zu löschende Themenzeichenfolge in einer Nachricht angezeigt. Je mehr einzelne Themenzeichenfolgen in einem Clusterthema verwendet werden und um so höher ist die Änderungsrate der Subskriptionen, so dass die Kommunikation zwischen WS-Managern mehr stattfindet.
- Jeder WS-Manager im Cluster behält die Kenntnis der subskribierten Themenzeichenfolgen, über die er informiert wird, selbst wenn der Warteschlangenmanager diese Themen weder veröffentlicht noch subskribiert.

Aus den oben genannten Gründen wird für alle Warteschlangenmanager in einem Cluster mit einem direkt geleiteten Thema ein zusätzlicher Systemaufwand entstehen. Je mehr WS-Manager in dem Cluster vorhanden sind, um so größer ist der Systemaufwand. Auch die mehr Themenzeichenfolgen subskribiert und um so größer ist ihr Änderungsrate, um so größer der Aufwand. Dies kann zu einer zu hohen Auslastung

von Warteschlangenmanagern führen, die auf kleinen Systemen in einem großen oder dynamischen Direct-Routing-Publish/Subscribe-Cluster ausgeführt werden. Weitere Informationen finden Sie unter Direct routed Publish/Subscribe performance .

Wenn Sie wissen, dass ein Cluster die Overheads von Direct-Routing-Publish/Subscribe nicht aufnehmen kann, können Sie stattdessen topic host routed publish/subscribe verwenden. Alternativ dazu können Sie die Cluster-Publish/Subscribe-Funktionalität auch in extremen Situationen vollständig inaktivieren, indem Sie das Warteschlangenmanager-Attribut **PSCLUS** auf jedem WS-Manager im Cluster auf DISABLED setzen. Siehe „Clusterveröffentlichungs-/Subskriptionssubskribieren" auf Seite 111. Dadurch wird verhindert, dass ein Cluster-Topic erstellt wird, und stellt daher sicher, dass Ihrem Netz keine Überleitung zugeordnet ist, die mit einem Cluster-Publish/Subscribe verknüpft sind.

Topic-Host-Verlegte Publish/Subscribe-Cluster

Bei Topic-Host-Routing werden die Warteschlangenmanager, in denen Clusterthemen administrativ definiert sind, zu Routern für Veröffentlichungen. Veröffentlichungen von Nicht-Hosting-WS-Managern im Cluster werden über den Host-WS-Manager an jeden Warteschlangenmanager im Cluster mit einer übereinstimmenden Subskription weitergeleitet.

Ein Publish/Subscribe-Cluster mit Topic-Host-Routing bietet die folgenden zusätzlichen Vorteile für einen direkt weitergeleiteten Publish/Subscribe-Cluster:

- Nur WS-Manager, auf denen Topic-Host-Routing-Themen definiert sind, werden von allen anderen Warteschlangenmanagern im Cluster informiert.
- Nur der Topic-Host-Warteschlangenmanager muss in der Lage sein, eine Verbindung zu allen anderen Warteschlangenmanagern im Cluster herzustellen. In der Regel wird nur die Verbindung zu den Warteschlangenmanagern hergestellt, in denen Subskriptionen vorhanden sind. Daher gibt es deutlich weniger Kanäle, die zwischen WS-Managern ausgeführt werden.
- Cluster-WS-Manager, die eine oder mehrere Subskriptionen für ein Clusterthema hosten, erstellen Clustersenderkanäle automatisch nur zu Warteschlangenmanagern, die ein Clusterthema enthalten, das der Themenzeichenfolge der Subskription zugeordnet ist.
- Die erste Subskription auf einem WS-Manager in einer Themenzeichenfolge unter einem Clusterthema führt dazu, dass eine Nachricht an einen Warteschlangenmanager im Cluster gesendet wird, in dem das Clusterthema gehostet wird. In ähnlicher Weise wird auch die letzte Subskription für eine zu löschende Themenzeichenfolge in einer Nachricht angezeigt. Je mehr einzelne Themenzeichenfolgen in einem Clusterthema verwendet werden, und je höher die Änderungsrate der Subskriptionen ist, wird die Kommunikation zwischen den WS-Managern, aber nur zwischen Subskriptionshosts und Themenhosts, durchgeführt.
- Größere Kontrollmöglichkeiten bei der physischen Konfiguration. Bei direkter Weiterleitung müssen alle WS-Manager am Publish/Subscribe-Cluster teilnehmen und ihre Overheads erhöhen. Bei der Weiterleitung von Topic-Hosts sind nur die Warteschlangenmanager des Topic-Hosts von anderen Warteschlangenmanagern und deren Subskriptionen bekannt. Sie wählen die Topic-Host-Warteschlangenmanager explizit aus. Daher können Sie sicherstellen, dass diese WS-Manager auf einer geeigneten Ausrüstung ausgeführt werden, und Sie können weniger leistungsfähige Systeme für die anderen Warteschlangenmanager verwenden.

Beim Verwenden eines Publish/Subscribe-Clusters für einen Topic-Host ist Folgendes zu beachten:

- Ein zusätzlicher " Hop " zwischen einem Veröffentlichungswarteschlangenmanager und einem subskribierenden Warteschlangenmanager wird eingeführt, wenn der Bereitsteller oder der Subskribent sich nicht auf einem Topic-Hosting-Warteschlangenmanager befindet. Die Latenzzeit, die durch den zusätzlichen " Hop " verursacht wird, kann bedeuten, dass die Routing-Weiterleitung durch das Topic-Host weniger effizient ist.
- Bei großen Clustern vereinfacht das Thema Host-Routing die wichtigen Leistungs-und Skalierungsprobleme, die Sie mit der direkten Weiterleitung erreichen können.
- Sie können alle Themen in einem einzigen Warteschlangenmanager oder in einer sehr kleinen Anzahl von Warteschlangenmanagern definieren. Wenn Sie dies tun, stellen Sie sicher, dass die Host-WS-Manager auf leistungsfähigen Systemen mit guter Konnektivität gehostet werden.

- Sie können dasselbe Thema in mehr als einem Warteschlangenmanager definieren. Dadurch wird die Verfügbarkeit des Themas erhöht und die Skalierbarkeit verbessert, da die IBM MQ-Workload die Veröffentlichungen zu einem Thema auf alle Hosts für dieses Thema verteilt. Beachten Sie jedoch, dass die Definition desselben Themas in mehr als einem Warteschlangenmanager die Nachrichtenreihenfolge für dieses Thema verliert.
- Wenn Sie verschiedene Themen auf verschiedenen Warteschlangenmanagern hosten, können Sie die Skalierbarkeit verbessern, ohne die Nachrichtenreihenfolge zu verlieren.

Zugehörige Tasks

Publish/Subscribe-Cluster konfigurieren

Verteilte Publish/Subscribe-Netze optimieren

Verteilte Publish/Subscribe-Fehlerbehebung

Zugehörige Verweise

Szenario mit Publish/Subscribe-Cluster

Direktes Routing in Publish/Subscribe-Clustern

Veröffentlichungen von einem beliebigen Veröffentlichungswarteschlangenmanager werden direkt an alle anderen Warteschlangenmanager im Cluster weitergeleitet, die eine übereinstimmende Subskription aufweisen.

Eine Einführung dazu, wie Nachrichten zwischen Warteschlangenmanagern in Publish/Subscribe-Hierarchien und Clustern weitergeleitet werden, finden Sie unter Verteilte Publish/Subscribe-Netze.

Ein Direct-Routing-Publish/Subscribe-Cluster verhält sich wie folgt:

- Alle WS-Manager kennen automatisch alle anderen Warteschlangenmanager.
- Alle WS-Manager mit Subskriptionen für Clusterthemen erstellen Kanäle zu allen anderen WS-Managern im Cluster und informieren sie über ihre Subskriptionen.
- Nachrichten, die von einer Anwendung veröffentlicht werden, werden von dem Warteschlangenmanager weitergeleitet, mit dem sie verbunden ist, direkt zu jedem Warteschlangenmanager, auf dem eine übereinstimmende Subskription vorhanden ist.

Das folgende Diagramm zeigt einen WS-Manager-Cluster, der derzeit nicht für Publish/Subscribe- oder Punkt-zu-Punkt-Aktivitäten verwendet wird. Es ist zu beachten, dass Warteschlangenmanager im Cluster jeweils nur eine Verbindung zu und von den Warteschlangenmanagern mit vollständigem Repository herstellt.

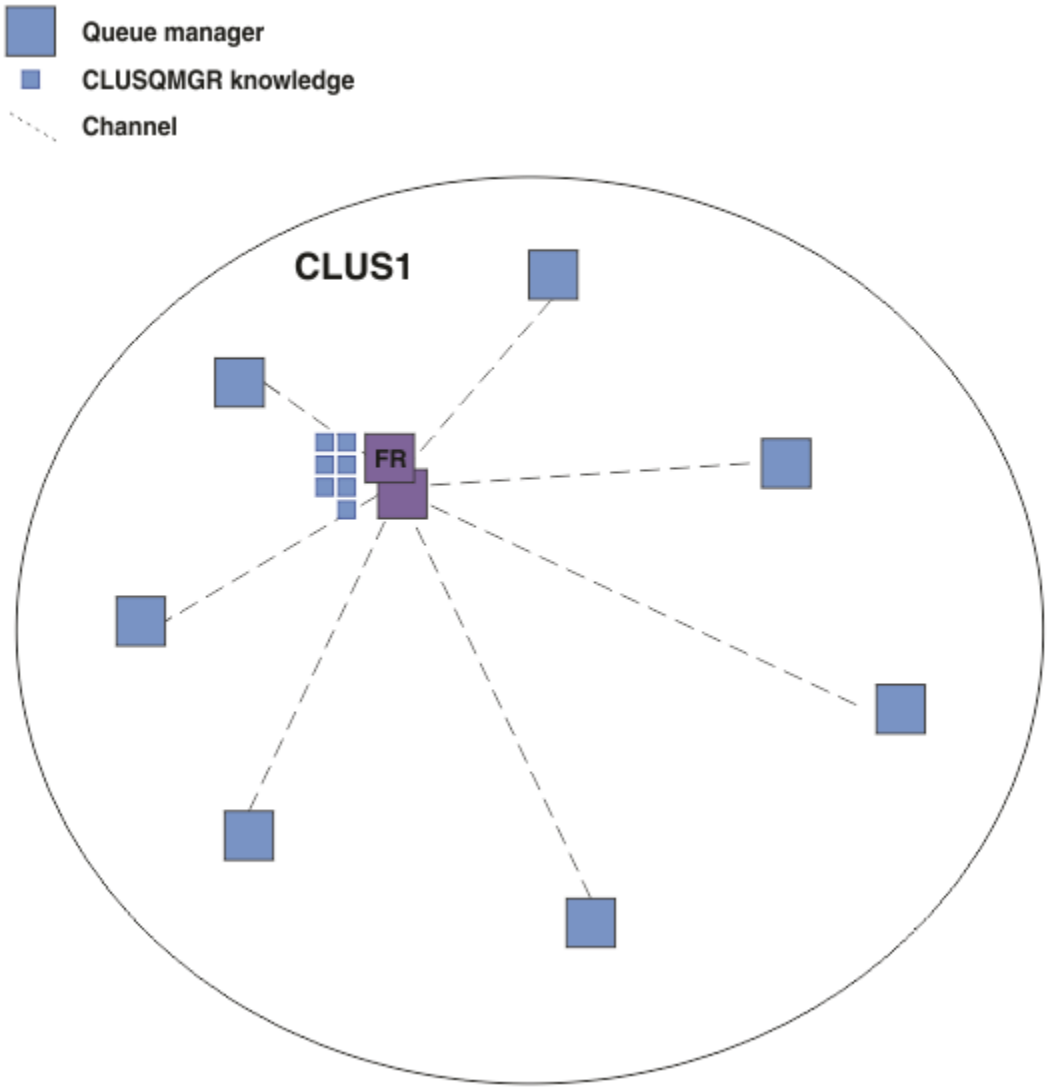


Abbildung 16. Ein WS-Manager-Cluster

Damit Veröffentlichungen zwischen Warteschlangenmanagern in einem direkt weitergeleiteten Cluster fließen können, müssen Sie eine Verzweigung der Themenstruktur wie im Abschnitt Publish/Subscribe-Cluster konfigurieren beschrieben und *direktes Routing* (Standardeinstellung) angeben.

In einem direkt weitergeleiteten Publish/Subscribe-Cluster definieren Sie das Themenobjekt auf jedem WS-Manager im Cluster. Wenn Sie dies tun, werden die Kenntnisse über das Objekt und die Kenntnisse aller anderen Warteschlangenmanager im Cluster automatisch von den vollständigen WS-Managern in den WS-Managern in alle Warteschlangenmanager des Clusters übertragen. Dies geschieht, bevor ein WS-Manager auf das Thema verweist:

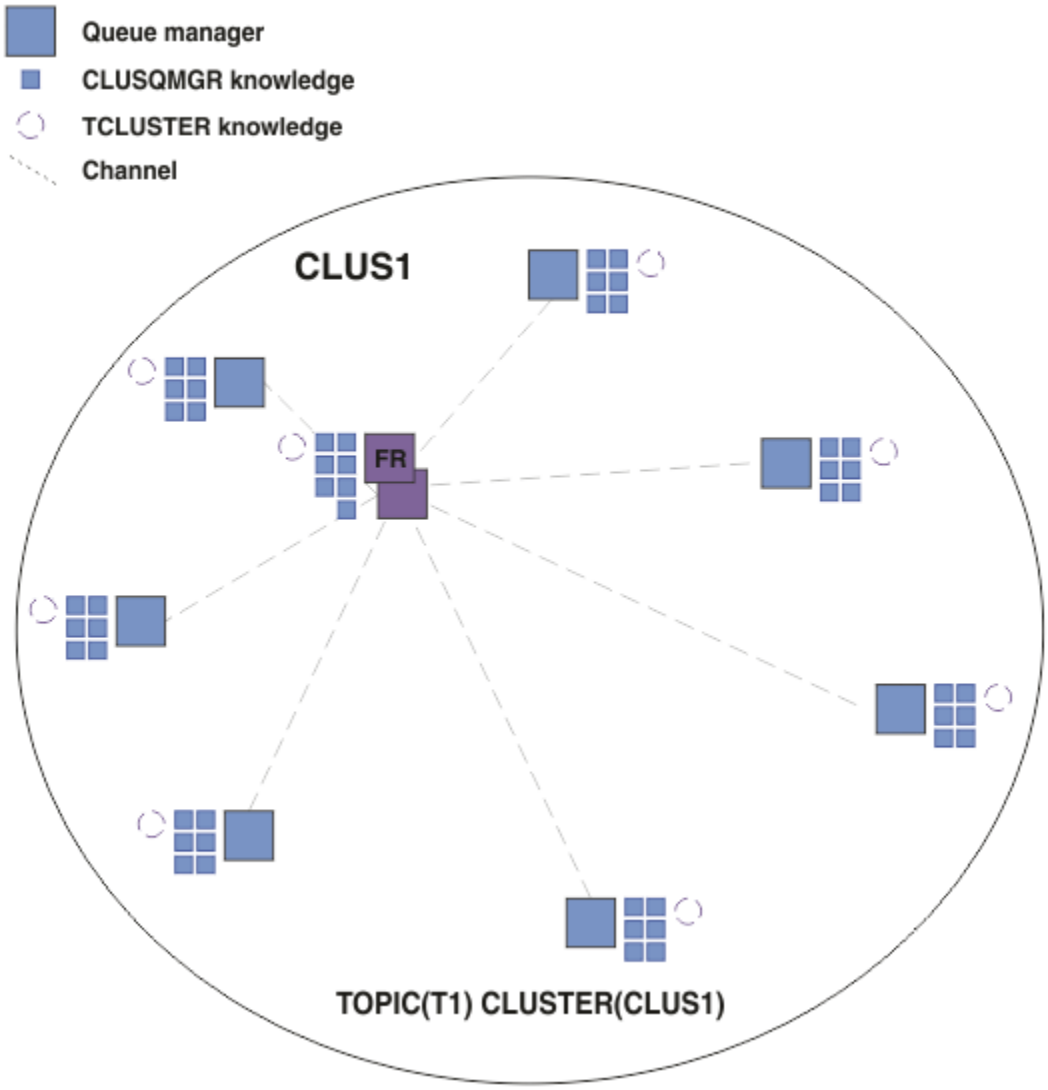


Abbildung 17. Ein Direct-Routing-Publish/Subscribe-Cluster

Wenn eine Subskription erstellt wird, erstellt der Warteschlangenmanager, der die Subskription enthält, einen Kanal zu jedem WS-Manager im Cluster und sendet Details zur Subskription. Dieses verteilte Wissen über Abonnements wird durch ein Proxy-Abonnement auf jedem Warteschlangenmanager dargestellt. Wenn eine Veröffentlichung auf einem Warteschlangenmanager im Cluster erstellt wird, der mit der Themenzeichenfolge dieser Proxy-Subskription übereinstimmt, wird ein Clusterkanal vom Publisher-Warteschlangenmanager zu jedem Warteschlangenmanager eingerichtet, der eine Subskription hostet, und die Nachricht wird an jeden Warteschlangenmanager gesendet.

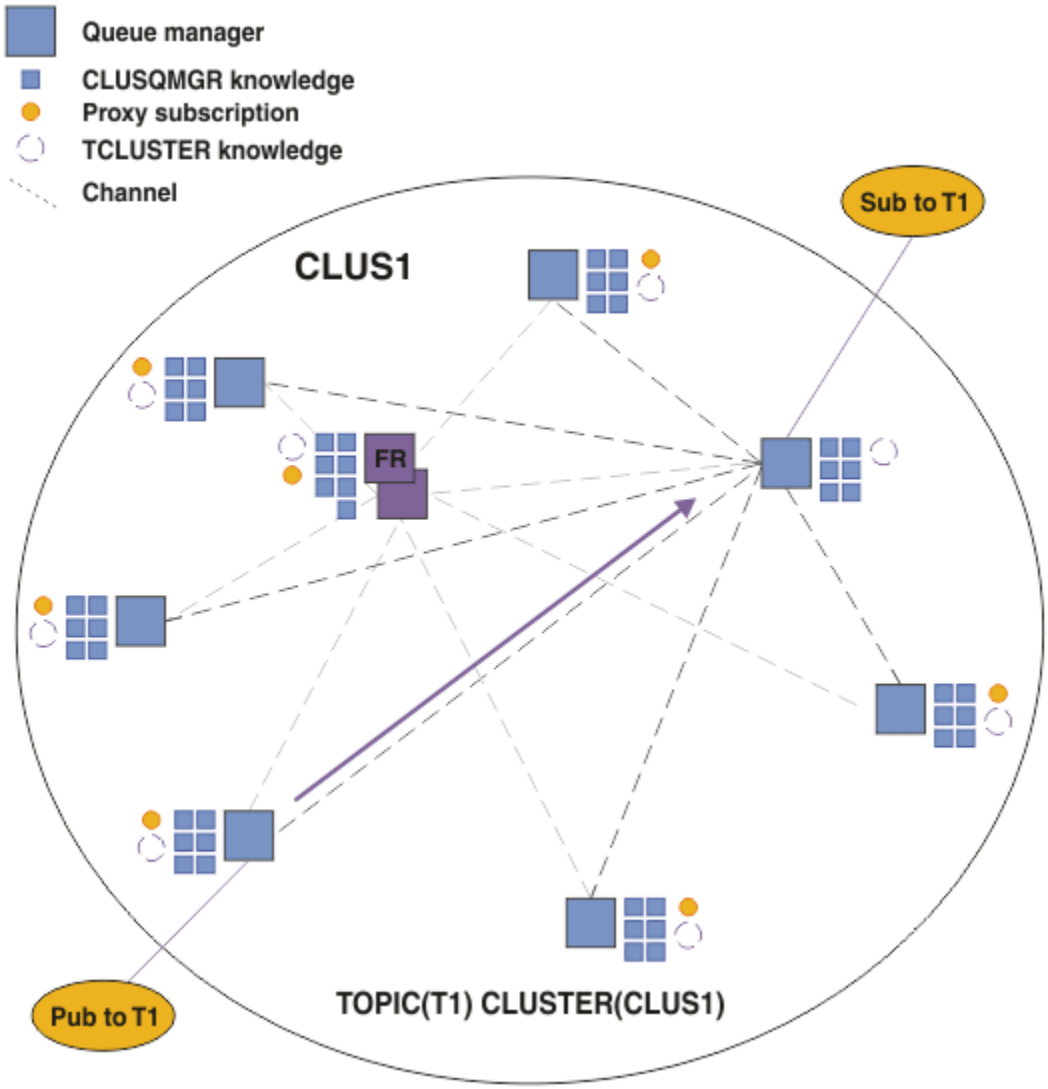


Abbildung 18. Ein direkt weitergeleitete Publish/Subscribe-Cluster mit einem Publisher und einem Subskribenten zu einem Cluster-Thema

Die direkte Weiterleitung von Veröffentlichungen an Subskriptionswarteschlangenmanager vereinfacht die Konfiguration und minimiert die Latenzzeit bei der Bereitstellung von Veröffentlichungen zu Subskriptionen.

Abhängig von der Position der Subskriptionen und Publisher kann Ihr Cluster jedoch schnell vollständig miteinander verbunden werden, wobei jeder WS-Manager eine direkte Verbindung zu jedem anderen Warteschlangenmanager hat. Dies kann in Ihrer Umgebung akzeptabel sein oder nicht. Auch wenn die Gruppe der Themenzeichenfolgen, die subskribiert werden, häufig geändert wird, kann sich der Systemaufwand für die Weitergabe dieser Informationen zwischen allen Warteschlangenmanagern ebenfalls erheblich ändern. Alle Warteschlangenmanager in einem direkt weitergeleiteten Publish/Subscribe-Cluster müssen in der Lage sein, diese Overheads zu bewältigen.

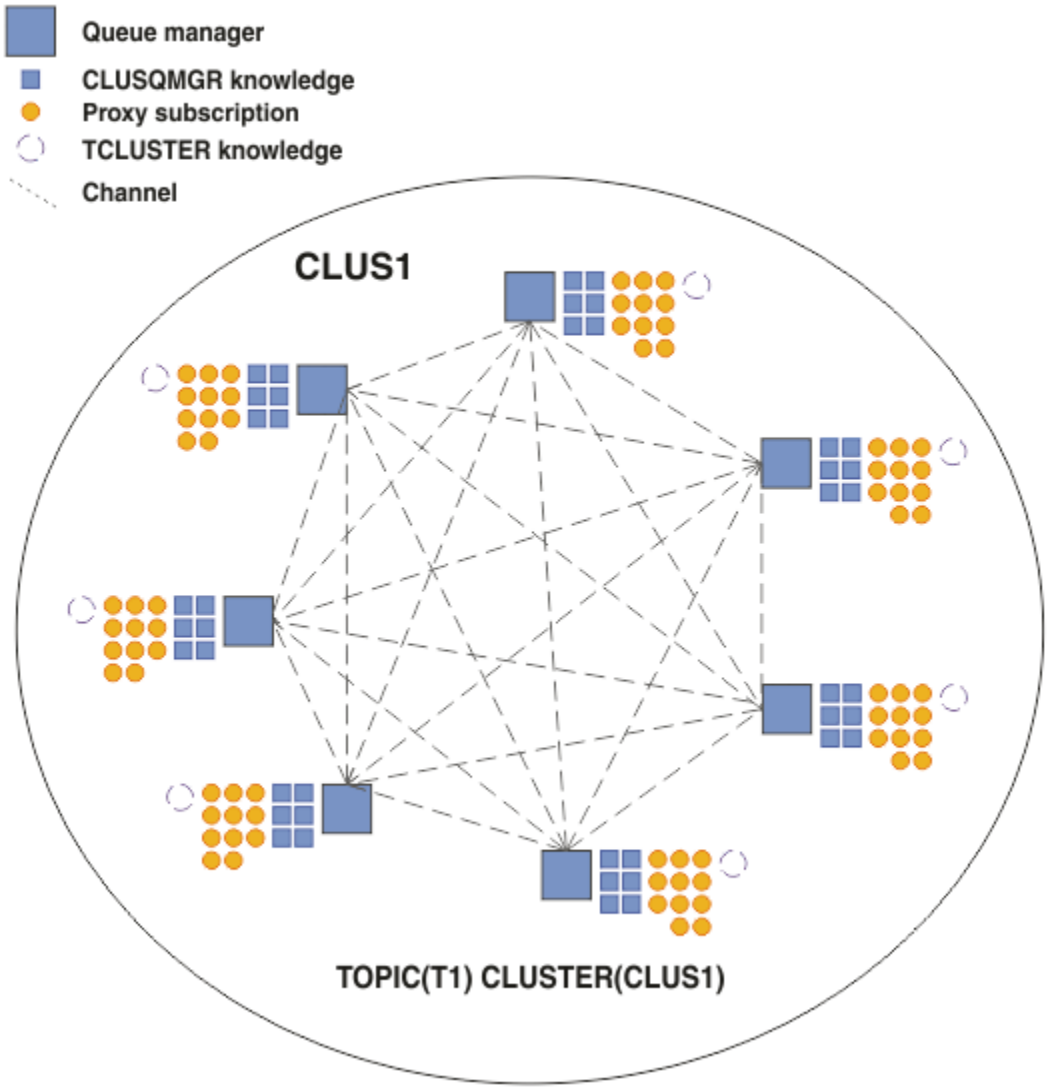


Abbildung 19. Ein direkt weitergeleitete Publish/Subscribe-Cluster, die vollständig miteinander verbunden sind.

Zusammenfassung und weitere Hinweise

Ein direkt weitergeleitete Publish/Subscribe-Cluster benötigt wenig manuellen Eingriff zum Erstellen oder Verwalten von und ermöglicht direktes Routing zwischen Publishern und Subskribenten. Bei bestimmten Konfigurationen ist es in der Regel die am besten geeignete Topologie, insbesondere Cluster mit wenigen Warteschlangenmanagern, oder wenn eine hohe Warteschlangenmanagerkonnektivität akzeptabel ist, und die Subskriptionen selten geändert werden. Es gibt jedoch auch bestimmte Einschränkungen auf Ihrem System:

- Die Auslastung der einzelnen WS-Manager ist proportional zur Gesamtzahl der Warteschlangenmanager im Cluster. Daher können in größeren Clustern einzelne WS-Manager und das System als Ganzes Leistungsprobleme erfahren.
- Standardmäßig werden alle im Cluster subskribierten Themenzeichenfolgen im gesamten Cluster weitergegeben, und die Veröffentlichungen werden nur an ferne Warteschlangenmanager weitergegeben, die über eine Subskription für das zugeordnete Thema verfügen. Daher können schnelle Änderungen an der Gruppe von Subskriptionen zu einem Begrenzungsfaktor werden. Sie können dieses Standardverhalten ändern und stattdessen alle Publizierungsveröffentlichungen an alle Warteschlangenmanager weitergeben, wodurch die Notwendigkeit von Proxy-Subskriptionen entfällt. Dadurch reduziert sich der Austausch der Subskriptionsdaten, der durch Veröffentlichungen bewirkte Datenverkehr sowie mögli-

cherweise die Anzahl der von den Warteschlangenmanagern eingerichteten Kanäle erhöht sich hingegen. Weitere Informationen finden Sie im Abschnitt Subskriptionsleistung in Publish/Subscribe-Netzen.

Anmerkung: Eine ähnliche Einschränkung gilt auch für Hierarchien.

- Aufgrund der Vernetzung von Publish/Subscribe-Queue-Managern dauert es, bis Proxy-Subskriptionen sich über alle Knoten im Netz ausbreiten. Ferne Veröffentlichungen beginnen nicht unbedingt sofort, wenn sie sofort subskribiert werden, so dass frühzeitige Veröffentlichungen möglicherweise nicht nach einer Subskription für eine neue Themenzeichenfolge gesendet werden. Sie können die Probleme, die durch die Subskriptionsverzögerung verursacht werden, entfernen, indem alle Veröffentlichungen an alle Warteschlangenmanager weitergegeben werden, wodurch die Notwendigkeit von Proxy-Subskriptionen entfernt wird. Weitere Informationen finden Sie im Abschnitt Subskriptionsleistung in Publish/Subscribe-Netzen.

  Anmerkung: Diese Einschränkung gilt auch für Hierarchien.

Bevor Sie direktes Routing verwenden, untersuchen Sie die alternativen Ansätze, die in „Thema Host-Routing in Publish/Subscribe-Clustern" auf Seite 90 und „Routing in Publish/Subscribe-Hierarchien" auf Seite 116 detailliert beschrieben sind.

Thema Host-Routing in Publish/Subscribe-Clustern

Veröffentlichungen von Nicht-Hosting-WS-Managern im Cluster werden über den Host-WS-Manager an jeden Warteschlangenmanager im Cluster mit einer übereinstimmenden Subskription weitergeleitet.

Eine Einführung dazu, wie Nachrichten zwischen Warteschlangenmanagern in Publish/Subscribe-Hierarchien und Clustern weitergeleitet werden, finden Sie unter Verteilte Publish/Subscribe-Netze.

Um das Verhalten und die Vorteile von Topic-Host-Routing zu verstehen, ist es am besten, „Direktes Routing in Publish/Subscribe-Clustern" auf Seite 85 zu verstehen.

Der Publish/Subscribe-Cluster eines Topic-Hosts verhält sich wie folgt:

- Gruppierte verwaltete Themenobjekte werden manuell auf einzelnen Warteschlangenmanagern im Cluster definiert. Diese werden als *Topic-Host-Warteschlangenmanager* bezeichnet.
- Wenn eine Subskription für einen Cluster-WS-Manager ausgeführt wird, werden Kanäle vom Subskriptionshostwarteschlangenmanager zum Topic-Host-Warteschlangenmanager erstellt, und Proxy-Subskriptionen werden nur auf den Warteschlangenmanagern erstellt, die das Thema enthalten.
- Wenn eine Anwendung Informationen zu einem Thema veröffentlicht, leitet der verbundene Warteschlangenmanager die Veröffentlichung immer an einen Warteschlangenmanager weiter, der das Thema hostet, das es an alle WS-Manager im Cluster weiterleitet, die übereinstimmende Subskriptionen für das Thema haben.

Dieser Vorgang wird in den folgenden Beispielen näher erläutert.

Thema Hostweiterleitung unter Verwendung eines einzelnen Themenhosts

Damit Veröffentlichungen zwischen Warteschlangenmanagern in einem Topic-Host-Routing-Cluster fließen können, müssen Sie eine Verzweigung der Themenstruktur wie im Abschnitt Publish/Subscribe-Cluster konfigurieren beschrieben erstellen und *Topic-Host-Routing* angeben.

Es gibt eine Reihe von Gründen, ein Topic-Host-Topic-Objekt auf mehreren Warteschlangenmanagern in einem Cluster zu definieren. Der Einfachheit jedoch beginnen wir mit einem einzigen Themenhost zu beginnen.

Das folgende Diagramm zeigt einen WS-Manager-Cluster, der derzeit nicht für Publish/Subscribe- oder Punkt-zu-Punkt-Aktivitäten verwendet wird. Es ist zu beachten, dass Warteschlangenmanager im Cluster jeweils nur eine Verbindung zu und von den Warteschlangenmanagern mit vollständigem Repository herstellt.

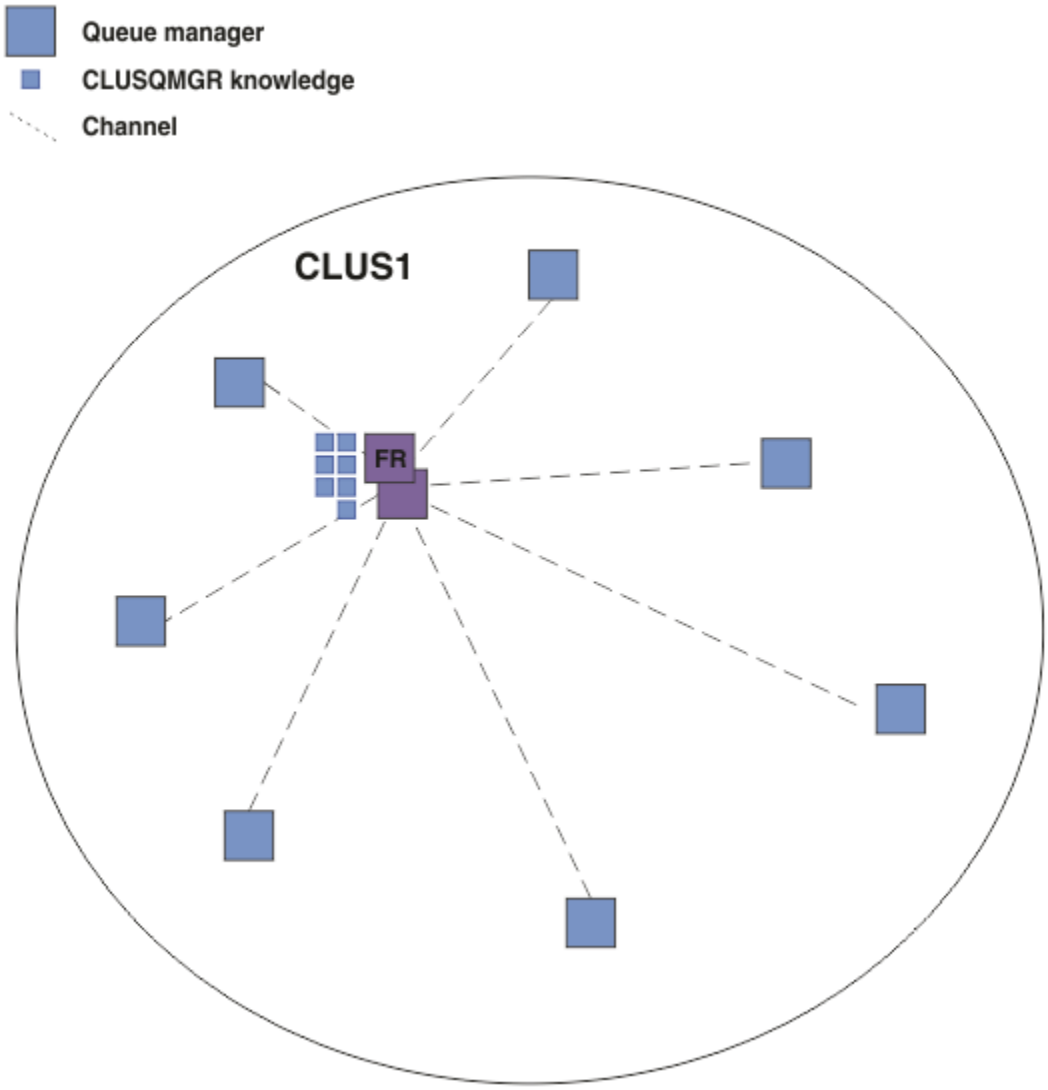


Abbildung 20. Ein WS-Manager-Cluster

In einem Publish/Subscribe-Cluster des Topic-Hosts definieren Sie das Themenobjekt auf einem bestimmten Warteschlangenmanager im Cluster. Der Publish/Subscribe-Datenverkehr fließt dann durch diesen Warteschlangenmanager und macht ihn zu einem kritischen Warteschlangenmanager im Cluster und erhöht seine Auslastung. Aus diesen Gründen wird es nicht empfohlen, einen vollständigen WS-Manager-Repository zu verwenden, aber einen anderen WS-Manager im Cluster zu verwenden. Wenn Sie das Themenobjekt auf dem Host-WS-Manager definieren, wird die Kenntnis des Objekts und seines Hosts automatisch von den vollständigen WS-Managern des Repositorys an alle anderen WS-Manager im Cluster übertragen. Beachten Sie, dass im Gegensatz zu *direktes Routing* jeder Warteschlangenmanager nicht zu jedem anderen WS-Manager im Cluster gehört.

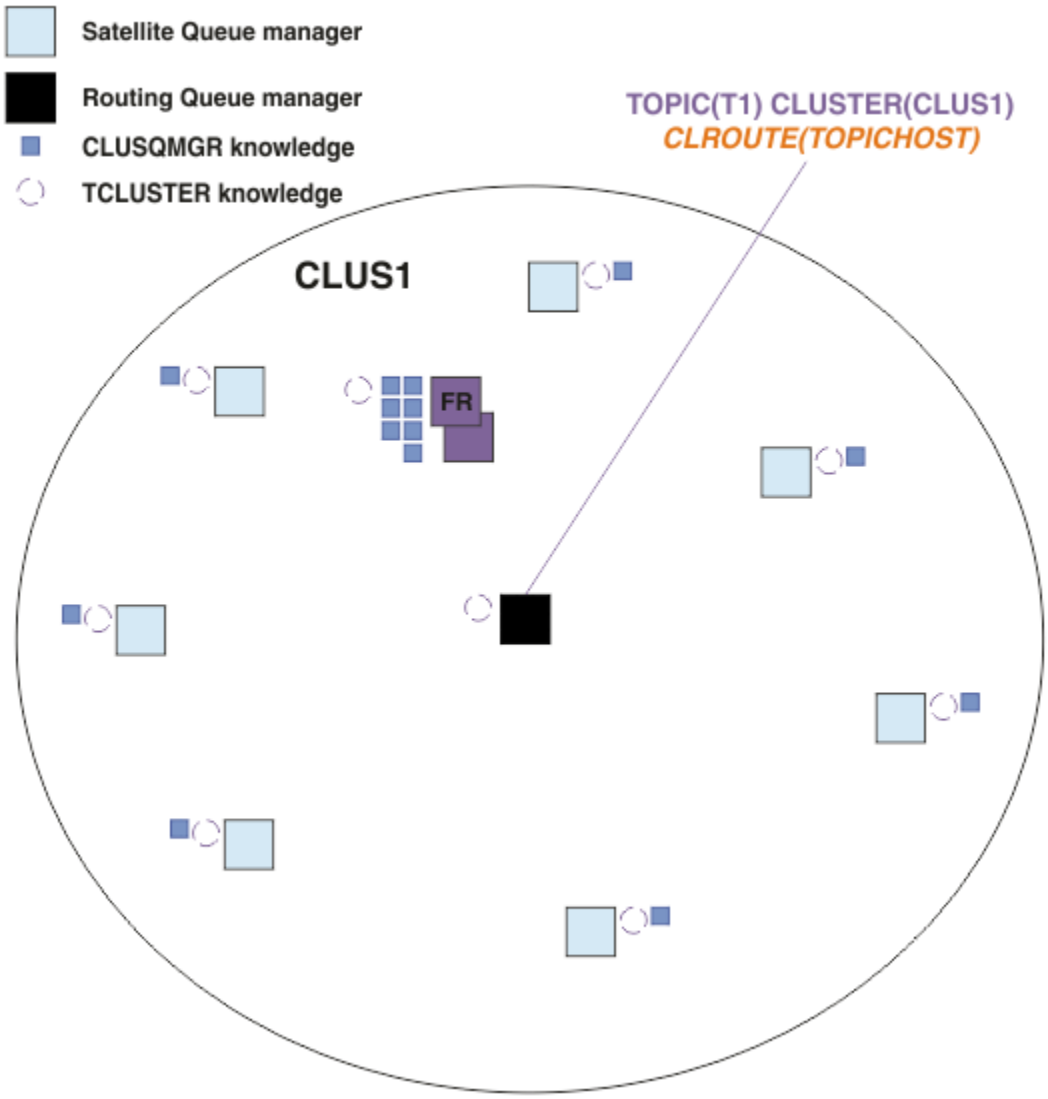


Abbildung 21. Ein Topic-Host-Publish/Subscribe-Cluster mit einem Thema, das auf einem Topic-Host definiert ist

Wenn eine Subskription auf einem Warteschlangenmanager erstellt wird, wird ein Kanal zwischen dem subskribierenden Warteschlangenmanager und dem Topic-Host-Warteschlangenmanager erstellt. Der subskribierende Warteschlangenmanager stellt nur eine Verbindung zum Topic-Host-Warteschlangenmanager her und sendet die Details der Subskription (in Form einer *Proxy-Subskription*). Der Topic-Host-WS-Manager leitet diese Subskriptionsinformationen nicht an alle weiteren Warteschlangenmanager im Cluster weiter.

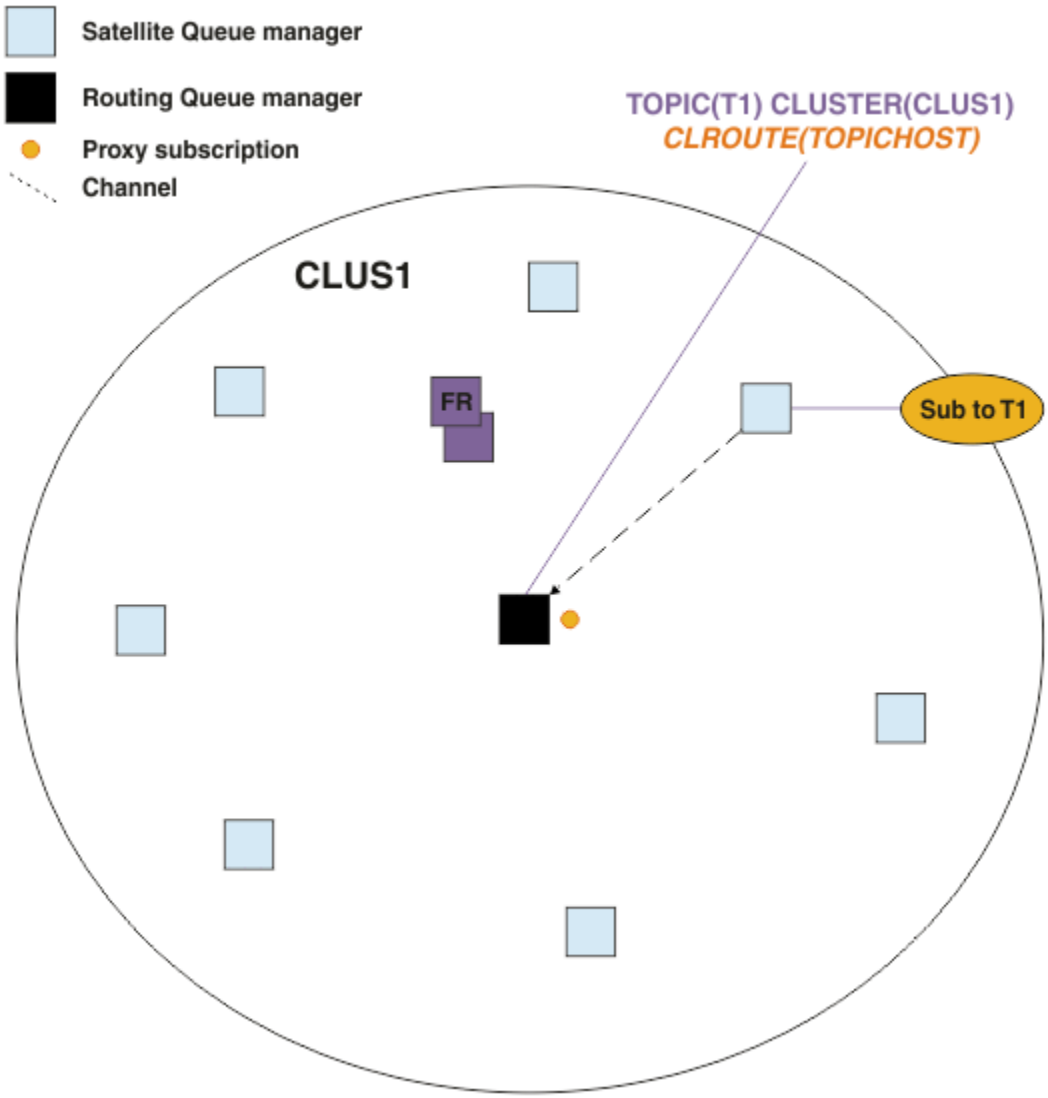


Abbildung 22. Ein Topic-Host-Publish/Subscribe-Cluster mit einem Thema, das auf einem Topic-Host definiert ist, und einen Subskribenten

Wenn eine Veröffentlichungsanwendung eine Verbindung zu einem anderen Warteschlangenmanager herstellt und eine Nachricht veröffentlicht wird, wird ein Kanal zwischen dem Veröffentlichungswarteschlangenmanager und dem Topic-Host-Warteschlangenmanager erstellt, und die Nachricht wird an diesen Warteschlangenmanager weitergeleitet. Der Veröffentlichungswarteschlangenmanager hat keine Kenntnis von Subskriptionen auf anderen WS-Managern im Cluster, daher wird die Nachricht auch dann an den Topic-Host-Warteschlangenmanager weitergeleitet, wenn es keine Subskribenten zu diesem Thema im Cluster gibt. Der Veröffentlichungswarteschlangenmanager stellt eine Verbindung nur mit dem Topic-Host-Warteschlangenmanager her. Veröffentlichungen werden, falls vorhanden, über den Themenhost an die subskribierenden Warteschlangenmanager weitergeleitet.

Subskriptionen auf demselben Warteschlangenmanager wie der Bereitsteller werden direkt erfüllt, ohne dass die Nachrichten zuerst an einen Topic-Host-Warteschlangenmanager gesendet werden.

Beachten Sie, dass Sie aufgrund der kritischen Rolle, die jeder Topic-Host-Warteschlangenmanager gespielt hat, Warteschlangenmanager auswählen müssen, die die Anforderungen zum Laden, Verfügbarkeits-und Konnektivitätsanforderungen des Topic-Hosts verarbeiten können.

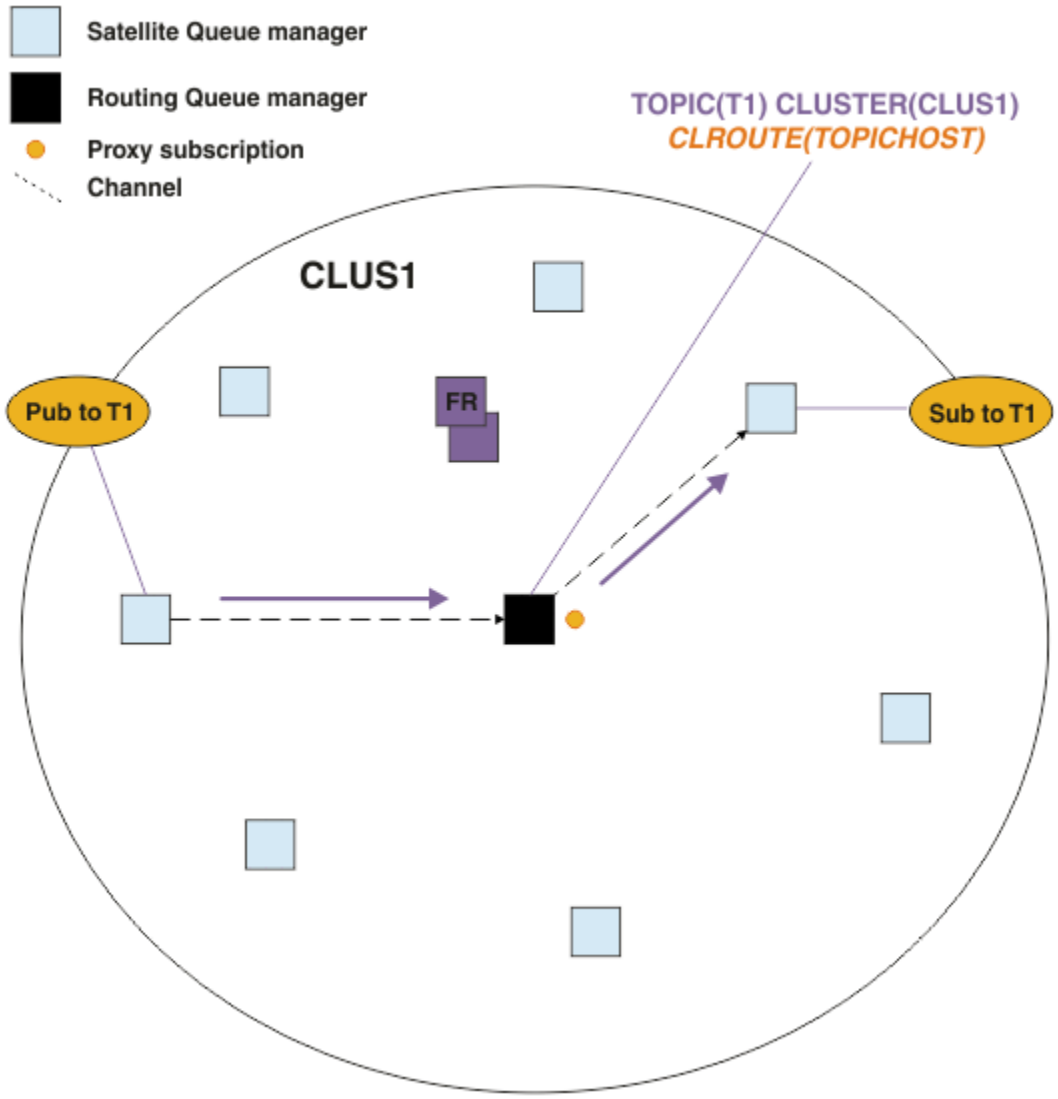


Abbildung 23. Ein Topic-Host-Publish/Subscribe-Cluster mit einem Topic, einem Subskribenten und einem Publisher

Unterteilung der Themenstruktur auf mehrere Warteschlangenmanager

Ein weitergeleitete Topic-Host-Warteschlangenmanager ist nur für die Subskriptionswissens-und Veröffentlichungsnachrichten zuständig, die sich auf die Verzweigung der Themenstruktur beziehen, für die das verwaltete Themenobjekt konfiguriert ist. Wenn verschiedene Publish/Subscribe-Anwendungen im Cluster verwendet werden, können Sie verschiedene WS-Manager für die verschiedenen Clusterverzweigungen der Themenstruktur konfigurieren. Dies ermöglicht die Skalierung, indem der Veröffentlichungsdatenverkehr, die Subskriptionskenntnisse und die Kanäle auf den einzelnen Topic-Host-WS-Managern im Cluster reduziert werden. Sie sollten diese Methode für unterschiedliche Bereiche mit hohem Datenvolumen verwenden, die in der Themenstruktur enthalten sind:

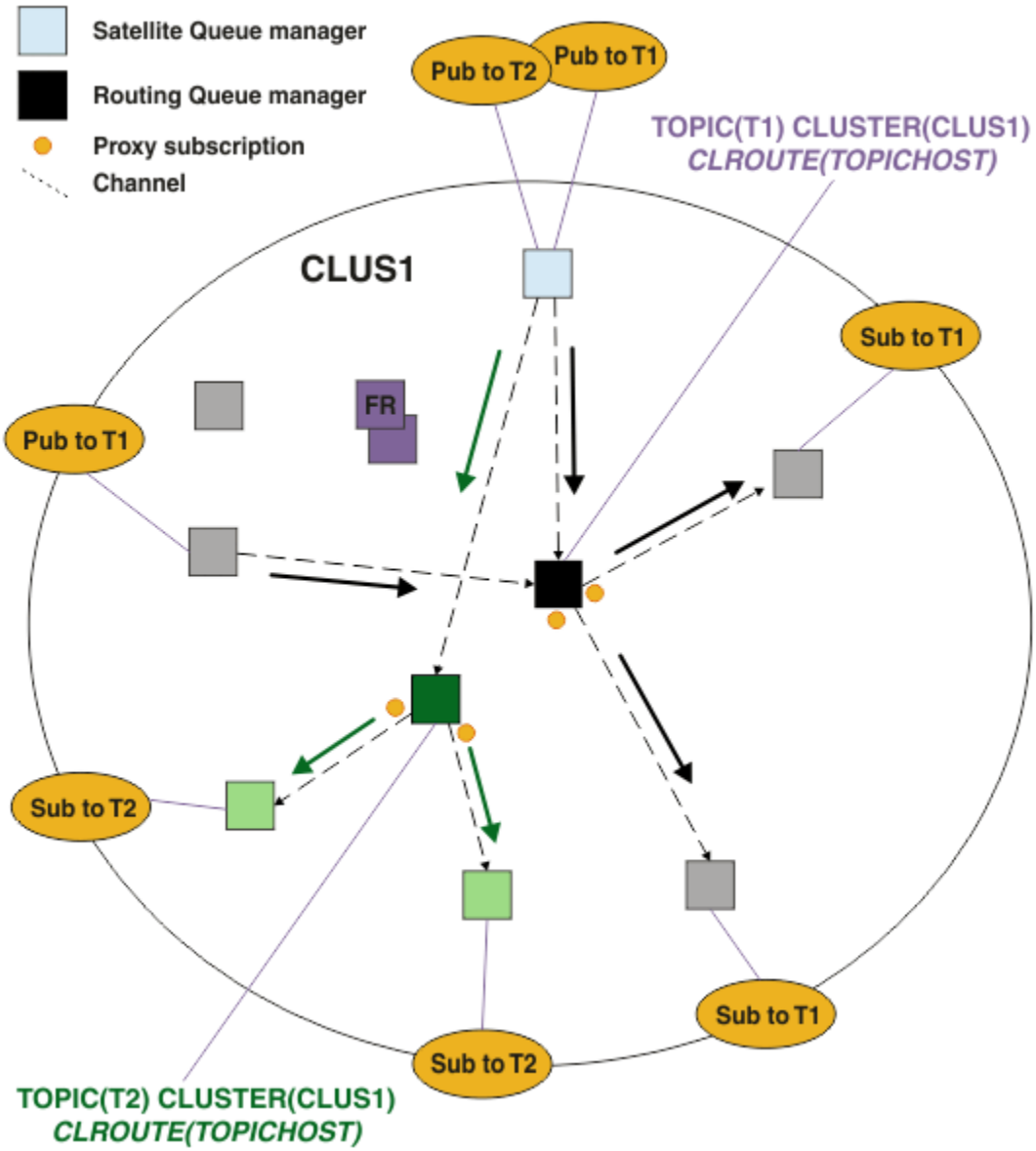


Abbildung 24. Ein Topic-Host-Publish/Subscribe-Cluster mit zwei Themen, die jeweils auf einem Themenhost definiert sind

Wenn Sie beispielsweise die in Themenstrukturen beschriebenen Themen verwenden und das Thema T1 mit der Themenzeichenfolge `/USA/Alabama` und das Thema T2 mit der Themenzeichenfolge `/USA/Alaska` konfiguriert wurde, wird eine in `/USA/Alabama/Mobile` veröffentlichte Nachricht über den Warteschlangenmanager, auf dem sich T1 befindet, und eine in `/USA/Alaska/Juneau` veröffentlichte Nachricht über den Warteschlangenmanager, auf dem sich T2 befindet, weitergeleitet.

Anmerkung: Sie können keine einzelne Subskription über mehrere Clusterverzweigungen der Themenstruktur erstellen, indem Sie in der Themenstruktur ein höheres Platzhalterzeichen verwenden als die Punkte, die in Gruppen zusammengefasst sind. Siehe Platzhalter für Platzhalterzeichen .

Thema Hostweiterleitung unter Verwendung mehrerer Topic-Hosts für ein einzelnes Thema

Wenn ein einzelner Warteschlangenmanager die Verantwortung für die Weiterleitung eines Themas hat und dass der Warteschlangenmanager nicht mehr verfügbar oder nicht in der Lage ist, die Auslastung zu verarbeiten, werden die Veröffentlichungen nicht zeitnah an die Subskriptionen weitergeleitet.

Wenn Sie mehr Ausfallsicherheit, Skalierbarkeit und Lastausgleich benötigen, als Sie bei der Definition eines Themas in nur einem Warteschlangenmanager ein Thema definieren, können Sie ein Thema in mehr als einem Warteschlangenmanager definieren. Jede einzelne veröffentlichte Nachricht wird über einen einzigen Themenhost weitergeleitet. Wenn mehrere übereinstimmende Topic-Hostdefinitionen vorhanden sind, wird einer der Themenhosts ausgewählt. Die Auswahl erfolgt auf die gleiche Weise wie für Clusterwarteschlangen. Dadurch können Nachrichten an verfügbare Topic-Hosts weitergeleitet werden, so dass keine vorhanden sind, die nicht verfügbar sind, und es ermöglicht, dass die Nachrichtenlast auf mehrere Topic-Host-WS-Manager und -Kanäle verteilt wird. Wenn Sie mehrere Topic-Hosts für dasselbe Thema im Cluster verwenden, wird die Sortierung über mehrere Nachrichten jedoch nicht aufrechterhalten.

Das folgende Diagramm zeigt einen Topic-Host-Routing-Cluster, in dem das gleiche Thema auf zwei Warteschlangenmanagern definiert wurde. In diesem Beispiel senden die subskribierenden Warteschlangenmanager Informationen zu dem subskribierten Thema an beide Topic-Host-Warteschlangenmanager in Form einer Proxy-Subskription:

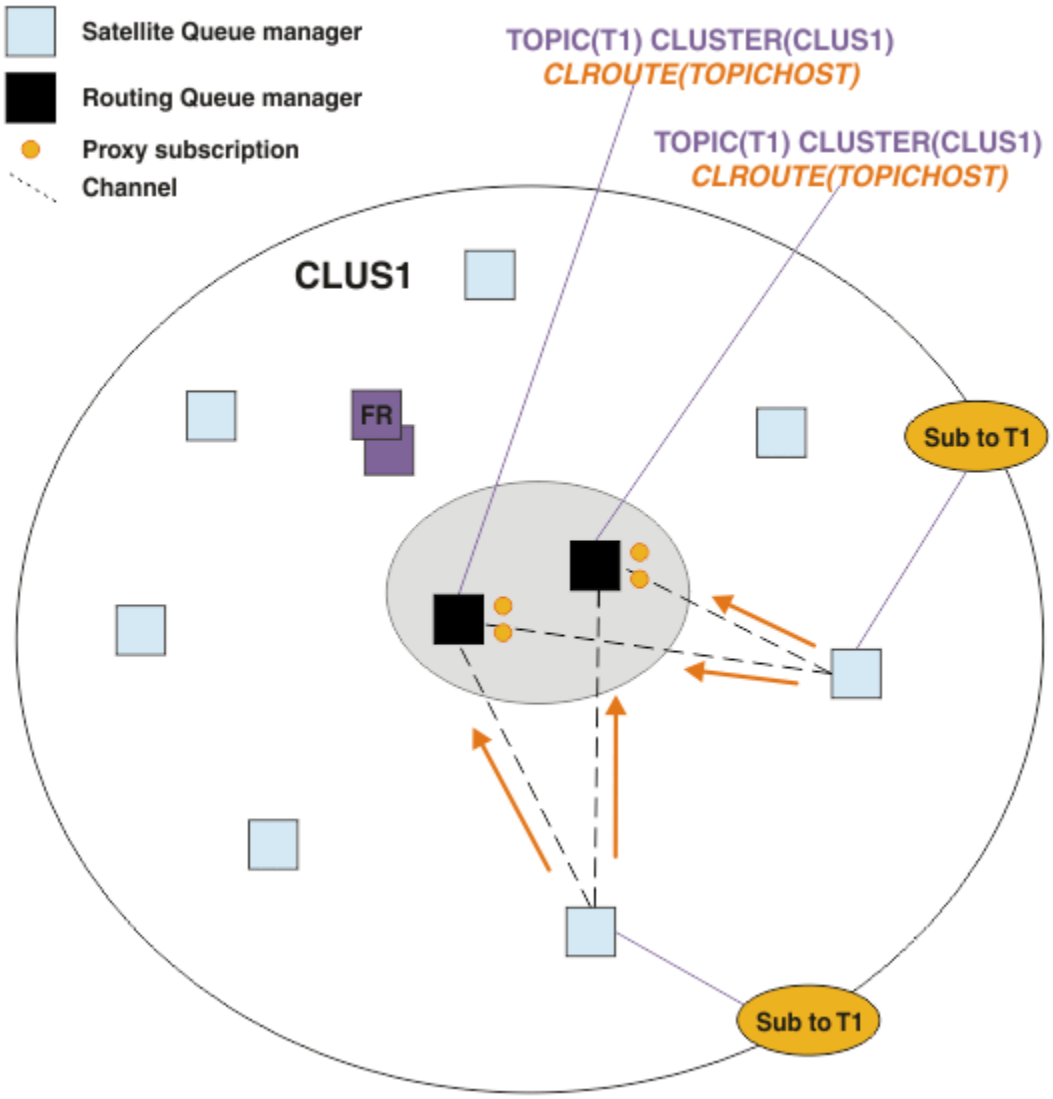


Abbildung 25. Proxy-Subskriptionen in einem Publish/Subscribe-Cluster mit mehreren Topics erstellen

Wenn eine Veröffentlichung von einem Nicht-Hosting-Warteschlangenmanager erstellt wird, sendet der Warteschlangenmanager eine Kopie der Veröffentlichung an *einen* des Topic-Host-WS-Managers für dieses Thema. Das System wählt den Host basierend auf dem Standardverhalten des Algorithmus für die Clusterauslastungsverwaltung aus. In einem typischen System nähert sich dies einer Round-Robin-Verteilung über die einzelnen Themenhostwarteschlangenmanager an. Es gibt keine Affinität zwischen

Nachrichten aus derselben Veröffentlichungsanwendung. Dies entspricht der Verwendung eines Clusterbindungs-Typs `NOTFIXED` .

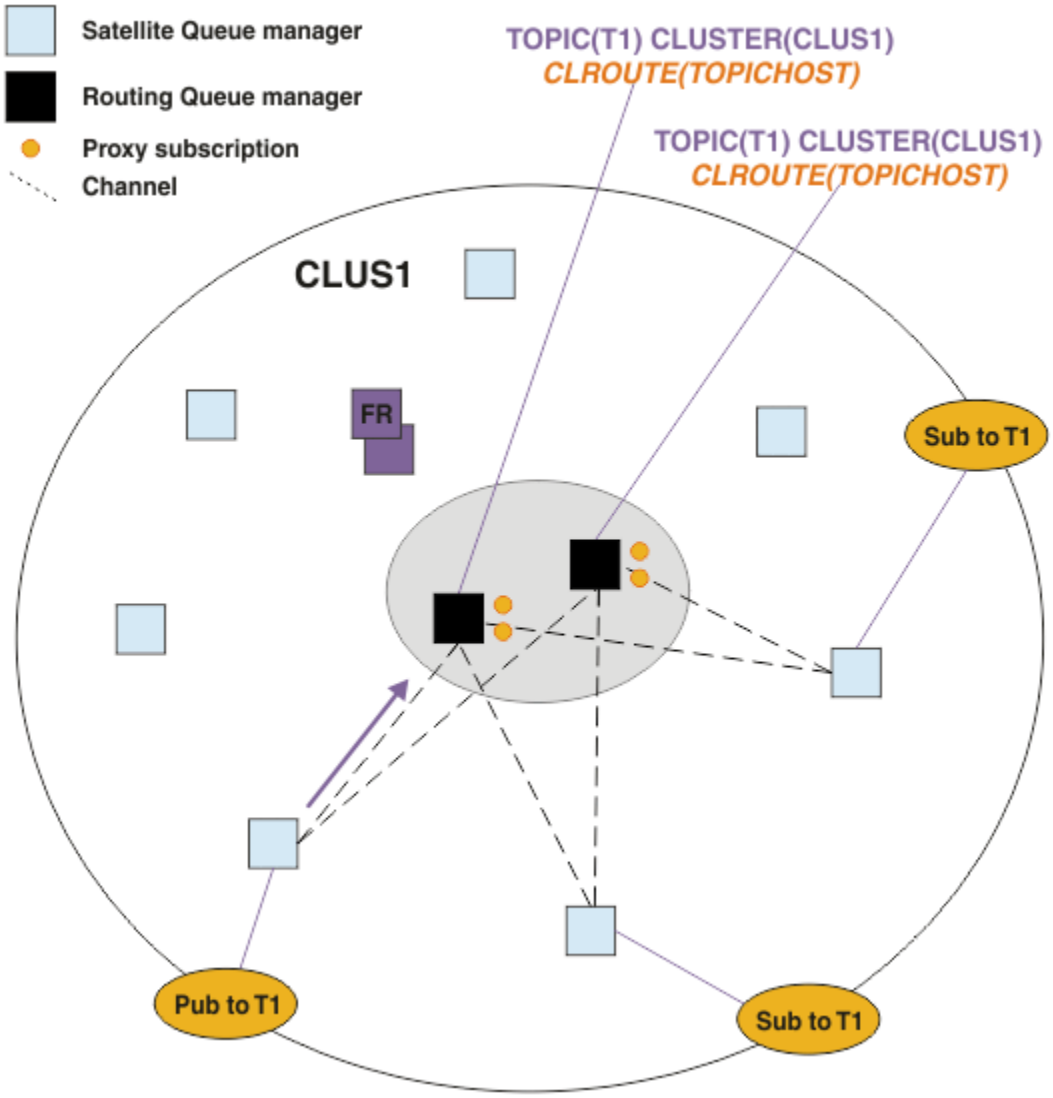


Abbildung 26. Empfangen von Veröffentlichungen in einem Publish/Subscribe-Cluster mit mehreren Themenhost

Inbound-Veröffentlichungen zum ausgewählten Topic-Host-Warteschlangenmanager werden dann an alle WS-Manager weitergeleitet, die eine übereinstimmende Proxy-Subskription registriert haben:

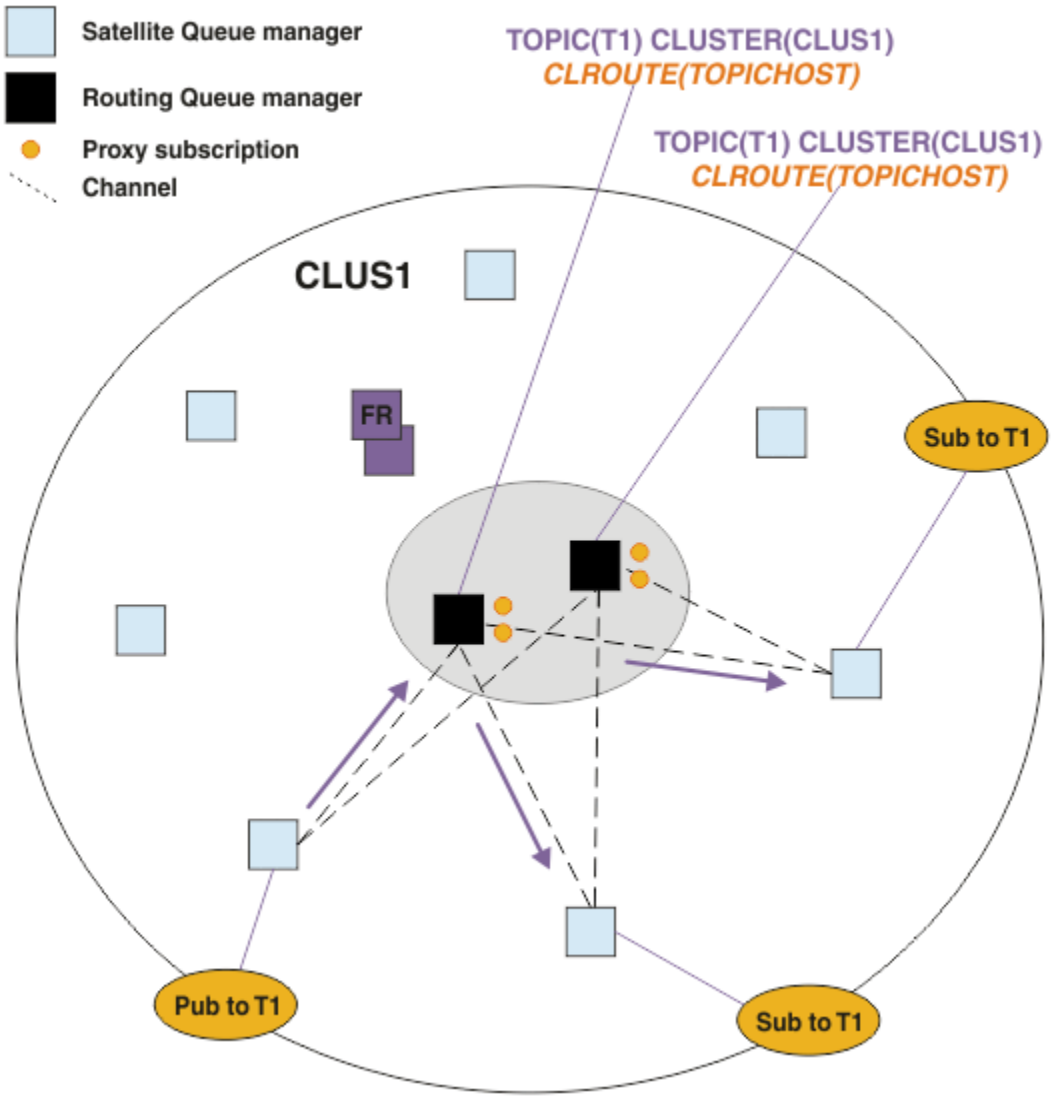


Abbildung 27. Weiterleiten von Veröffentlichungen an Subskribenten in einem Publish/Subscribe-Cluster mit mehreren Themen

Subskriptionen und Publiziern lokal für einen Topic-Host-Warteschlangenmanager erstellen

Die oben genannten Beispiele zeigen das Routing zwischen Publishern und Subskribenten auf WS-Managern, die keine verwalteten Themenobjekte im Host verwalten. In diesen Topologien benötigen Nachrichten mehrere *Hops* , um die Subskriptionen zu erreichen.

Wenn der zusätzliche Hop nicht erwünscht ist, kann es sinnvoll sein, wichtige Publisher mit Topic-Hosting-Warteschlangenmanagern zu verbinden. Wenn es jedoch mehrere Themenhosts für ein Thema und nur einen Bereitsteller gibt, wird der gesamte Veröffentlichungsdatenverkehr über den Topic-Host-Warteschlangenmanager weitergeleitet, mit dem der Bereitsteller verbunden ist.

In ähnlicher Weise, wenn es Schlüsselsubskriptionen gibt, können diese sich auf einem Topic-Host-Warteschlangenmanager befinden. Wenn es jedoch mehrere Hosts des weitergeleiteten Themas gibt, wird der zusätzliche Hop nur durch einen Teil der Veröffentlichungen vermieden, wobei der Rest zuerst durch die anderen Topic-Host-Warteschlangenmanager weitergeleitet wird.

Topologien wie diese werden hier weiter beschrieben: Topic-Host-Routing mit zentralisierten Publishern oder Subskribenten .

Anmerkung: Eine spezielle Planung ist erforderlich, wenn die Konfiguration des weitergeleiteten Topics geändert wird, wenn Publisher oder Subskriptionen mit Routing-Topic-Hosts gemeinsam lokalisiert werden. Weitere Informationen finden Sie im Abschnitt Einem Topic-Host-Cluster zusätzliche Topic-Hosts hinzufügen .

Zusammenfassung und weitere Hinweise

Ein Topic-Host-Publish/Subscribe-Cluster gibt Ihnen präzise Kontrolle darüber, welche Warteschlangenmanager die einzelnen Themen enthalten, und diese Warteschlangenmanager werden zu den *Routing* -Warteschlangenmanagern für diese Verzweigung in der Themenstruktur. Außerdem müssen Warteschlangenmanager ohne Subskriptionen oder Publisher keine Verbindung zu den Topic-Host-Warteschlangenmanagern herstellen, und Warteschlangenmanager mit Subskriptionen müssen keine Verbindung zu Warteschlangenmanagern herstellen, die kein Thema enthalten. Diese Konfiguration kann die Anzahl der Verbindungen zwischen WS-Managern im Cluster und die Menge der Informationen, die zwischen WS-Managern übertragen werden, erheblich reduzieren. Dies gilt insbesondere für große Cluster, in denen nur eine Untergruppe von Warteschlangenmanagern Publish/Subscribe-Arbeiten ausführt. Diese Konfiguration gibt Ihnen auch die Möglichkeit, die Auslastung einzelner Warteschlangenmanager im Cluster zu steuern, so dass Sie z. B. hochaktive Themen auf leistungsfähigeren und ausfallsicheren Systemen hosten können. Für bestimmte Konfigurationen-insbesondere größere Cluster-ist es in der Regel eine besser geeignete Topologie als *direktes Routing* .

Beim TOPICHOST-Routing gelten für Ihr System jedoch bestimmte Einschränkungen:

- Die Systemkonfiguration und -wartung muss sorgfältiger geplant werden als dies beim DIRECT-Routing erforderlich ist. Sie müssen in der Themenstruktur die Punkte festlegen, die zu Clustern zusammengeschlossen werden sollen; ebenso müssen Sie festlegen, wo im Cluster sich die Themendefinitionen befinden.
- Wenn ein neues Thema mit TOPICHOST-Routing definiert wird, werden die Informationen wie bei Themen, für die DIRECT-Routing definiert ist, an die Warteschlangenmanager mit vollständigem Repository und von dort direkt an alle Clustermitglieder übertragen. Dadurch werden von den vollständigen Repositorys aus Kanäle zu jedem Clustermitglied gestartet (sofern dies noch nicht geschehen ist).
- Veröffentlichungen werden immer von einem Warteschlangenmanager, bei dem es sich nicht um einen Themenhost handelt, an einen Warteschlangenmanager, der als Themenhost dient, gesendet; dies ist auch dann der Fall, wenn im Cluster keine Subskriptionen vorhanden sind. Wenn daher davon ausgegangen werden kann, dass Subskriptionen vorliegen, oder wenn der Aufwand für die globale Konnektivität und für globale Informationen höher ist als der eventuell zusätzliche Datenverkehr beim Übertragen von Veröffentlichungen, sollten Sie Themen-Routing verwenden.

  Anmerkung: Wie bereits beschrieben, kann das Veröffentlichen von Publishern auf einem Topic-Host dieses Risiko mindern.
- Nachrichten, die auf Warteschlangenmanagern veröffentlicht werden, die keine Hosts sind, gehen nicht direkt an den Warteschlangen, der die Subskription hostet, sondern werden immer über einen TOPICHOST-Warteschlangenmanager weitergeleitet. Dadurch erhöhen sich der Gesamtaufwand für den Cluster und die Latenzzeit bei der Nachrichtenübertragung, wodurch sich die Leistung verschlechtert.

  Anmerkung: Wie bereits beschrieben, können Subskriptionen oder Publisher, die für einen Topic-Host lokal sind, dieses Risiko mindern.
- Die Verwendung nur eines Warteschlangenmanagers als Themenhost stellt einen SPoF (Single Point of Failure) für alle Nachrichten dar, die zu einem Thema veröffentlicht werden. Durch eine Definition mehrerer Themenhosts wird ein solcher SPoF ausgeschlossen. Bei Verwendung mehrerer Hosts ändert sich allerdings die Reihenfolge, in der veröffentlichte Nachrichten für Subskriptionen empfangen werden.
- TOPICHOST-Warteschlangenmanager erzeugen ein zusätzliches Nachrichtenvolumen, weil sie Veröffentlichungsdatenverkehr von mehreren Warteschlangenmanagern verarbeiten müssen. Dieses Volumen kann verringert werden, indem mehrere TOPICHOSTs für ein einzelnes Thema verwendet werden (wobei die Reihenfolge der Nachrichten nicht beibehalten wird) oder indem verschiedene Warteschlangenmanager als Hosts für weitergeleitete Themen für verschiedene Zweige der Themenstruktur verwendet werden.

Bevor Sie Topic-Host-Routing verwenden, untersuchen Sie die alternativen Ansätze in „Direktes Routing in Publish/Subscribe-Clustern” auf Seite 85 und „Routing in Publish/Subscribe-Hierarchien” auf Seite 116.

Publish/Subscribe-Clustering: Bewährte Verfahren

Durch die Verwendung von Clusterthemen wird die Publish/Subscribe-Domäne zwischen der Warteschlange erweitert. Manager einfach, kann aber zu Problemen führen, wenn die Mechanik und die Auswirkungen nicht vollständig sind verstanden. Es gibt zwei Modelle für die gemeinsame Nutzung von Informationen und das Routing von Veröffentlichungen. Implementieren Sie das Modell, das Ihren individuellen Geschäftsanforderungen am besten entspricht, und führt Sie am besten für Ihre Auswahl aus. Cluster.

Die Best-Practice-Informationen in den folgenden Abschnitten bieten nicht eine Gesamtgröße für alle Lösungen an, sondern gemeinsame Ansätze zur Lösung allgemeiner Probleme. Es wird vorausgesetzt, dass Sie ein grundlegendes Verständnis von IBM MQ-Clustern und von Publish/Subscribe-Nachrichtenübermittlung haben und dass Sie mit den Informationen aus Verteilte Publish/Subscribe-Netze und „Publish/Subscribe-Cluster entwerfen” auf Seite 83 vertraut sind.

Wenn Sie einen Cluster für Punkt-zu-Punkt-Messaging verwenden, arbeitet jeder WS-Manager im Cluster auf einer Basis-zu-Know-Basis. Dies bedeutet, dass es nur Informationen zu anderen Clusterressourcen, wie z. B. anderen WS-Managern im Cluster und in Clusterwarteschlangen, findet, wenn Anwendungen, die eine Verbindung zu ihnen herstellen, sie verwenden möchten. Wenn Sie Publish/Subscribe-Messaging zu einem Cluster hinzufügen, wird ein erhöhtes Maß an Informationsaustausch und Konnektivität zwischen Cluster-WS-Managern eingeführt. Um die Best Practices für Publish/Subscribe-Cluster verfolgen zu können, müssen Sie die Auswirkungen dieser Änderung im Verhalten umfassend verstehen.

Um Ihnen die beste Architektur zu ermöglichen, basierend auf Ihren präzisen Bedürfnissen, gibt es zwei Modelle Informationen zur gemeinsamen Nutzung und Veröffentlichung von Veröffentlichungen in Publish/Subscribe-Clustern: *direktes Routing* und *Topic-Host-Routing* . Um das richtige zu machen Auswahl, müssen beide Modelle und die unterschiedlichen Anforderungen, die jeweils Modell genügt. Diese Anforderungen werden in den folgenden Abschnitten erläutert: Verbindung mit „Verteiltes Publish/Subscribe-Netz planen” auf Seite 79:

- „Gründe für die Begrenzung der Anzahl der Cluster-WS-Manager, die in Publish/Subscribe-Aktivität” auf Seite 100
- „Vorgehensweise bei der Entscheidung, welche Themen in einem Cluster” auf Seite 101
- „Wie Sie Ihr System als Größe” auf Seite 102
- „Bereitsteller-und Subskriptionsposition” auf Seite 103
- „Veröffentlichungsdatenverkehr” auf Seite 103
- „Subskriptionsänderung und dynamische Themenzeichenfolgen” auf Seite 104

Gründe für die Begrenzung der Anzahl der Cluster-WS-Manager, die in Publish/Subscribe-Aktivität

Wenn Sie Publish/Subscribe-Messaging in einem Cluster verwenden, sind Kapazitätserwägungen und Leistungsaspekte zu beachten. Daher ist es die beste Praxis, die die Publish/Subscribe-Aktivität über Warteschlangenmanager hinweg erforderlich ist, und sie nur auf die Anzahl der Warteschlangenmanager, die diese erfordern. Nach der Mindestanzahl an Warteschlangen Manager, die Themen veröffentlichen und subskribieren müssen, werden identifiziert. Sie können Mitglieder eines Clusters sein, der nur sie enthält, und keine anderen Warteschlangenmanager.

Dieser Ansatz ist besonders nützlich, wenn Sie bereits einen etablierten Cluster haben. funktionieren gut für Punkt-zu-Punkt-Messaging. Wenn Sie eine vorhandene Großer Cluster in einem Publish/Subscribe-Cluster. Es ist eine bessere Methode, zunächst einen separaten Cluster für die Publish/Subscribe-Arbeit zu erstellen, in dem die Anwendungen nicht mit dem aktuellen Cluster versucht werden. Sie können eine Teilmenge der vorhandenen WS-Manager, die sich bereits in einem oder mehreren Punkt-zu-Punkt-Clustern befinden, und Diese Teilmenge der Member des neuen Publish/Subscribe-Clusters. Allerdings ist

die vollständige Repository-WS-Manager für Ihren neuen Cluster dürfen keine Member eines anderen Clusters sein. Dies isoliert die zusätzliche Last aus dem vorhandenen Cluster. Repositorys.

Wenn Sie keinen neuen Cluster erstellen können, müssen Sie einen vorhandenen großen Cluster in einen Publish/Subscribe-Cluster, verwenden Sie kein direktes Routing-Modell. Der Topic-Host, der weitergeleitet -Modell wird in der Regel besser in größeren Clustern ausgeführt, da es im Allgemeinen die Publish/Subscribe-gemeinsame Nutzung von Informationen und Konnektivität mit der Gruppe von Warteschlangenmanagern die aktiv Publish/Subscribe-Arbeiten ausführen und sich auf die Warteschlange konzentrieren Manager, die die Themen enthalten. Die Ausnahme ist die, wenn eine manuelle Aktualisierung der Subskriptionsinformationen werden auf einem Warteschlangenmanager aufgerufen, auf dem eine Themendefinition gehostet wird. An diesem Punkt wird der Topic-Host-Warteschlangenmanager mit jedem WS-Manager in Verbindung der Cluster. Lesen Sie hierzu den Abschnitt Resynchronisation von Proxy-Subskriptionen.

Wenn Sie feststellen, dass ein Cluster aufgrund seiner Größe nicht für Publish/Subscribe verwendet werden kann oder die aktuelle Last, es ist eine gute Methode, um zu verhindern, dass dieser Cluster unerwartet ausgeführt wird. in einen Publish/Subscribe-Cluster. WS-Manager von **PSCLUS** verwenden Eigenschaft zum Stoppen von jedem, der ein Clusterthema in einem WS-Manager in der Cluster. Siehe „Clusterveröffentlichungs-/Subskriptionssubskribieren” auf Seite 111.

Vorgehensweise bei der Entscheidung, welche Themen in einem Cluster

Es ist wichtig, sorgfältig auszuwählen, welche Themen dem Cluster hinzugefügt werden: Je höher die Themenstruktur in diesen Themen ist, desto breiter wird ihre Verwendung. Dies kann Sie führen dazu, dass mehr Subskriptionsinformationen und Veröffentlichungen weitergegeben werden, als dies erforderlich ist. Wenn es mehrere, eindeutige Zweige der Themenstruktur gibt, wo einige müssen in Gruppen zusammengefasst sein, andere nicht, erstellen Sie verwaltete Themenobjekte im Stammverzeichnis. von jeder Verzweigung, die Clustering benötigt, und die dem Cluster hinzufügen. Wenn z. B. Verzweigungen `/A`, `/B` und `/C` benötigen Clustering, definieren eine separate Clusterthemenobjekte für jede Verzweigung.

Anmerkung: Die Das System verhindert das Verschachtzen von Clusterthemendefinitionen in der Themenstruktur. Sie dürfen nur Topics an einem Punkt in der Themenstruktur für die einzelnen Unterverzweigung. So können Sie beispielsweise keine Clusterthemenobjekte für `/A` und für `/A/B` definieren. Die Verschachtelung von Clusterthemen kann zu Verwechslungen dabei führen, welches Clusterobjekt für welches Abonnement gilt, insbesondere wenn Abonnements Wildcards verwenden. Das ist noch wichtiger, bei Verwendung von Topic-Host-Routing, bei dem Routing-Entscheidungen genau definiert sind durch Ihre Zuordnung von Themenhosts.

Wenn Clusterthemen hoch in der Themenstruktur hinzugefügt werden müssen, aber einige Verzweigungen der Baum unter dem Clusterpunkt erfordert nicht das Clustering-Verhalten, das Sie verwenden können. die Attribute der Subskriptions-und Veröffentlichungsbereiche, um die Ebene von Abonnements-und Publikationsfreigabe für weitere Themen.

Sie sollten den Topic-Root-Knoten nicht in den Cluster stellen, ohne die Verhalten, das angezeigt wird. Globale Themen möglichst naheliegend machen, z. B. durch mit einem übergeordneten Qualifikationsmerkmal in der Themenzeichenfolge: `/global` oder `/cluster`.

Es gibt einen weiteren Grund, warum der Root-Topic-Knoten nicht in einem Cluster zusammengefasst werden soll. Dies liegt daran, dass jeder Warteschlangenmanager über eine lokale Definition für den Stammknoten, das Themenobjekt `SYSTEM.BASE.TOPIC` , verfügt. Wenn dieses Objekt in Gruppen zusammengefasst ist Auf einem WS-Manager im Cluster werden alle anderen WS-Manager auf diese Warteschlangenmanager aufmerksam gemacht. Wenn jedoch eine lokale Definition desselben Objekts vorhanden ist, wird die zugehörige Eigenschaft überschrieben. das Clusterobjekt. Dies führt dazu, dass diese WS-Manager so handeln, als wäre das Thema nicht gruppiert. Um dies zu beheben, müssten Sie jede Definition von `SYSTEM.BASE.TOPIC`in einem Cluster zusammenfassen. Sie könnten dies für direkte Weiterleitung tun. Definitionen, aber nicht für Topic-Host-Routing-Definitionen, da sie alle WS-Manager zu einem Themenhost.

Wie Sie Ihr System als Größe

Publish/Subscribe-Cluster führen in der Regel zu einem anderen Cluster-Muster. Kanäle zu Punkt-zu-Punkt-Messaging in einem Cluster. Das Punkt-zu-Punkt-Modell ist ein 'opt in' eine, aber Publish/Subscribe-Cluster haben eine mehr wahllose Natur mit Abonnement-Fan-out, insbesondere bei Verwendung von direkt weitergeleiteten Themen. Daher ist es Wichtige Angabe, welche WS-Manager in einem Publish/Subscribe-Cluster verwendet werden sollen Clusterkanäle, um eine Verbindung zu anderen Warteschlangenmanagern herzustellen und unter welchen Umständen.

In der folgenden Tabelle ist die typische Gruppe der Clustersender-und -Empfängerkanäle aufgeführt. für jeden WS-Manager in einem Publish/Subscribe-Cluster unter normaler Ausführung erwartet wird, in Abhängigkeit von der Rolle des WS-Managers im Publish/Subscribe-Cluster.

Tabelle 5. Clustersender-und Empfängerkanäle für jede Routing-Methode.

WS-Manager-Rolle	Direkte Clusterempfänger	Direkte Clustersender	Topic-Clusterempfänger	Topic-Clustersender
Vollständiger Repository	AllQmgrs	AllQmgrs	AllQmgrs	AllQMgrs
Host der Themendefinition	Nicht zutreffend	Nicht zutreffend	AllSubs + AllPubs (1)	Alle Subs (1)
Subskriptionen erstellt	AllPubs (1)	AllQMgrs	AllHosts	AllHosts
Bereitgeschaltete Veröffentlichungskomponenten	Alle Subs (1)	Alle Subs (1)	AllHosts	AllHosts
Keine Publisher oder Subskribenten	Alle Subs (1)	Keiner (1)	Keiner (2)	Keiner (2)

Schlüssel:

AllQmgrs
Ein Kanal zu und von jedem WS-Manager im Cluster.

AllSubs
Ein Kanal zu und von jedem WS-Manager, in dem eine Subskription erstellt.

AllPubs
Ein Kanal zu und von jedem WS-Manager, an den eine Veröffentlichungsanwendung angeschlossen wurde.

AllHosts
Ein Kanal zu und von jedem Warteschlangenmanager, in dem eine Definition des s Clusterthemenobjekt wurde konfiguriert.

--
Keine Kanäle zu oder von anderen Warteschlangenmanagern im Cluster für die einzige Zweck des Publish/Subscribe-Messaging.

Anmerkungen:

1. Wenn eine WS-Manageraktualisierung von Proxy-Subskriptionen aus dieser Warteschlange erstellt wird Manager, ein Kanal zu und von allen anderen WS-Managern im Cluster automatisch erstellt werden.
2. Wenn eine WS-Manageraktualisierung von Proxy-Subskriptionen aus dieser Warteschlange erstellt wird Manager, einen Kanal zu und von allen anderen WS-Managern im Cluster, die host kann eine Definition eines Clusterthemas automatisch erstellt werden.

In der vorherigen Tabelle wird gezeigt, dass das Thema Host Routing in der Regel deutlich weniger verwendet. Clustersender-und Empfängerkanäle als direktes Routing. Wenn die Kanalkonnektivität ein

Problem für bestimmte Warteschlangenmanager in einem Cluster, aus Gründen der Kapazität oder der Fähigkeit, bestimmte Kanäle einzurichten (z. B. über Firewalls), Topic-Host Die Weiterleitung ist daher eine bevorzugte Lösung.

Bereitsteller-und Subskriptionsposition

Ein Cluster-Publish/Subscribe aktiviert Nachrichten, die auf einem WS-Manager veröffentlicht werden. an Subskriptionen für alle anderen WS-Manager im Cluster zugestellt werden. Wie für Punkt-zu-Punkt-Messaging, die Kosten für die Übertragung von Nachrichten zwischen Warteschlangenmanagern kann sich negativ auf die Leistung auswirken. Daher sollten Sie die Erstellung von Subskriptionen für Themen in denselben Warteschlangenmanagern, in denen Nachrichten angezeigt werden veröffentlicht.

Bei der Verwendung von Topic-Host-Routing in einem Cluster ist es wichtig, dass auch die Position der Subskriptionen und Publisher in Bezug auf die Topic-Hosting-Warteschlange Manager. Wenn der Publisher nicht mit einem Warteschlangenmanager verbunden ist, der ein Host von ist Das Clusterthema Nachrichten, die veröffentlicht werden, werden immer an einen Topic-Hosting-Warteschlangenmanager gesendet. Gleichermaßen, wenn eine Subskription auf einem Warteschlangenmanager erstellt wird, der nicht Topic-Host für ein Clusterthema, Nachrichten, die von anderen WS-Managern in veröffentlicht werden Der Cluster wird immer zuerst an einen Topic-Host-Warteschlangenmanager gesendet. Mehr wenn sich die Subskription auf einem WS-Manager befindet, auf dem sich die -Thema, aber es gibt einen oder mehrere andere Warteschlangenmanager, die ebenfalls dieses Thema hosten, Ein Teil der Veröffentlichungen von anderen Warteschlangenmanagern wird durch diese weitergeleitet. andere Topic-Hosting-WS-Manager. Weitere Informationen finden Sie unter Topic-Host-Routing mit zentralen Publishern oder Subskribenten Informationen zum Entwerfen eines Topic-Host-Publish/Subscribe-Clusters zum Minimieren Abstand zwischen veröffentlichenden Stellen und Abonnements.

Veröffentlichungsdatenverkehr

Nachrichten, die von einer Anwendung veröffentlicht werden, die mit einem Warteschlangenmanager in einem Cluster verbunden ist Übertragung an Subskriptionen auf anderen WS-Managern mit Clustersender Kanäle.

Wenn Sie direktes Routing verwenden, nehmen die veröffentlichten Nachrichten den kürzesten Pfad zwischen WS-Manager. Das heißt, sie gehen direkt vom Veröffentlichungswarteschlangenmanager zu jedem der folgenden die Warteschlangenmanager mit Subskriptionen. Nachrichten werden nicht an die Warteschlange übertragen Manager, die keine Subskriptionen für das Thema haben. Siehe Proxy-Abonnements in einem Publish/Subscribe-Netz.

Gibt die Rate der Veröffentlichungsnachrichten zwischen einem Warteschlangenmanager und einem anderen in Der Cluster ist hoch, die Cluster-Channel-Infrastruktur zwischen diesen beiden Punkten. muss in der Lage sein, die Rate beizubehalten. Dies kann die Optimierung der Kanäle und Übertragungswarteschlange wird verwendet.

Wenn Sie Topic-Host-Routing verwenden, wird jede Nachricht, die in einem Warteschlangenmanager veröffentlicht wird, Es wird kein Themenhost an einen Topic-Host-WS-Manager übertragen. Dies ist unabhängig Gibt an, ob eine oder mehrere Subskriptionen an einer anderen Stelle im Cluster vorhanden sind. Dies enthält weitere Faktoren, die bei der Planung berücksichtigt werden müssen:

- Ist die zusätzliche Latenzzeit des ersten Sendens jeder Veröffentlichung an einen Topic-Host WS-Manager akzeptabel?
- Kann jeder Topic-Host-Warteschlangenmanager die eingehende und abgehende Veröffentlichung unterstützen rate? Betrachten Sie ein System mit Publishern auf vielen verschiedenen WS-Managern. Wenn sie senden ihre Nachrichten an eine sehr kleine Gruppe von Topic-Hosting-Warteschlangen Manager, werden diese Themenhosts zu einem Engpass bei der Verarbeitung dieser -Nachrichten und Routing-Nachrichten an die Subskribements von Warteschlangenmanagern.
- Erwartet wird, dass ein erheblicher Teil der veröffentlichten Nachrichten nicht einen übereinstimmenden Subskribenten haben? Ist dies der Fall, und ist die Veröffentlichungsrate dieser Nachrichten hoch ist, kann es am besten sein, den Warteschlangenmanager des Publishers zu einem Topic-Host zu

machen. In Eine veröffentlichte Nachricht, in der keine Subskriptionen im Cluster vorhanden sind, wird nicht an andere WS-Manager übertragen.

Diese Probleme können auch durch die Einführung mehrerer Themenhosts gelockert werden, um die Publikationslast auf sie:

- Wenn es mehrere unterschiedliche Themen gibt, die jeweils einen Teil der Veröffentlichungsdatenverkehr in Betracht ziehen, in Betracht ziehen, sie auf verschiedenen Warteschlangenmanagern
- Wenn die Themen nicht auf verschiedene Themenhosts getrennt werden können, sollten Sie Definieren desselben Themenobjekts auf mehreren Warteschlangenmanagern. Dies führt zu -Veröffentlichungen, die für die Weiterleitung auf die einzelnen von ihnen verteilt werden. Dies ist jedoch nur dann sinnvoll, wenn die Reihenfolge der Publizistnachrichten nicht sortiert ist. erforderlich.

Subskriptionsänderung und dynamische Themenzeichenfolgen

Eine weitere Überlegung ist die Auswirkung auf die Leistung des Systems für die Weitergabe. Proxy-Subskriptionen. Gewöhnlich sendet ein Warteschlangenmanager eine Proxy-Subskriptionsnachricht. bei bestimmten anderen WS-Managern im Cluster, wenn die erste Subskription für einen Eine bestimmte Clusterthemenzeichenfolge (nicht nur ein konfiguriertes Themenobjekt) wird unter erstellt. dieser WS-Manager. In ähnlicher Weise wird eine Proxy-Abonnementlöschungsnachricht gesendet, wenn Die letzte Subskription für eine bestimmte Clusterthemenzeichenfolge wird gelöscht.

Für direktes Routing sendet jeder WS-Manager mit Subskriptionen diese Proxy-Server Subskriptionen für alle anderen WS-Manager im Cluster. Bei Topic-Host-Routing sendet jeder WS-Manager mit Subskriptionen nur die Proxy-Subskriptionen an jede WS-Manager, der eine Definition für dieses Clusterthema enthält. Daher wird mit Direktes Routing, die mehr Warteschlangenmanager, die sich im Cluster befinden, um so höher ist die Der Systemaufwand für die Verwaltung von Proxy-Subskriptionen in allen In der Erwägung, dass der Themenhost Routing, die Anzahl der Warteschlangenmanager im Cluster ist kein Faktor.

Bei beiden Routing-Modellen, wenn eine Publish/Subscribe-Lösung aus vielen eindeutigen Themenzeichenfolgen, die subskribiert werden, oder die Themen in einem WS-Manager im Cluster häufig subskribiert und nicht subskribiert sind, wird ein erheblicher Systemaufwand in diesem Warteschlangenmanager zu sehen ist, verursacht durch die ständige Generierung von Nachrichten, die die Verteilung und die Proxy-Subskriptionen löschen. Bei direkter Weiterleitung wird dies durch die Notwendigkeit verbunden, diese Nachrichten an jeden WS-Manager im Cluster zu senden.

Wenn die Änderungsrate der Subskriptionen zu hoch ist, um sie aufnehmen zu können, selbst in einem Topic-Host-Routing-System, siehe Subskriptionsleistung in Publish/Subscribe-Netzen für Informationen über Möglichkeiten zum Reduzieren des Overhead des Proxy-Abonnements

Clusterthemen definieren

Clusterthemen sind Verwaltungsthemen mit definiertem Attribut **`cluster`** . Informationen zu Clusterthemen werden an alle Clustermitglieder übertragen und mit lokalen Themen zu warteschlangenmanagerübergreifenden Thementeilbereichen verbunden. Damit können Nachrichten, die auf einem Warteschlangenmanager zu einem Thema veröffentlicht werden, an die Subskriptionen anderer Warteschlangenmanager im Cluster übermittelt werden.

Wenn Sie ein Clusterthema für einen Warteschlangenmanager definieren, wird diese Clusterthemendefinition an die Warteschlangenmanager mit vollständigem Repository gesendet. Anschließend leiten die vollständigen Repositorys die Clusterthemendefinition an alle Warteschlangenmanager im Cluster weiter, sodass das Clusterthema für alle Bereitsteller und Subskribenten verfügbar ist, die in einem Warteschlangenmanager im Cluster vorhanden sind. Der Warteschlangenmanager, in dem ein Clusterthema erstellt wird, wird als Clusterthemenhost bezeichnet. Das Clusterthema kann von allen Warteschlangenmanagern im Cluster verwendet werden; alle Änderungen an einem Clusterthema müssen jedoch in dem Warteschlangenmanager vorgenommen werden, in dem das Thema definiert ist (d. h. im Clusterthemenhost); anschließend wird die Änderung über die vollständigen Repositorys an alle Clustermitglieder weitergegeben.

Wenn Sie direktes Routing verwenden, wird die Position der Clusterthemendefinition nicht wirkt sich direkt auf das Verhalten des Systems aus, da alle Warteschlangenmanager im Cluster Verwenden Sie die

Themendefinition auf die gleiche Weise. Daher sollten Sie das Thema in jedem beliebigen Warteschlangenmanager, der ein Mitglied des Clusters sein wird, solange das Thema benötigt wird, und das ist auf einem System zuverlässig genug, um regelmäßig in Kontakt mit der vollen Repository-WS-Manager.

Wenn Sie Topic-Host-Routing verwenden, ist die Position der Clusterthemendefinition sehr wichtig. wichtig, da andere WS-Manager im Cluster Kanäle zu dieser Warteschlange erstellen Verwalter und Abonnements-Informationen und Veröffentlichungen an sie senden. So wählen Sie die beste WS-Manager zum Hosten der Themendefinition, müssen Sie das Thema Host-Routing verstehen. Siehe „Thema Host-Routing in Publish/Subscribe-Clustern" auf Seite 90.

Wenn Sie über ein Clusterthema und ein lokales Themenobjekt verfügen, hat das lokale Thema Vorrang. Siehe „Mehrere Cluster-Topic-Definitionen mit demselben Namen" auf Seite 107.

Informationen zu den Befehlen, mit denen Clusterthemen angezeigt werden, finden Sie in den zugehörigen Informationen.

Vererbung von Clustern

In der Regel erwarten Veröffentlichungs-und Subskribierungsanwendungen in einer Publish/Subscribe-Clustertopologie die gleiche Arbeit, unabhängig davon, welcher WS-Manager im Cluster sie enthält. sind verbunden mit. Aus diesem Grund werden die verwalteten Themenobjekte in Clustern an die jeden WS-Manager im Cluster.

Ein verwaltungs-Topic-Objekt übernimmt sein Verhalten von einem anderen verwalteten Thema. Objekte höher in der Themenstruktur. Diese Vererbung tritt auf, wenn ein expliziter Wert wurde nicht für einen Themenparameter festgelegt.

Im Falle eines in Gruppen zusammengefassten Publish/Subscribe ist es wichtig, eine solche zu berücksichtigen. Vererbung, weil sie die Möglichkeit bietet, dass Publisher und Abonnenten verhält sich abhängig von dem Warteschlangenmanager, zu dem sie eine Verbindung herstellen, unterschiedlich. Wenn ein Das Clusterthemenobjekt hinterlässt Parameter, die von höheren Themenobjekten übernommen werden. Das Thema kann sich auf verschiedenen Warteschlangenmanagern im Cluster unterschiedlich verhalten. Ebenso werden lokal definierte Themenobjekte, die unter einem Clusterthemenobjekt definiert sind, in Die Themenstruktur bedeutet, dass die niedrigeren Themen noch in Gruppen zusammengefasst sind, aber die lokale -Objekt kann sein Verhalten in einer Weise ändern, die sich von anderen Warteschlangenmanagern unterscheidet. im Cluster.

Platzhaltersubskriptionen

Proxy-Subskriptionen werden erstellt, wenn lokale Subskriptionen an eine Themenzeichenfolge vorgenommen werden. der in einem Clusterthemenobjekt aufgelöst wird oder darunter ist. Bei einer Subskription mit Platzhalterzeichen höher in der Themenhierarchie als ein beliebnises Clusterthema erstellt hat, hat es keinen Proxy Subskriptionen, die um den Cluster für das übereinstimmende Clusterthema gesendet werden, und daher keine Veröffentlichungen von anderen Membern des Clusters empfängt. Sie erhält jedoch Veröffentlichungen aus dem lokalen WS-Manager.

Wenn eine andere Anwendung jedoch eine Themenzeichenfolge subskribiert, die in oder aufgelöst wird, unterhalb des Clusterthemas werden Proxy-Subskriptionen generiert und Veröffentlichungen an diesen WS-Manager weitergegeben werden. Bei Ankunft das ursprüngliche, höhere Wildcard Subskription wird als rechtmäßiger Empfänger dieser Veröffentlichungen betrachtet und erhält eine Kopie. Wenn dieses Verhalten nicht erforderlich ist, legen Sie **`WILDCARD(BLOCK)`** im Clusterthema fest. Dadurch wird das ursprüngliche Platzhalterzeichen nicht als legitimes Platzhalterzeichen betrachtet. -Subskription und stoppt das Empfangen von Veröffentlichungen (lokal oder an anderer Stelle in den Cluster) im Clusterthema oder in dessen Unterthemen.

Zugehörige Konzepte

Mit Verwaltungsthemen arbeiten

Mit Subskriptionen arbeiten

Zugehörige Verweise

ANZEIGEN TOPIC

ANZEIGEN TPSTATUS
ANZEIGEN SUB

Clusterthemenattribute
Wenn ein Themenobjekt das Attribut "Clustername" definiert hat, wird die Themendefinition auf alle Warteschlangenmanager im Cluster verteilt. Jeder WS-Manager verwendet die weitergegebenen Themenattribute, um das Verhalten von Publish/Subscribe-Anwendungen zu steuern.

Ein Themenobjekt verfügt über eine Reihe von Attributen, die für Publish/Subscribe-Cluster gelten. Einige steuern das allgemeine Verhalten der Veröffentlichungs-und Subskribierungsanwendungen und steuern, wie das Thema im gesamten Cluster verwendet wird.

Eine Clusterthemenobjektdefinition muss so konfiguriert werden, dass sie alle Warteschlangenmanager im Cluster korrekt verwenden kann.

Wenn beispielsweise die Modellwarteschlangen für verwaltete Subskriptionen (`MDURMDL` und `MNDURMDL`) auf einen nicht standardmäßigen Warteschlangennamen gesetzt werden, muss diese benannte Modellwarteschlange auf allen Warteschlangenmanagern definiert werden, in denen verwaltete Subskriptionen erstellt werden.

Wenn ein Attribut auf ASPARENT gesetzt ist, hängt das Verhalten des Abschnitts in ähnlicher Weise von den höheren Knoten in der Themenstruktur (siehe Verwaltungsthemenobjekte) auf jedem einzelnen Queue-Manager im Cluster ab. Dies kann zu einem anderen Verhalten beim Veröffentlichen oder Subskribieren von verschiedenen Warteschlangenmanagern führen.

Die Hauptattribute, die sich direkt auf das Publish/Subscribe-Verhalten im Cluster beziehen, lauten wie folgt:

CLROUTE
Dieser Parameter steuert das Routing von Nachrichten zwischen WS-Managern, in denen Publisher verbunden sind, und Warteschlangenmanagern, in denen übereinstimmende Subskriptionen vorhanden sind.

- Sie konfigurieren die Route entweder direkt zwischen diesen WS-Managern oder über einen Warteschlangenmanager, der eine Definition des Clusterthemas enthält. Weitere Informationen dazu finden Sie im Artikel Publish/Subscribe-Cluster.
- Sie können den **CLROUTE** nicht ändern, solange der Parameter **CLUSTER** festgelegt ist. Wenn Sie den **CLROUTE** ändern möchten, müssen Sie zunächst die Eigenschaft **CLUSTER** auf leer setzen. Dies stoppt Anwendungen, die das Thema in einer Cluster-Art verwenden. Dies führt wiederum zu einer Unterbrechung der Veröffentlichungen, die an Subskriptionen zugestellt werden, so dass Sie auch die Publish/Subscribe-Messaging während der Änderung in den Quiescemodus versetzt haben sollten.

PROXYSUB
Dieser Parameter steuert, wann Proxy-Subskriptionen erstellt werden.

- `FIRSTUSE` ist der Standardwert und bewirkt, dass Proxy-Subskriptionen als Antwort auf lokale Subskriptionen auf einem Warteschlangenmanager in einer verteilten Publish/Subscribe-Topologie gesendet werden und abgebrochen werden, wenn sie nicht mehr benötigt werden. Weitere Informationen darüber, warum Sie dieses Attribut möglicherweise vom Standardwert `FIRSTUSE` ändern möchten, finden Sie im Abschnitt Individuelle Proxy-Subskriptionsweiterleitung und *Veröffentlichung überall* .
- Um *publish überall* zu aktivieren, setzen Sie den Parameter **PROXYSUB** auf `FORCE` für ein übergeordneter Themenobjekt. Dies führt zu einer einzelnen Proxy-Subskription mit Platzhalterzeichen, die alle Topics unter diesem Themenobjekt in der Themenstruktur abgleicht.

Anmerkung: Wenn Sie das Attribut **PROXYSUB(FORCE)** in einem großen Publish/Subscribe-Cluster festlegen, kann es zu einer übermäßigen Auslastung der Systemressourcen kommen. Das Attribut **PROXYSUB(FORCE)** wird an jeden Warteschlangenmanager weitergegeben, nicht nur an den Warteschlangenmanager, auf dem das Thema definiert wurde. Dies bewirkt, dass jeder WS-Manager im Cluster ein Platzhalterzeichen für ein Platzhalterzeichen erstellt.

Eine Kopie einer Nachricht zu diesem Thema, die auf einem beliebigen WS-Manager im Cluster veröffentlicht wird, wird abhängig von der Einstellung **CLROUTE** an jeden Warteschlangenmanager im Cluster gesendet-entweder direkt oder über einen Topic-Host-Warteschlangenmanager.

Wenn das Thema direkt weitergeleitet wird, erstellt jeder WS-Manager Clustersenderkanäle zu jedem anderen Warteschlangenmanager. Wenn der Topic-Host weitergeleitet wird, werden die Kanäle zu jedem Topic-Host-Warteschlangenmanager von jedem WS-Manager im Cluster erstellt.

Weitere Informationen zum **PROXYSUB** -Parameter bei Verwendung in Clustern finden Sie unter Direct routed Publish/Subscribe performance .

PUBSCOBE und SUBSCOPE

Diese Parameter legen fest, ob dieser Warteschlangenmanager Veröffentlichungen an Warteschlangenmanager in der Topologie (Publish/Subscribe-Cluster oder Hierarchie) weitergibt oder den Geltungsbereich nur auf den lokalen WS-Manager beschränkt. Sie können den entsprechenden Job über das Programm mit `MQPMO_SCOPE_QMGR` und `MQSO_SCOPE_QMGR` ausführen.

PUBSCOPE

Wenn ein Clusterthemenobjekt mit **PUBSCOPE(QMGR)** definiert wird, wird die Definition gemeinsam mit dem Cluster verwendet, aber der Umfang der Veröffentlichungen, die auf diesem Thema basieren, ist nur lokal und wird nicht an andere WS-Manager im Cluster gesendet.

SUBSCOPE

Wenn ein Clusterthemenobjekt mit **SUBSCOPE(QMGR)** definiert wird, wird die Definition gemeinsam mit dem Cluster gemeinsam genutzt, aber der Geltungsbereich von Subskriptionen, die auf diesem Thema basieren, ist nur lokal. Daher werden keine Proxy-Subskriptionen an andere Warteschlangenmanager im Cluster gesendet.

Diese beiden Attribute werden im Allgemeinen zusammen verwendet, um einen Warteschlangenmanager von der Interaktion mit anderen Membern des Clusters zu bestimmten Themen zu trennen. Der Warteschlangenmanager veröffentlicht oder empfängt keine Veröffentlichungen zu diesen Themen in und von anderen Membern des Clusters. Diese Situation verhindert nicht die Veröffentlichung oder Subskription, wenn Themenobjekte in Unterabschnitten definiert sind.

Wenn Sie **SUBSCOPE** in einer lokalen Definition eines Themas auf `QMGR` setzen, werden andere WS-Manager im Cluster nicht daran gehindert, ihre Proxy-Subskriptionen an den Warteschlangenmanager weiterzugeben, wenn sie eine Clusterversion des Themas mit **SUBSCOPE(ALL)** verwenden. Wenn die lokale Definition jedoch auch **PUBSCOPE** auf `QMGR` setzt, werden diese Proxy-Subskriptionen keine Veröffentlichungen von diesem Warteschlangenmanager gesendet.

Zugehörige Konzepte

Veröffentlichungsumfang

Subskriptionsumfang

Mehrere Cluster-Topic-Definitionen mit demselben Namen

Sie können dasselbe benannte Clusterthemenobjekt in mehreren Warteschlangenmanagern im Cluster definieren, und in bestimmten Szenarios kann dies ein bestimmtes Verhalten ermöglichen. Wenn mehrere Clusterthemendefinitionen mit demselben Namen vorhanden sind, sollte die Mehrzahl der Eigenschaften übereinstimmen. Wenn dies nicht der Fall ist, werden in Abhängigkeit von der Signifikanz der Abweichung Fehler oder Warnungen ausgegeben.

Wenn in den Eigenschaften mehrerer Cluster-Topic-Definitionen eine Diskrepanz vorliegt, werden Warnungen ausgegeben und eine der Themenobjektdefinitionen wird von jedem WS-Manager im Cluster verwendet. Welche Definition von jedem WS-Manager verwendet wird, ist nicht deterministisch oder konsistent über die Warteschlangenmanager im Cluster hinweg. Solche Diskrepanzen sollten so schnell wie möglich gelöst werden.

Bei der Clusterkonfiguration oder -wartung müssen Sie manchmal mehrere Clusterthemendefinitionen erstellen, die nicht identisch sind. Dies ist jedoch nur als vorübergehende Maßnahme sinnvoll und wird daher als Fehlerbedingung behandelt.

Wenn Diskrepanzen festgestellt werden, werden die folgenden Warnungen in jedes Fehlerprotokoll des Warteschlangenmanagers geschrieben:

- Multi Unter Multiplatforms, AMQ9465 und AMQ9466.
- z/OS Unter z/OS: CSQX465I und CSQX466I

Die ausgewählten Eigenschaften für jede Themenzeichenfolge auf jedem Warteschlangenmanager können bestimmt werden, indem der Themenstatus anstelle der Themenobjektdefinitionen angezeigt wird, z. B. mithilfe von **DISPLAY TPSTATUS**.

In einigen Situationen ist ein Konflikt in den Konfigurationseigenschaften so schwer wiegend, dass das zu erstellende Themenobjekt gestoppt wird, oder dass die falsch übereinstimmenden Objekte als ungültig markiert und nicht im Cluster weitergegeben werden (siehe **CLSTATE** in DISPLAY TOPIC). Diese Situationen treten auf, wenn ein Konflikt in der Eigenschaft der Clusterweiterleitung (**CLROUTE**) der Themendefinitionen auftritt. Darüber hinaus werden weitere Inkonsistenzen aufgrund der Bedeutung der Konsistenz zwischen den Themenhost-Routing-Definitionen wie in den nachfolgenden Abschnitten dieses Artikels abgelehnt.

Wenn der Konflikt zu dem Zeitpunkt erkannt wird, zu dem das Objekt definiert ist, wird die Konfigurationsänderung zurückgewiesen. Wenn später von den vollständigen Repository-WS-Managern festgestellt wird, werden die folgenden Warnungen in die Fehlerprotokolle der WS-Manager geschrieben:

- Multi Unter Multiplatforms: AMQ9879.
- z/OS Unter z/OS: CSQX879E.

Wenn mehrere Definitionen desselben Themenobjekts im Cluster definiert sind, hat eine lokal definierte Definition Vorrang vor einer fernen Definition, die über Remotezugriff definiert ist. Wenn also Unterschiede in den Definitionen vorhanden sind, verhalten sich die WS-Manager, die die verschiedenen Definitionen hosten, unterschiedlich.

Die Auswirkung der Definition eines Nicht-Cluster-Themas mit demselben Namen wie ein Clusterthema aus einem anderen Warteschlangenmanager.

Es ist möglich, ein verwalttes Themenobjekt zu definieren, das sich nicht auf einem Warteschlangenmanager befindet, der sich in einem Cluster befindet, und gleichzeitig dasselbe benannte Themenobjekt wie eine Clusterthemendefinition in einem anderen Warteschlangenmanager definieren. In diesem Fall hat das lokal definierte Themenobjekt Vorrang vor allen fernen Definitionen mit dem gleichen Namen.

Dadurch wird verhindert, dass das Clustering-Verhalten des Themas bei Verwendung dieses Warteschlangenmanagers verhindert wird. Dies bedeutet, dass Subskriptionen möglicherweise keine Veröffentlichungen von fernen Publishern empfangen, und Nachrichten von Publishern werden möglicherweise nicht an ferne Subskriptionen im Cluster weitergegeben.

Vor der Konfiguration eines solchen Systems sollte sorgfältig geprüft werden, da dies zu verwirrenden Verhaltensweisen führen kann.

Anmerkung: Wenn ein einzelner Warteschlangenmanager Veröffentlichungen und Subskriptionen von der Weitergabe an den Cluster verhindern muss, selbst wenn das Thema an anderer Stelle in einem Cluster zusammengefasst wurde, besteht ein alternativer Ansatz darin, die Veröffentlichungs-und Subskriptionsbereiche nur auf den lokalen WS-Manager zu setzen. Siehe „Clusterthemenattribute” auf Seite 106.

Mehrere Cluster-Topic-Definitionen in einem Cluster mit direktem Routing

Für direktes Routing definieren Sie in der Regel einen Clusterabschnitt nicht für mehrere Cluster-Queue-Manager. Dies liegt daran, dass das direkte Routing das Thema an allen Warteschlangenmanagern im Cluster verfügbar macht, unabhängig davon, auf welchem Warteschlangenmanager er definiert wurde. Darüber hinaus erhöht das Hinzufügen mehrerer Clusterthemendefinitionen die Systemaktivität und die Verwaltungskomplexität erheblich, und die Wahrscheinlichkeit, dass die Komplexität zunimmt, erhöht die Wahrscheinlichkeit eines Benutzerfehlers:

- Jede Definition führt dazu, dass ein weiteres Clusterthemenobjekt an die anderen WS-Manager im Cluster übertragen wird, einschließlich der anderen Cluster-Topic-Host-Warteschlangenmanager.

- Alle Definitionen für ein bestimmtes Thema in einem Cluster müssen identisch sein. Andernfalls ist es schwierig, herauszufinden, welche Themendefinition von einem WS-Manager verwendet wird.

Es ist außerdem nicht unbedingt erforderlich, dass der einzige Host-WS-Manager permanent für die ordnungsgemäße Funktion des Themas im Cluster verfügbar ist, da die Clusterthemendefinition von den vollständigen WS-Managern des Repositorys und von allen anderen Warteschlangenmanagern in den Teilclusterrepositorys zwischengespeichert wird. Weitere Informationen hierzu finden Sie im Abschnitt Verfügbarkeit von Topic-Host-WS-Managern, die direktes Routing verwenden .

Für eine Situation, in der Sie möglicherweise vorübergehend ein Clusterthema auf einem zweiten Warteschlangenmanager definieren müssen, z. B., wenn der vorhandene Host des Themas aus dem Cluster entfernt werden soll, finden Sie weitere Informationen unter Clusterthemendefinition in einen anderen Warteschlangenmanager verschieben .

Wenn Sie die Definition eines Cluster-Topics ändern müssen, achten Sie darauf, sie in dem Warteschlangenmanager zu ändern, in dem sie auch definiert wurde. Der Versuch, ihn von einem anderen WS-Manager zu ändern, kann versehentlich eine zweite Definition des Themas mit widersprüchlichen Themenattributen erstellen.

Mehrere Cluster-Topic-Definitionen in einem Cluster mit Topic-Host-Routing

Wenn ein Clusterthema mit einer Clusterroute von *topic host* definiert wird, wird das Thema in allen WS-Managern im Cluster genauso wie für *direkte* weitergeleitete Themen weitergegeben. Darüber hinaus wird das gesamte Publish/Subscribe-Messaging für dieses Thema über die Warteschlangenmanager weitergeleitet, in denen dieses Thema definiert ist. Daher wird die Position und die Anzahl der Definitionen des Themas im Cluster wichtig (siehe „Thema Host-Routing in Publish/Subscribe-Clustern” auf Seite 90).

Um eine ausreichende Verfügbarkeit und Skalierbarkeit zu gewährleisten, ist es sinnvoll, wenn möglich mehrere Themendefinitionen zu haben. Siehe Verfügbarkeit von Topic-Host-WS-Managern, die Topic-Host-Routing verwenden .

Beim Hinzufügen oder Entfernen zusätzlicher Definitionen eines *Topic-Host* -Themas in einem Cluster sollten Sie den Fluss der Nachrichten zum Zeitpunkt der Konfigurationsänderung berücksichtigen. Wenn zum Zeitpunkt der Änderung Nachrichten im Cluster zu dem Thema veröffentlicht werden, ist ein zwischengespeicherten Prozess erforderlich, um eine Themendefinition hinzuzufügen oder zu entfernen. Weitere Informationen hierzu finden Sie im Abschnitt Clusterthemendefinition in einen anderen Warteschlangenmanager verschieben und Weitere Themenhosts zu einem Topic-Host-Routing-Cluster hinzufügen .

Wie bereits erläutert, sollten die Eigenschaften der Mehrfachdefinitionen mit der möglichen Ausnahme des **PUB** -Parameters übereinstimmen, wie im nächsten Abschnitt beschrieben. Wenn Veröffentlichungen über Topic-Host-Warteschlangenmanager weitergeleitet werden, ist es sogar noch wichtiger, dass mehrere Definitionen konsistent sind. Daher wird eine Inkonsistenz, die in der Themenzeichenfolge oder dem Clusternamen festgestellt wurde, zurückgewiesen, wenn eine oder mehrere der Themendefinitionen für das Thema Host-Cluster-Routing konfiguriert wurden.

Anmerkung: Clusterthemendefinitionen werden auch zurückgewiesen, wenn versucht wird, sie oberhalb oder unterhalb eines anderen Themas in der Themenstruktur zu konfigurieren, in dem die vorhandene Clusterthemendefinition für das Thema Host-Routing konfiguriert ist. Dies verhindert die Mehrdeutigkeit bei der Weiterleitung von Veröffentlichungen in Bezug auf Platzhaltersubskriptionen.

Sonderbehandlung für den Parameter PUB

Der Parameter **PUB** wird verwendet, um zu steuern, wann Anwendungen in einem Thema veröffentlichen können. Im Fall des Topic-Host-Routing in einem Cluster kann er auch steuern, welche Topic-Host-Warteschlangenmanager verwendet werden, um Veröffentlichungen zu verlegen. Aus diesem Grund ist es zulässig, dass mehrere Definitionen desselben Themenobjekts im Cluster mit unterschiedlichen Einstellungen für den Parameter PUB vorhanden sind.

Wenn mehrere ferne Clusterdefinitionen eines Themas über unterschiedliche Einstellungen für diesen Parameter verfügen, ermöglicht das Thema, dass Veröffentlichungen an Subskriptionen gesendet und zugestellt werden, wenn die folgenden Bedingungen erfüllt sind:

- Es ist kein übereinstimmender Themenobjekt definiert, der auf dem Warteschlangenmanager definiert ist, mit dem der Publisher verbunden ist, der auf PUB(DISABLED) gesetzt ist.
- Mindestens eine der mehreren Themendefinitionen im Cluster ist auf PUB(ENABLED) gesetzt, oder es wird mindestens eine der Themendefinitionen auf PUB(ASPARENT) festgelegt und die lokalen Warteschlangenmanager, in denen der Bereitsteller verbunden ist, und die definierte Subskription auf PUB(ENABLED) an einem höheren Punkt in der Themenstruktur gesetzt.

Für Topic-Host-Routing, wenn Nachrichten von Anwendungen veröffentlicht werden, die mit Warteschlangenmanagern verbunden sind, die keine Topic-Hosts sind, werden Nachrichten nur an den Topic-Host-Warteschlangenmanager weitergeleitet, in dem der Parameter **PUB** nicht explizit auf DISABLED gesetzt wurde. Sie können daher die Einstellung PUB (DISABLED) verwenden, um den Nachrichtenverkehr über bestimmte Themenhosts in den Quiescemodus zu setzen. Möglicherweise möchten Sie dies tun, um die Wartung oder das Entfernen eines Warteschlangenmanagers vorzubereiten, oder aus den Gründen, die im Abschnitt Weitere Topic-Hosts zu einem Topic-Host-Routing-Cluster hinzufügen beschrieben werden.

Verfügbarkeit von Cluster-Topic-Host-Warteschlangenmanagern
Entwerfen Sie Ihren Publish/Subscribe-Cluster, um das Risiko zu minimieren, dass der Cluster nicht mehr in der Lage ist, den Datenverkehr für das Thema zu verarbeiten, wenn ein Topic-Host-Warteschlangenmanager nicht mehr verfügbar ist. Die Auswirkung eines Topic-Host-Warteschlangenmanagers, der nicht verfügbar wird, hängt davon ab, ob der Cluster Topic-Host-Routing oder direktes Routing verwendet.

Verfügbarkeit von Topic-Host-Warteschlangenmanagern, die direktes Routing verwenden

Für direktes Routing definieren Sie in der Regel einen Clusterabschnitt nicht für mehrere Cluster-Queue-Manager. Dies liegt daran, dass das direkte Routing das Thema an allen Warteschlangenmanagern im Cluster verfügbar macht, unabhängig davon, auf welchem Warteschlangenmanager er definiert wurde. Weitere Informationen finden Sie unter Mehrere Cluster-Topic-Definitionen in einem Cluster mit direkter Weiterleitung.

Wenn in einem Cluster der Host eines Clusterobjekts (z. B. eine Clusterwarteschlange oder ein Clusterthema) für einen längeren Zeitraum nicht mehr verfügbar ist, werden die anderen Mitglieder des Clusters schließlich die Kenntnis dieser Objekte verfallen lassen. Wenn der Cluster-Topic-Host-Warteschlangenmanager in einem Clusterthema nicht mehr verfügbar ist, verarbeiten die anderen Warteschlangenmanager weiterhin Publish/Subscribe-Anforderungen für das Thema in einer direkten Cluster-Methode (d. B. das Senden von Veröffentlichungen an Subskriptionen auf fernen Warteschlangenmanagern) für mindestens 60 Tage ab dem Zeitpunkt, ab dem der Topic-Hosting-Warteschlangenmanager zuletzt in der Kommunikation mit den vollständigen WS-Managern der Repository-WS-Managern stand. Wenn der Warteschlangenmanager, auf dem Sie das Clusterthemenobjekt definiert haben, nie wieder verfügbar gemacht wird, werden die zwischengespeicherten Themenobjekte auf den anderen Warteschlangenmanagern gelöscht, und das Thema wird auf ein lokales Thema zurückgesetzt, in dem die Subskriptionen nicht mehr Veröffentlichungen von Anwendungen empfangen, die mit fernen Warteschlangenmanagern verbunden sind.

Wenn der Warteschlangenmanager, auf dem Sie ein Clusterthemenobjekt definieren, mit dem 60-Tage-Zeitraum wiederhergestellt werden soll, müssen keine speziellen Maßnahmen ergriffen werden, um sicherzustellen, dass ein Clusterthemenhost verfügbar bleibt (beachten Sie jedoch, dass alle Subskriptionen, die auf dem nicht verfügbaren Clusterthemenhost definiert sind, nicht verfügbar bleiben). Der 60-Tage-Zeitraum reicht aus, um technische Probleme zu erfüllen, und wird wahrscheinlich nur aufgrund von Verwaltungsfehlern überschritten. Wenn der Cluster-Topic-Host nicht verfügbar ist, schreiben alle Member des Clusters stündlich Fehlerprotokollnachrichten, die stündlich angeben, dass ihr zwischengespeichertes Clusterthemenobjekt nicht aktualisiert wurde, um diese Möglichkeit zu beheben. Beantworten Sie diese Nachrichten, indem Sie sicherstellen, dass der WS-Manager, auf dem das Clusterthemenobjekt definiert ist, aktiv ist. Wenn es nicht möglich ist, den Cluster-Topic-Host-Warteschlangenmanager wieder verfügbar zu machen, definieren Sie die gleiche Clusterthemendefinition mit genau denselben Attributen in einem anderen Warteschlangenmanager im Cluster.

Verfügbarkeit von Topic-Host-Warteschlangenmanagern, die Topic-Host-Routing verwenden

Für das Topic-Host-Routing wird die gesamte Publish/Subscribe-Nachrichtenübertragung für ein Thema über die Warteschlangenmanager weitergeleitet, in denen dieses Thema definiert ist. Aus diesem Grund ist es sehr wichtig, dass die ständige Verfügbarkeit dieser WS-Manager im Cluster berücksichtigt wird. Wenn ein Themenhost nicht mehr verfügbar ist und kein anderer Host für das Thema vorhanden ist, wird der Datenverkehr von Publishern zu Subskribenten auf verschiedenen Warteschlangenmanagern im Cluster sofort für das Thema angehalten. Wenn weitere Topic-Hosts verfügbar sind, leiten die Cluster-WS-Manager den neuen Veröffentlichungsdatenverkehr durch diese Themenhosts, wodurch die kontinuierliche Verfügbarkeit von Nachrichtenrouten bereitgestellt wird.

Wie bei direkten Themen wird nach 60 Tagen, wenn der erste Themenhost noch nicht verfügbar ist, die Kenntnis des Topic-Hostthemas aus dem Cluster entfernt. Wenn es sich dabei um die letzte verbleibende Definition für dieses Thema im Cluster handelt, werden alle anderen Warteschlangenmanager die Weiterleitung von Veröffentlichungen an einen beliebigen Themenhost nicht mehr weiterleiten.

Um eine ausreichende Verfügbarkeit und Skalierbarkeit zu gewährleisten, ist es daher sinnvoll, wenn möglich, jedes Thema auf mindestens zwei Cluster-WS-Managern zu definieren. Dadurch wird der Schutz vor einem bestimmten Topic-Host-WS-Manager, der nicht mehr verfügbar ist Siehe auch Mehrere Clusterthemendefinitionen in einem Topic-Host-Routing-Cluster .

Wenn Sie nicht mehrere Themenhosts konfigurieren können (z. B. weil Sie die Nachrichtenreihenfolge beibehalten müssen) und Sie nicht nur einen Topic-Host konfigurieren können (weil die Verfügbarkeit eines einzelnen Warteschlangenmanagers den Fluss der Veröffentlichungen nicht auf Subskriptionen für alle Warteschlangenmanager im Cluster auswirken darf), ist es in Betracht zu ziehen, das Thema als direktes weitergeleitete Thema zu konfigurieren. Dadurch wird die Abhängigkeit von einem einzelnen Warteschlangenmanager für den gesamten Cluster vermieden, aber es ist immer noch erforderlich, dass jeder einzelne WS-Manager verfügbar ist, damit er lokal gehostete Subskriptionen und Publisher verarbeiten kann.

Clusterveröffentlichungs-/Subskriptionssubskribieren

Durch die Einführung des ersten direkt weitergeleiteten Clusterthemas in einen Cluster wird jeder WS-Manager im Cluster gezwungen, jeden anderen Warteschlangenmanager zu kennen und kann die Kanäle dazu bringen, Kanäle zu erstellen. Wenn dies nicht wünschenswert ist, sollten Sie stattdessen Topic-Host-Routing-Publish/Subscribe konfigurieren. Wenn das Vorhandensein eines direkt weitergeleiteten Clusterthemas die Stabilität des Clusters gefährden könnte, können Sie die Cluster-Publish/Subscribe-Funktionalität aufgrund von Skalierungsbedenken jedes Warteschlangenmanagers vollständig inaktivieren, indem Sie **PSCLUS** auf jedem WS-Manager im Cluster auf `DISABLED` setzen.

Wie unter „Direktes Routing in Publish/Subscribe-Clustern” auf Seite 85 beschrieben, werden bei der Einführung eines direkt weitergeleiteten Cluster-Topics im Cluster alle Teilrepositorys automatisch über alle anderen Mitglieder des Clusters benachrichtigt. Das Clusterthema kann auch Subskriptionen auf allen anderen Knoten erstellen (z. B. wo **PROXYSUB(FORCE)** angegeben ist) und verursacht eine große Anzahl von Kanälen, die von einem Warteschlangenmanager aus gestartet werden, auch wenn keine lokalen Subskriptionen vorhanden sind. Dadurch wird jedem WS-Manager im Cluster eine sofortige zusätzliche Belastung angezeigt. Für einen Cluster, der viele Warteschlangenmanager enthält, kann dies zu einer erheblichen Leistungsminderung führen. Daher muss die Einführung von Direct-Routing-Publish/Subscribe in einem Cluster sorgfältig geplant werden.

Wenn Sie wissen, dass ein Cluster die Overheads von Direct Routing Publish/Subscribe nicht aufnehmen kann, können Sie stattdessen Topic-Host-Routing-Publish/Subscribe verwenden. Eine Übersicht über die Unterschiede finden Sie in „Publish/Subscribe-Cluster entwerfen” auf Seite 83.

Wenn Sie es vorziehen, die Publish/Subscribe-Funktionalität für den Cluster vollständig zu inaktivieren, können Sie dies tun, indem Sie das WS-Managerattribut **PSCLUS** auf jedem WS-Manager im Cluster auf `DISABLED` setzen. Diese Einstellung inaktiviert die Publish/Subscribe-Publish/Subscribe im Cluster, indem drei Aspekte der WS-Manager-Funktionalität geändert werden:

- Ein Administrator dieses Warteschlangenmanagers ist nicht mehr in der Lage, ein `Topic` -Objekt als Cluster zu definieren.

- Eingehende Themendefinitionen oder Proxy-Subskriptionen von anderen Warteschlangenmanagern werden zurückgewiesen, und es wird eine Warnung protokolliert, um den Administrator über eine falsche Konfiguration zu informieren.
- Vollständige Repositorys teilen nicht mehr automatisch Informationen zu jedem Warteschlangenmanager mit allen anderen Teilrepositorys, wenn sie eine Themendefinition empfangen.

Obwohl **PSCLUS** ein Parameter jedes einzelnen Warteschlangenmanagers in einem Cluster ist, ist es nicht beabsichtigt, die Publish/Subscribe-Subskription in einer Untergruppe von Warteschlangenmanagern im Cluster selektiv zu inaktivieren. Wenn Sie auf diese Weise selektiv inaktivieren, werden häufige Fehlernachrichten angezeigt. Dies liegt daran, dass Proxy-Subskriptionen und Themendefinitionen permanent angezeigt und zurückgewiesen werden, wenn ein Thema in einem Warteschlangenmanager in einem Cluster zusammengefasst ist, in dem **PSCLUS** aktiviert ist.

Sie sollten daher versuchen, **PSCLUS** auf jedem WS-Manager im Cluster auf DISABLED zu setzen. In der Praxis kann es jedoch schwierig sein, diesen Status zu erreichen und zu verwalten, z. B. Warteschlangenmanager können beitreten und den Cluster zu jedem Zeitpunkt verlassen. Sie müssen mindestens sicherstellen, dass **PSCLUS** für alle vollständigen WS-Manager-Repository-Warteschlangenmanager auf DISABLED gesetzt ist. Wenn Sie dies tun und anschließend ein Clusterthema in einem ENABLED -Warteschlangenmanager im Cluster definiert wird, führt dies nicht dazu, dass die vollständigen Repositorys alle Warteschlangenmanager jedes anderen Warteschlangenmanagers informieren, und so dass Ihr Cluster vor potenziellen Skalierungsproblemen für alle Warteschlangenmanager geschützt ist. In diesem Szenario wird der Ursprung des Clusterthemas in den Fehlerprotokollen der vollständigen WS-Manager-Repositorys dokumentiert.

Wenn ein Warteschlangenmanager an einem oder mehreren Publish/Subscribe-Clustern und einem oder mehreren Punkt-zu-Punkt-Clustern beteiligt ist, müssen Sie **PSCLUS** auf ENABLED in diesem Warteschlangenmanager setzen. Aus diesem Grund sollten Sie bei der Überschneidung eines Punkt-zu-Punkt-Clusters mit einem Publish/Subscribe-Cluster eine separate Gruppe vollständiger Repositorys in jedem Cluster verwenden. Mit dieser Methode können Themendefinitionen und Informationen zu jedem WS-Manager nur im Publish/Subscribe-Cluster fließen.

Um inkonsistente Konfigurationen zu vermeiden, wenn Sie **PSCLUS** von ENABLED in DISABLED ändern, können keine Clusterthemenobjekte in einem Cluster vorhanden sein, in dem dieser WS-Manager Mitglied ist. Alle solchen Themen, die auch über Remotezugriff definiert sind, müssen gelöscht werden, bevor **PSCLUS** in DISABLED geändert wird.

Weitere Informationen zu **PSCLUS** finden Sie in ALTER QMGR (PSCLUS) .

Zugehörige Konzepte
Direkte Publish/Subscribe-Clusterleistung

Publish/Subscribe und mehrere Cluster

Ein einzelner WS-Manager kann Mitglied mehrerer Cluster sein. Diese Anordnung wird manchmal auch als *überlappende Cluster* bezeichnet. Durch eine solche Überlappung können Clusterwarteschlangen von mehreren Clustern aus zugänglich gemacht werden, und der Punkt-zu-Punkt-Datenverkehr kann von Warteschlangenmanagern in einem Cluster an Warteschlangenmanager in einem anderen Cluster weitergeleitet werden. Clusterthemen in Publish/Subscribe-Clustern bieten nicht die gleiche Funktionalität. Daher muss ihr Verhalten bei der Verwendung mehrerer Cluster klar verstanden werden.

Anders als bei einer Warteschlange können Sie eine Themendefinition nicht mehr als einem Cluster zuordnen. Der Geltungsbereich eines Clusterthemas ist auf die WS-Manager im selben Cluster beschränkt, für die das Thema definiert ist. Auf diese Weise können Veröffentlichungen an Subskriptionen nur auf diesen Warteschlangenmanagern in demselben Cluster weitergegeben werden.

Themenstruktur eines Warteschlangenmanagers

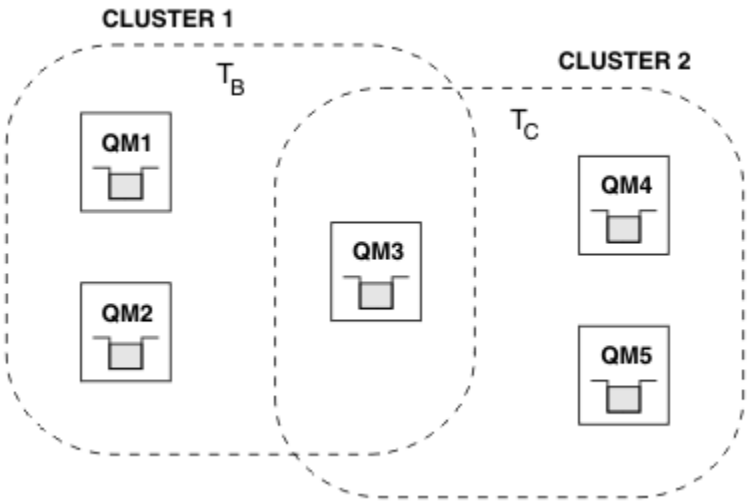


Abbildung 28. Überlappende Cluster: Zwei Cluster, die jeweils verschiedene Themen subskribieren

Wenn ein Warteschlangenmanager Mitglied mehrerer Cluster ist, wird er auf alle in den einzelnen Clustern definierten Clusterthemen aufmerksam gemacht. Zum Beispiel kennt in der vorherigen Abbildung QM3 die verwalteten Clusterthemenobjekte T_B und T_C, während QM1 nur T_B kennt. QM3 wendet beide Themendefinitionen auf sein lokales Thema an und hat daher für bestimmte Themen ein anderes Verhalten gegenüber QM1. Aus diesem Grund ist es wichtig, dass die Clusterthemen aus verschiedenen Clustern sich nicht gegenseitig stören. Kollisionen können auftreten, wenn ein Cluster-Topic oberhalb oder unterhalb eines anderen Clusterthemas in einem anderen Cluster definiert ist (z. B. haben sie Themenzeichenfolgen von `/Sport` und `/Sport/Football`) oder sogar für dieselbe Themenzeichenfolge in beiden. Eine andere Form der Kollision ist, wenn verwaltete Clusterthemenobjekte mit demselben Objektnamen in verschiedenen Clustern definiert werden, aber für unterschiedliche Themenzeichenfolgen.

Wenn eine solche Konfiguration vorgenommen wird, wird die Bereitstellung von Veröffentlichungen zu übereinstimmenden Subskriptionen sehr abhängig von den relativen Positionen der Bereitstellungs-und Subskribenten in Bezug auf den Cluster. Aus diesem Grund können Sie sich nicht auf eine solche Konfiguration verlassen, und Sie sollten es ändern, um die kollierenden Themen zu entfernen.

Wenn Sie eine überlappende Clustertopologie mit Publish/Subscribe-Messaging planen, können Sie jede Kollision vermeiden, indem Sie die Themenstruktur-und Clusterthemenobjektnamen so behandeln, als ob sie sich über alle überlappenden Cluster in der Topologie erstrecken.

Mehrere Publish/Subscribe-Cluster integrieren

Wenn Publish/Subscribe-Messaging in verschiedenen Clustern über Publish/Subscribe-Messaging erforderlich ist, stehen zwei Optionen zur Verfügung:

- Verbinden Sie die Cluster miteinander, indem Sie eine Publish/Subscribe-Hierarchiekonfiguration verwenden. Weitere Informationen hierzu finden Sie im Abschnitt Themenbereiche mehrerer Cluster zusammenfassen.
- Erstellen Sie einen zusätzlichen Cluster, der die vorhandenen Cluster überlagert, und schließt alle Warteschlangenmanager ein, die ein bestimmtes Thema veröffentlichen oder subskribieren müssen.

Bei letzterer Option sollten Sie die Größe des Clusters und den effizientesten Cluster-Routing-Mechanismus sorgfältig prüfen. Siehe„Publish/Subscribe-Cluster entwerfen” auf Seite 83.

Designüberlegungen zu ständigen Veröffentlichungen in Publish/Subscribe-Clustern

Beim Entwurf eines Publish/Subscribe-Clusters für die Arbeit mit ständigen Veröffentlichungen sind einige Einschränkungen zu beachten.

Überlegungen

Hinweise 1: Die folgenden Cluster-WS-Manager speichern immer die aktuellste Version einer ständigen Veröffentlichung:

- Der Warteschlangenmanager des Publishers
- In einem Topic-Host-Routing-Cluster der Themenhost (vorausgesetzt, es gibt nur einen Themenhost für das Thema, wie im nächsten Abschnitt dieses Artikels erläutert).
- Alle WS-Manager mit Subskriptionen, die mit der Themenzeichenfolge der ständigen Veröffentlichung übereinstimmen

Hinweise 2: Warteschlangenmanager erhalten keine aktualisierten ständigen Veröffentlichungen, während sie keine Subskriptionen haben. Daher wird jede gespeicherte Publizierung, die auf einem Warteschlangenmanager gespeichert ist und nicht mehr für das Thema subskribiert wird, veraltete Veröffentlichungen.

Hinweise 3: Wenn bei der Erstellung einer Subskription eine lokale Kopie einer ständigen Veröffentlichung für die Themenzeichenfolge vorhanden ist, wird die lokale Kopie an die Subskription übergeben. Wenn Sie der erste Subskribent für eine beliebige Themenzeichenfolge sind, wird eine übereinstimmende ständige Veröffentlichung auch von einem der folgenden Cluster-Member bereitgestellt:

- In einem direkt weitergeleiteten Cluster der Warteschlangenmanager des Publishers
- In einem Topic-Host-Routing-Cluster die Topic-Hosts für das angegebene Thema

Die Zustellung einer ständigen Veröffentlichung von einem Themenhost oder veröffentlichenden Warteschlangenmanager an den subskribierenden Warteschlangenmanager erfolgt asynchron zu den MQSUB-Aufrufen. Wenn Sie daher den Aufruf MQSUBRQ verwenden, wird die letzte ständige Veröffentlichung möglicherweise bis zu einem nachfolgenden Aufruf von MQSUBRQ verpasst.

Implikationen

Bei einem Publish/Subscribe-Cluster speichert der lokale WS-Manager beim Erstellen einer ersten Subskription möglicherweise eine veraltete Kopie einer ständigen Veröffentlichung, und dies ist die Kopie, die an die neue Subskription zugestellt wird. Das Vorhandensein einer Subskription auf dem lokalen WS-Manager bedeutet, dass dies beim nächsten Aktualisieren der ständigen Veröffentlichung behoben werden wird.

Wenn Sie für einen Topic-Host-Publish/Subscribe-Cluster mehr als einen Topic-Host für ein bestimmtes Thema konfigurieren, erhalten neue Subskribenten möglicherweise die neueste ständige Veröffentlichung von einem Themenhost oder sie erhalten möglicherweise eine veraltete Veröffentlichung von einem anderen Themenhost (mit der letzten verloren gegangenen). Für Topic-Host-Routing ist es üblich, mehrere Topic-Hosts für ein bestimmtes Thema zu konfigurieren. Wenn Sie jedoch von Anwendungen erwarten, dass sie ständige Veröffentlichungen verwenden, sollten Sie für jedes Thema nur einen Themahost konfigurieren.

Für alle angegebenen Themenzeichenfolgen sollten Sie nur einen einzigen Publisher verwenden und sicherstellen, dass der Publisher immer denselben Warteschlangenmanager verwendet. Wenn dies nicht der Fall ist, können verschiedene ständige Veröffentlichungen an verschiedenen Warteschlangenmanagern für dasselbe Thema aktiv sein, was zu unerwartetem Verhalten führt. Da mehrere Proxy-Subskriptionen verteilt sind, können mehrere ständige Veröffentlichungen empfangen werden.

Wenn die Subskribenten weiterhin über veraltete Veröffentlichungen besorgt sind, sollten Sie beim Erstellen jeder ständigen Veröffentlichung die Einstellung eines Nachrichtenablaufes in Erwägung ziehen.

Mit dem Befehl **CLEAR TOPICSTR** können Sie eine ständige Veröffentlichung aus einem Publish/Subscribe-Cluster entfernen. Unter bestimmten Umständen müssen Sie den Befehl möglicherweise auf mehreren Membern des Publish/Subscribe-Clusters absetzen, wie in **CLEAR TOPICSTR** beschrieben.

Subskriptionen mit Platzhalterzeichen und ständige Veröffentlichungen

Wenn Sie Platzhaltersubskriptionen verwenden, werden die entsprechenden Proxy-Subskriptionen, die anderen Mitgliedern des Publish/Subscribe-Clusters bereitgestellt werden, vom Topic-Trennzeichen unmittelbar vor dem ersten Platzhalterzeichen aus dem Topic-Trennzeichen entfernt. Siehe Wildcards und Clusterthemen.

Daher kann das verwendete Platzhalterzeichen möglicherweise mehr Themenzeichenfolgen und mehr ständigen Veröffentlichungen entsprechen, als es mit der subskribierenden Anwendung übereinstimmt.

Dadurch wird der für die ständigen Veröffentlichungen benötigte Speicherplatz erhöht, und Sie müssen daher sicherstellen, dass die Speicherkapazität der Host-WS-Manager ausreicht.

Zugehörige Konzepte

Ständige Veröffentlichungen

Individuelle Proxy-Abonnementweiterleitung und Veröffentlichen überall

Hinweise zu REFRESH CLUSTER für Publish/Subscribe-Cluster

Die Ausgabe des Befehls **REFRESH CLUSTER** führt dazu, dass der Warteschlangenmanager vorübergehend lokal gehaltene Informationen zu einem Cluster löscht, einschließlich aller Clusterthemen und der zugehörigen Proxy-Subskriptionen.

Die Zeit, die von der Ausgabe des Befehls **REFRESH CLUSTER** bis zu dem Punkt, an dem der Warteschlangenmanager die erforderlichen Informationen für das Cluster-Publish/Subscribe erhält, benötigt wird, hängt von der Größe des Clusters, der Verfügbarkeit und der Reaktionsfähigkeit der Warteschlangenmanager mit vollständigem Repository ab.

Während der Aktualisierungsverarbeitung erfolgt die Unterbrechung des Publish/Subscribe-Datenverkehrs in einem Publish/Subscribe-Cluster. Bei großen Clustern kann die Verwendung des Befehls **REFRESH CLUSTER** den Cluster unterbrechen, während er in Bearbeitung ist, und danach in 27-Tage-Intervallen, wenn die Clusterobjekte automatisch Statusaktualisierungen an alle interessierten Warteschlangenmanager senden. Nähere Informationen hierzu erhalten Sie im Abschnitt Die Aktualisierung in einem großen Cluster kann sich auf die Leistung und Verfügbarkeit auswirken. Daher darf der Befehl **REFRESH CLUSTER** in einem Publish/Subscribe-Cluster nur unter Anleitung durch das zuständige IBM Support Center verwendet werden.

Die Unterbrechung des Clusters kann extern als die folgenden Symptome auftreten:

- Subskriptionen zu Clusterthemen in diesem WS-Manager erhalten keine Veröffentlichungen von Publishern, die mit anderen WS-Managern im Cluster verbunden sind.
- Nachrichten, die in Clusterthemen in diesem Warteschlangenmanager veröffentlicht werden, werden nicht an Subskriptionen auf anderen Warteschlangenmanagern weitergegeben.
- Subskriptionen für Clusterthemen in diesem Warteschlangenmanager, die in diesem Zeitraum erstellt wurden, senden nicht konsistent Proxy-Subskriptionen an andere Mitglieder des Clusters.
- Subskriptionen für Clusterthemen auf diesem Warteschlangenmanager, die in diesem Zeitraum gelöscht wurden, entfernen nicht konsistent die Proxy-Subskriptionen von anderen Membern des Clusters.
- 10-Sekunden-Pausen oder länger, bei Nachrichtenübermittlung.
- **MQPUT**-Fehler, z. B. MQRC_PUBLICATION_FAILURE.
- Veröffentlichungen, die in der Warteschlange für nicht zustellbare Nachrichten mit dem Grund MQRC_UNKNOWN_REMOTE_Q_MGR platziert wurden

Aus diesen Gründen müssen Publish/Subscribe-Anwendungen in den Quiescemodus versetzt werden, bevor der Befehl **REFRESH CLUSTER** ausgegeben wird.

Nachdem ein **REFRESH CLUSTER** -Befehl auf einem Warteschlangenmanager in einem Publish/Subscribe-Cluster ausgegeben wurde, warten Sie, bis alle Clusterwarteschlangenmanager und Clusterthemen erfolgreich aktualisiert wurden, und synchronisieren Sie dann die Proxy-Subskriptionen wie unter Resynchronisation von Proxy-Subskriptionenbeschrieben. Wenn alle Proxy-Subskriptionen ordnungsgemäß resynchronisiert wurden, starten Sie Ihre Publish/Subscribe-Anwendungen erneut.

Wenn die Ausführung eines **REFRESH CLUSTER** -Befehls viel Zeit in Anspruch nimmt, können Sie ihn überwachen, indem Sie sich die CURDEPTH von SYSTEM.CLUSTER.COMMAND.QUEUEansehen.

Zugehörige Konzepte

„Clustering: Best Practices für REFRESH CLUSTER verwenden" auf Seite 76
Sie verwenden den Befehl **REFRESH CLUSTER** , um alle lokal gespeicherten Informationen zu einem Cluster zu löschen und diese Informationen aus den vollständigen Repositorys im Cluster erneut zu erstellen. Sie sollten diesen Befehl nicht verwenden, außer in außergewöhnlichen Umständen. Wenn Sie es verwenden müssen, gibt es besondere Hinweise darauf, wie Sie es verwenden. Diese Informationen sind ein Leitfaden, der auf Tests und Feedback von Kunden basiert.

Anwendungsprobleme bei der Ausführung von REFRESH CLUSTER

Zugehörige Verweise

MQSC-Befehlsreferenz: REFRESH CLUSTER

Routing in Publish/Subscribe-Hierarchien

Wenn Ihre verteilte WS-Manager-Topologie eine Publish/Subscribe-Hierarchie ist und eine Subskription auf einem WS-Manager erfolgt, wird standardmäßig eine Proxy-Subskription auf jedem Warteschlangenmanager in der Hierarchie erstellt. Veröffentlichungen, die auf einem beliebigen WS-Manager empfangen werden, werden dann über die Hierarchie an jeden Warteschlangenmanager weitergeleitet, der eine übereinstimmende Subskription enthält.

Eine Einführung dazu, wie Nachrichten zwischen Warteschlangenmanagern in Publish/Subscribe-Hierarchien und Clustern weitergeleitet werden, finden Sie unter Verteilte Publish/Subscribe-Netze.

Wenn eine Subskription für ein Thema in einem Warteschlangenmanager in einer verteilten Publish/Subscribe-Hierarchie ausgeführt wird, verwaltet der Warteschlangenmanager den Prozess, mit dem die Subskription an verbundene Warteschlangenmanager weitergegeben wird. *Proxy-Subskriptionen* fließen zu allen Warteschlangenmanagern im Netz. Eine Proxy-Subskription gibt einem WS-Manager die Informationen, die er benötigt, um eine Veröffentlichung an diese Warteschlangenmanager weiterzuleiten, die Subskriptionen für dieses Thema enthalten. Jeder WS-Manager in einer Publish/Subscribe-Hierarchie kennt nur seine direkten Beziehungen. Veröffentlichungen, die an einen Warteschlangenmanager gestellt werden, werden über die direkten Beziehungen zu diesen Warteschlangenmanagern mit Subskriptionen gesendet. Dies wird in der folgenden Abbildung veranschaulicht, in der *Subskribent 1* eine Subskription für ein bestimmtes Thema auf dem Warteschlangenmanager *Asien* registriert (1). Proxy-Subskriptionen für diese Subskription auf dem Warteschlangenmanager *Asien* werden an alle anderen Warteschlangenmanager im Netz (2, 3, 4) weitergeleitet.

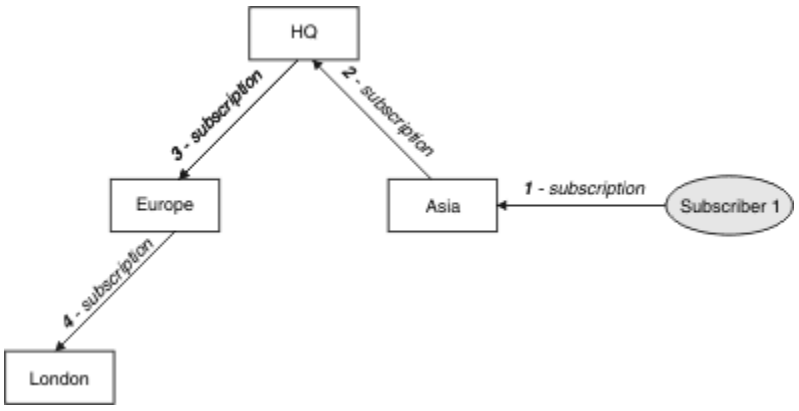


Abbildung 29. Weitergabe von Subskriptionen über ein Warteschlangenmanagernetzwerk

Ein Warteschlangenmanager konsolidiert alle erstellten Subskriptionen, unabhängig davon, ob er von lokalen Anwendungen oder von fernen Warteschlangenmanagern erstellt wird. Es erstellt Proxy-Subskriptionen für die Themen der Subskriptionen mit seinen Nachbarn, es sei denn, es ist bereits eine Proxy-Subskription vorhanden. Dies wird in der folgenden Abbildung veranschaulicht, in der *Subscriber 2* eine

Subskription für dasselbe Thema wie in Abbildung 29 auf Seite 116 auf dem Warteschlangenmanager *HQ* (5) registriert. Die Subskription für dieses Thema wird an den *Asia* -Warteschlangenmanager weitergeleitet, so dass es sich bewusst ist, dass Subskriptionen an anderer Stelle im Netz (6) vorhanden sind. Die Subskription wird nicht an den *Europe* -Warteschlangenmanager weitergeleitet, da bereits eine Subskription für dieses Thema registriert wurde. Weitere Informationen finden Sie in Schritt 3 in Abbildung 29 auf Seite 116.

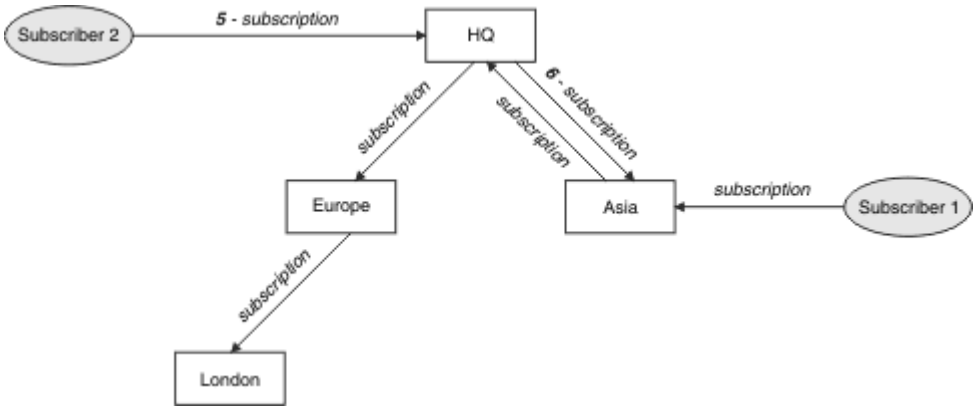


Abbildung 30. Mehrere Subskriptionen

Wenn eine Anwendung Informationen zu einem Thema veröffentlicht, leitet der empfangende WS-Manager sie standardmäßig an alle Warteschlangenmanager weiter, die gültige Subskriptionen für das Thema besitzen. Er kann ihn über einen oder mehrere temporäre Warteschlangenmanager weiterleiten. Dies wird in der folgenden Abbildung veranschaulicht, in der ein Publisher eine Veröffentlichung zu demselben Thema wie in Abbildung 30 auf Seite 117 an den Warteschlangenmanager *Europe* (7) sendet. Es ist eine Subskription für dieses Thema von *HQ* in *Europa* vorhanden, sodass die Veröffentlichung an den Warteschlangenmanager *HQ* (8) weitergeleitet wird. Es ist jedoch keine Subskription von *London* in *Europa* vorhanden (nur von *Europa* nach *London*), daher wird die Veröffentlichung nicht an den *London* -Warteschlangenmanager weitergeleitet. Der Warteschlangenmanager *HQ* sendet die Veröffentlichung direkt an *Subskribent 2* und an den Warteschlangenmanager *Asien* (9). Die Veröffentlichung wird an *Subskribent 1* von *Asien* (10) weitergeleitet.

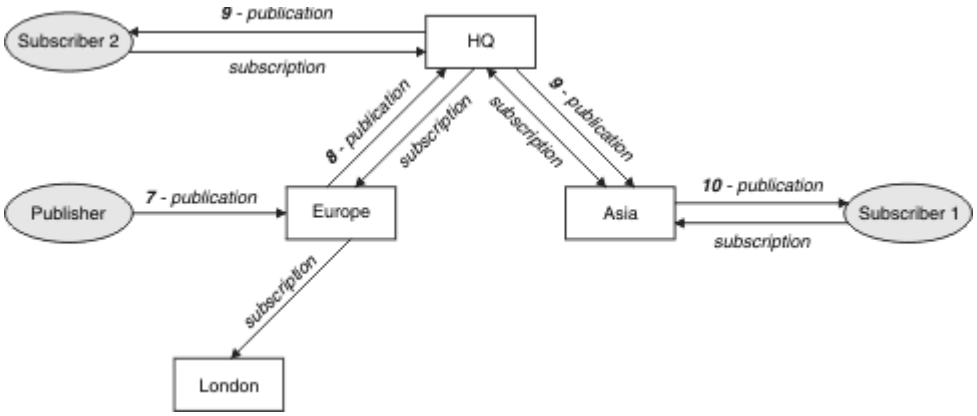


Abbildung 31. Weitergabe von Veröffentlichungen über ein Warteschlangenmanagernetzwerk

Wenn ein Warteschlangenmanager beliebige Veröffentlichungen oder Subskriptionen an einen anderen Warteschlangenmanager sendet, wird seine eigene Benutzer-ID in der Nachricht festgelegt. Wenn Sie eine Publish/Subscribe-Hierarchie verwenden und der eingehende Kanal so konfiguriert ist, dass Nachrichten mit der Berechtigung der Benutzer-ID in der Nachricht angezeigt werden, müssen Sie die Benutzer-ID des sendenden Warteschlangenmanagers berechtigen. Weitere Informationen finden Sie unter Standardbenutzer-IDs mit einer WS-Manager-Hierarchie verwenden .

Anmerkung: Wenn Sie stattdessen Publish/Subscribe-Cluster verwenden, wird die Berechtigung vom Cluster verarbeitet.

Zusammenfassung und weitere Hinweise

Eine Publish/Subscribe-Hierarchie gibt Ihnen präzise Kontrolle über die Beziehung zwischen WS-Managern. Nachdem er erstellt wurde, benötigt er wenig manuellen Eingriff für die Verwaltung. Es gibt jedoch auch bestimmte Einschränkungen auf Ihrem System:

- Die höheren Knoten in der Hierarchie, insbesondere der Stammknoten, müssen auf leistungsfähigen, hoch verfügbaren und leistungsfähigen Geräten gehostet werden. Dies liegt daran, dass mehr Veröffentlichungsverkehr durch diese Knoten fließen soll.
- Die Verfügbarkeit jedes Nicht-Leaf-WS-Managers in der Hierarchie wirkt sich auf die Fähigkeit des Netzes aus, Nachrichten von Publishern an Subskribenten auf anderen Warteschlangenmanagern zu abfließen.
- Standardmäßig werden alle Themenzeichenfolgen, die subskribiert sind, in der gesamten Hierarchie weitergegeben, und die Veröffentlichungen werden nur an ferne Warteschlangenmanager weitergegeben, die über eine Subskription für das zugeordnete Thema verfügen. Daher können schnelle Änderungen an der Gruppe von Subskriptionen zu einem Begrenzungsfaktor werden. Sie können dieses Standardverhalten ändern und stattdessen alle Publizierungsveröffentlichungen an alle Warteschlangenmanager weitergeben, wodurch die Notwendigkeit von Proxy-Subskriptionen entfällt. Weitere Informationen finden Sie im Abschnitt Subskriptionsleistung in Publish/Subscribe-Netzen.

  Anmerkung: Eine ähnliche Einschränkung gilt auch für direkte Routing-Cluster.
- Aufgrund der Vernetzung von Publish/Subscribe-Queue-Managern dauert es, bis Proxy-Subskriptionen sich über alle Knoten im Netz ausbreiten. Ferne Veröffentlichungen beginnen nicht unbedingt sofort, wenn sie sofort subskribiert werden, so dass frühzeitige Veröffentlichungen möglicherweise nicht nach einer Subskription für eine neue Themenzeichenfolge gesendet werden. Sie können die Probleme, die durch die Subskriptionsverzögerung verursacht werden, entfernen, indem alle Veröffentlichungen an alle Warteschlangenmanager weitergegeben werden, wodurch die Notwendigkeit von Proxy-Subskriptionen entfernt wird. Weitere Informationen finden Sie im Abschnitt Subskriptionsleistung in Publish/Subscribe-Netzen.

  Anmerkung: Diese Einschränkung gilt auch für direkte Routing-Cluster.
- Für eine Publish/Subscribe-Hierarchie erfordert das Hinzufügen oder Entfernen von Warteschlangenmanagern eine manuelle Konfiguration der Hierarchie, wobei die Position dieser Warteschlangenmanager und ihre Abhängigkeit von anderen WS-Managern sorgfältig berücksichtigt werden. Wenn Sie keine WS-Manager hinzufügen oder entfernen, die sich am Ende der Hierarchie befinden und deshalb keine weiteren Verzweigungen unterhalb der Hierarchie vorhanden sind, müssen Sie auch andere Warteschlangenmanager in der Hierarchie konfigurieren.

Bevor Sie eine Publish/Subscribe-Hierarchie als Routing-Mechanismus verwenden, untersuchen Sie die alternativen Ansätze, die in „Direktes Routing in Publish/Subscribe-Clustern” auf Seite 85 und „Thema Host-Routing in Publish/Subscribe-Clustern” auf Seite 90 detailliert beschrieben werden.

Verteilte Publish/Subscribe-Systemwarteschlangen

Vier Systemwarteschlangen werden von WS-Managern für Publish/Subscribe-Messaging verwendet. Sie müssen ihr Vorhandensein nur für Fehlerbestimmungs-und Kapazitätsplanungszwecke kennen.

Informationen zum Überwachen dieser Warteschlangen finden Sie im Abschnitt Produzenten und Konsumenten in Publish/Subscribe-Netzen abgleichen .

Tabelle 6. Publish/Subscribe-Systemwarteschlangen auf Multiplatforms-Plattformen

Systemwarteschlange	**Zweck**
SYSTEM.INTER.QMGR.CONTROL	Steuerwarteschlange für verteiltes Publish/Subscribe in IBM MQ

Tabelle 6. Publish/Subscribe-Systemwarteschlangen auf Multiplatforms-Plattformen (Forts.)	
Systemwarteschlange	**Zweck**
SYSTEM.INTER.QMGR.FANREQ	Eingabewarteschlange für den Fan-Out-Prozess der internen Proxy-Subskriptionen beim verteilten Publish/Subscribe in IBM MQ
SYSTEM.INTER.QMGR.PUBS	Veröffentlichungen für verteiltes Publish/Subscribe in IBM MQ
SYSTEM.HIERARCHY.STATE	Status der Hierarchiebeziehungen für verteiltes Publish/Subscribe in IBM MQ

z/OS Unter z/OS konfigurieren Sie die erforderlichen Systemobjekte beim Erstellen des Warteschlangenmanagers, indem Sie die Beispiele "CSQ4INSX", "CSQ4INSR" und "CSQ4INSG" in die Initialisierungseingabedatei "CSQINP2" einfügen. Weitere Informationen finden Sie in Task 13: Eingabedatengruppen für Initialisierung anpassen .

Die Attribute der Publish/Subscribe-Systemwarteschlangen sind in Tabelle 7 auf Seite 119 aufgeführt.

Tabelle 7. Attribute von Publish/Subscribe-Systemwarteschlangen	
Attribut	**Standardwert**
DEFPSIST	Ja
DEFSOPT	SHARED
MAXMSGL	Multi Unter Multiplatforms: Der des Parameters "MAXMSGL" im Befehl "ALTER QMGR" z/OS Unter z/OS: 4194304 (d. h. 4 MB)
MAXDEPTH	999999999
SHARE	nicht zutreffend
z/OS z/OS STGKLASSE	Dieses Attribut wird nur auf z/OS-Plattformen verwendet.

Anmerkung: Die einzige Warteschlange, die von Anwendungen gestellte Nachrichten enthält, ist SYSTEM.INTER.QMGR.PUBS. **MAXDEPTH** wird auf den Maximalwert für diese Warteschlange gesetzt, um eine temporäre Erstellung veröffentlichter Nachrichten während Ausfällen oder Zeiten übermäßiger Auslastung zu ermöglichen. Wenn der WS-Manager auf einem System ausgeführt wird, auf dem die Warteschlangenlänge nicht enthalten sein konnte, sollte dies angepasst werden.

Zugehörige Tasks

Verteilte Publish/Subscribe-Fehlerbehebung

Fehler in verteilten Publish/Subscribe-Systemwarteschlangen

Fehler können auftreten, wenn verteilte Publish/Subscribe-WS-Manager-Warteschlangen nicht verfügbar sind. Dies wirkt sich auf die Weitergabe von Subskriptionswissen über das Publish/Subscribe-Netz und die Veröffentlichung auf Subskriptionen auf fernen Warteschlangenmanagern aus.

Wenn die Fan-out-Anforderungswarteschlange SYSTEM.INTER.QMGR.FANREQ nicht verfügbar ist, kann die Erstellung einer Subskription einen Fehler generieren. Fehlernachrichten werden in das Fehlerprotokoll des Warteschlangenmanagers geschrieben, wenn Proxy-Subskriptionen direkt verbundenen Warteschlangenmanagers zugestellt werden müssen.

Wenn die Statuswarteschlange SYSTEM.HIERARCHY.STATE für Hierarchiebeziehungen nicht verfügbar ist, wird eine Fehlernachricht in das Fehlerprotokoll des Warteschlangenmanagers geschrieben und die Publish/Subscribe-Engine wird in den Modus COMPAT versetzt. Verwenden Sie den Befehl DISPLAY QMGR PSMODE, um den Publish/Subscribe-Modus anzuzeigen.

Wenn eine andere der SYSTEM.INTER.QMGR-Warteschlangen nicht verfügbar ist, wird eine Fehlernachricht in das Fehlerprotokoll des Warteschlangenmanagers geschrieben. Obwohl die Funktion nicht inaktiviert ist, werden Publish/Subscribe-Nachrichten wahrscheinlich in Warteschlangen auf diesem oder fernen Warteschlangenmanagern erstellt.

Wenn die Publish/Subscribe-Systemwarteschlange oder die erforderliche Übertragungswarteschlange für einen übergeordneten, untergeordneten oder Publish/Subscribe-Cluster-WS-Manager nicht verfügbar ist, treten die folgenden Ergebnisse auf:

- Die Veröffentlichungen werden nicht zugestellt, und eine Veröffentlichungsanwendung kann einen Fehler empfangen. Ausführliche Informationen zu Fehlern, welche die Veröffentlichungsanwendung empfängt, finden Sie in den folgenden Parametern des Befehls **DEFINE TOPIC**: **PMSGDLV**, **NPMSGDLV** und **USEDLQ**.
- Empfangen von Veröffentlichungen zwischen WS-Managern wird in der Eingabewarteschlange zurückgesetzt und anschließend erneut versucht. Wenn der Rücksetzungsschwellenwert erreicht ist, werden die unzustellbare Veröffentlichungen in die Warteschlange für nicht zustellbare Nachrichten gestellt. Das Fehlerprotokoll des Warteschlangenmanagers enthält Details zu dem Problem.
- Eine unzustellbare Proxy-Subskription wird in der Warteschlange für die Fanoutanforderungswarteschlange zurückgesetzt und anschließend erneut versucht. Wenn der Rücksetzungsschwellenwert erreicht ist, wird die unzustellbare Proxy-Subskription nicht an einen verbundenen Warteschlangenmanager geliefert und in die Warteschlange für nicht zustellbare Nachrichten gestellt. Das Fehlerprotokoll des Warteschlangenmanagers enthält Details zu dem Problem, einschließlich der Details der erforderlichen erforderlichen Korrekturmaßnahmen.
- Nachrichten des Hierarchiebeziehungsprotokolls schlagen fehl und der Verbindungsstatus wird als ERROR markiert. Verwenden Sie den Befehl **DISPLAY PUBSUB**, um den Verbindungsstatus anzuzeigen.

Zugehörige Tasks

Verteilte Publish/Subscribe-Fehlerbehebung

Multi Speicher-und Leistungsanforderungen auf Multiplatforms planen

Sie müssen realistische und erreichbare Speicher-und Leistungsziele für Ihr IBM MQ-System festlegen. Verwenden Sie die Links, um Informationen zu Faktoren zu finden, die sich auf die Speicherung und Leistung auf Ihrer Plattform auswirken.

Die Anforderungen sind unterschiedlich und hängen davon ab, auf welchen Systemen Sie IBM MQ einsetzen und welche Komponenten Sie verwenden möchten.

Aktuelle Informationen zu den unterstützten Hardware- und Softwareumgebungen finden Sie unter Systemvoraussetzungen für IBM MQ.

IBM MQ speichert Warteschlangenmanagerdaten im Dateisystem. Unter den folgenden Links finden Sie Informationen zur Planung und Konfiguration der Verzeichnisstrukturen für die Verwendung mit IBM MQ:

- „Unterstützung von Dateisystemen auf Multiplatforms planen” auf Seite 125
- „Voraussetzungen für gemeinsam genutzte Dateisysteme auf Multiplatforms” auf Seite 126
- „IBM MQ-Dateien in Multiplatforms gemeinsam nutzen” auf Seite 136
- Linux AIX „Verzeichnisstruktur auf Systemen mit AIX and Linux” auf Seite 138
- Windows „Verzeichnisstruktur auf Systemen mit Windows” auf Seite 148
- IBM i „Verzeichnisstruktur unter IBM i” auf Seite 152

Unter folgenden Links erhalten Sie Informationen zu Systemressourcen, gemeinsam genutzten Speicher und Prozesspriorität unter AIX and Linux:

- Linux AIX „IPC-Ressourcen für IBM MQ und UNIX System V” auf Seite 156
- AIX „gemeinsam genutzter Speicher unter AIX” auf Seite 156
- Linux AIX „Prozesspriorität von IBM MQ und UNIX” auf Seite 156

Verwenden Sie die folgenden Links, um Informationen zu Protokolldateien zu erhalten:

- „Kreisförmige oder lineare Protokollierung auf Multiplatforms auswählen” auf Seite 155
- Protokollgröße berechnen

Zugehörige Konzepte

„IBM MQ-Umgebung unter z/OS planen” auf Seite 157
Bei der Planung einer IBM MQ-Umgebung müssen Sie den Ressourcenbedarf für Datasets, Seitengruppen, Db2 und Coupling-Facilitys sowie den Bedarf an Protokollierungs- und Sicherungsfunktionen berücksichtigen. Die Informationen in diesem Thema helfen Ihnen, eine IBM MQ-Umgebung zu planen.

Zugehörige Tasks

„IBM MQ-Architektur planen” auf Seite 5
Beachten Sie bei der Planung einer IBM MQ-Umgebung die Unterstützung, die IBM MQ für Architekturen mit einzelnen oder mehreren Warteschlangenmanagern sowie für Punkt-zu-Punkt- und Publish/Subscribe-Messaging bereitstellt. Planen Sie auch den Ressourcenbedarf und die Nutzung von Protokollierungs- und Sicherheitsfunktionen.

Zugehörige Verweise

Hardware- und Softwarevoraussetzungen unter AIX and Linux
Hardware- und Softwarevoraussetzungen unter Windows

Multi Erforderl. Plattenspeicherplatz auf Multiplatforms-Plattformen

Der Speicherbedarf für IBM MQ ist davon abhängig, welche Komponenten Sie installieren und wie viel Arbeitsspeicher Sie benötigen.

Der Plattenspeicher ist für die optionalen Komponenten, die Sie installieren möchten, erforderlich, einschließlich aller vorausgesetzten Komponenten, die sie benötigen. Der Gesamtspeicherbedarf hängt auch von der Anzahl der verwendeten Warteschlangen, der Anzahl und Größe der Nachrichten in den Warteschlangen und davon ab, ob die Nachrichten permanent sind. Sie benötigen außerdem die Archivierungskapazität auf Platte, Band oder anderen Medien sowie Speicherplatz für Ihre eigenen Anwendungsprogramme.

Die folgenden Tabellen zeigen den ungefähren Plattenspeicherplatz, der erforderlich ist, wenn Sie verschiedene Kombinationen des Produkts auf verschiedenen Plattformen installieren. (Die Werte werden auf die nächsten 5 MB aufgerundet, wobei ein MB 1.048.576 Byte beträgt.)

- LTS „Erforderlicher Plattenspeicherplatz für Long Term Support” auf Seite 121
- CD „Erforderlicher Plattenspeicherplatz für Continuous Delivery” auf Seite 122

Erforderlicher Plattenspeicherplatz für Long Term Support

V 9.2.0 LTS

Tabelle 8. IBM MQ-Plattenspeicherbedarf für Multiplatforms für Long Term Support

Plattform	Clientinstallation „1” auf Seite 122	Serverinstallation „2” auf Seite 122	Vollständige Installation „3” auf Seite 122
AIX AIX	325 MB	370 MB	1690 MB

Tabelle 8. IBM MQ-Plattenspeicherbedarf für Multiplatforms für Long Term Support (Forts.)			
Plattform	**Clientinstallation** „1" auf Seite 122	**Serverinstallation** „2" auf Seite 122	**Vollständige Installation** „3" auf Seite 122
IBM i IBM i (siehe Zusätzliche Hinweise für IBM i)	480 MB	840 MB	1815 MB
Linux Linux for x86-64	245 MB	270 MB	1835 MB
Linux Linux on POWER Systems - Little Endian	150 MB	170 MB	1205 MB
Linux Linux for IBM Z	235 MB	260 MB	1240 MB
Windows Windows (64-Bit-Installation) „4" auf Seite 122	280 MB	390 MB	1755 MB

Anmerkungen:

1. Eine Clientinstallation umfasst die folgenden Komponenten:
   - Laufzeit
   - Client
2. Eine Serverinstallation umfasst die folgenden Komponenten:
   - Laufzeit
   - Server
3. Eine vollständige Installation enthält alle verfügbaren Komponenten.
4. Windows Nicht alle der hier aufgelisteten Komponenten können auf Windows-Systemen installiert werden; ihre Funktionalität ist gelegentlich in anderen Komponenten enthalten. Siehe IBM MQ-Features für Windows-Systeme.

Zusätzliche Hinweise für IBM i: IBM i

1. Unter IBM i können Sie den nativen Client nicht vom Server trennen. Die Zahlenangaben für den Server in der Tabelle beziehen sich auf 5724H72*BASE ohne Java und mit dem englischen Sprachenlademodul (2924). Es gibt 22 mögliche eindeutige Sprachladevorgänge.
2. Die Zahlenangaben in der Tabelle beziehen sich auf den nativen Client 5725A49 *BASE ohne Java.
3. Java- und JMS-Klassen können Servern und Clients als Bindungen hinzugefügt werden. Wenn Sie diese Features hinzufügen möchten, fügen Sie 110 MB hinzu.
4. Wenn dem Client oder Server eine Beispielquelle hinzugefügt wird, werden zusätzliche 10 MB hinzugefügt.
5. Durch das Hinzufügen von Beispielen zu Java und JMS-Klassen werden zusätzliche 5 MB benötigt.

Erforderlicher Plattenspeicherplatz für Continuous Delivery

CD

Tabelle 9. IBM MQ-Plattenspeicherbedarf für Multiplatforms für Continuous Delivery			
Plattform/CD-Release	**Clientinstallation** „1" auf Seite 124	**Serverinstallation** „2" auf Seite 125	**Vollständige Installation** „3" auf Seite 125
AIX **AIX**			
V 9.2.0 IBM MQ 9.2.0	150 MB	205 MB	1410 MB
V 9.2.1 IBM MQ 9.2.1	325 MB	370 MB	1690 MB
V 9.2.2 IBM MQ 9.2.2	325 MB	370 MB	1690 MB
V 9.2.3 IBM MQ 9.2.3	325 MB	370 MB	1690 MB
V 9.2.4 IBM MQ 9.2.4	330 MB	375 MB	1690 MB
V 9.2.5 IBM MQ 9.2.5	330 MB	375 MB	1760 MB
Linux **Linux für x86-64 (64 Bit)**			
V 9.2.0 IBM MQ 9.2.0	130 MB	185 MB	1645 MB
V 9.2.1 IBM MQ 9.2.1	245 MB	270 MB	1835 MB
V 9.2.2 IBM MQ 9.2.2	245 MB	270 MB	1835 MB
V 9.2.3 IBM MQ 9.2.3	245 MB	270 MB	1835 MB
V 9.2.4 IBM MQ 9.2.4	245 MB	270 MB	1870 MB
V 9.2.5 IBM MQ 9.2.5	265 MB	295 MB	2010 MB
Linux **Linux on POWER Systems - Little Endian**			
V 9.2.0 IBM MQ 9.2.0	95 MB	135 MB	1100 MB
V 9.2.1 IBM MQ 9.2.1	150 MB	170 MB	1205 MB
V 9.2.2 IBM MQ 9.2.2	150 MB	170 MB	1205 MB

Tabelle 9. IBM MQ-Plattenspeicherbedarf für Multiplatforms für Continuous Delivery (Forts.)			
Plattform/CD-Release	**Clientinstallation** **„1" auf Seite 124**	**Serverinstallation** **„2" auf Seite 125**	**Vollständige Installation** **„3" auf Seite 125**
V 9.2.3 IBM MQ 9.2.3	150 MB	170 MB	1205 MB
V 9.2.4 IBM MQ 9.2.4	150 MB	170 MB	1210 MB
V 9.2.5 IBM MQ 9.2.5	170 MB	190 MB	1350 MB
Linux **Linux for IBM Z**			
V 9.2.0 IBM MQ 9.2.0	130 MB	175 MB	1130 MB
V 9.2.1 IBM MQ 9.2.1	235 MB	265 MB	1255 MB
V 9.2.2 IBM MQ 9.2.2	235 MB	265 MB	1255 MB
V 9.2.3 IBM MQ 9.2.3	235 MB	265 MB	1255 MB
V 9.2.4 IBM MQ 9.2.4	235 MB	265 MB	1300 MB
V 9.2.5 IBM MQ 9.2.5	255 MB	290 MB	1435 MB
Windows **Windows (64-Bit-Installation)** „4" auf Seite 125			
V 9.2.0 IBM MQ 9.2.0	230 MB	365 MB	1565 MB
V 9.2.1 IBM MQ 9.2.1	280 MB	390 MB	1900 MB
V 9.2.2 IBM MQ 9.2.2	280 MB	390 MB	1900 MB
V 9.2.3 IBM MQ 9.2.3	280 MB	390 MB	1900 MB
V 9.2.4 IBM MQ 9.2.4	280 MB	390 MB	1950 MB
V 9.2.5 IBM MQ 9.2.5	290 MB	410 MB	2095 MB

Anmerkungen:

1. Eine Clientinstallation umfasst die folgenden Komponenten:

- Laufzeit
- Client

2. Eine Serverinstallation umfasst die folgenden Komponenten:
   - Laufzeit
   - Server
3. Eine vollständige Installation enthält alle verfügbaren Komponenten.
4. Windows Nicht alle der hier aufgelisteten Komponenten können auf Windows-Systemen installiert werden; ihre Funktionalität ist gelegentlich in anderen Komponenten enthalten. Siehe IBM MQ-Features für Windows-Systeme.

Zugehörige Konzepte
Komponenten und Funktionen von IBM MQ

Multi Unterstützung von Dateisystemen auf Multiplatforms planen

WS-Manager-Daten werden im Dateisystem gespeichert. Ein Warteschlangenmanager verwendet die Sperrung von Dateisystemen, um zu verhindern, dass mehrere Instanzen eines Warteschlangenmanagers mit mehreren Instanzen gleichzeitig aktiv sind.

Gemeinsam genutzte Dateisysteme

Gemeinsam genutzte Dateisysteme ermöglichen es mehreren Systemen, gleichzeitig auf dieselbe physische Speichereinheit zuzugreifen. Eine Unterbrechung würde auftreten, wenn mehrere Systeme direkt auf dieselbe physische Speichereinheit zugegriffen haben, ohne dass die Steuerung von Sperren und gemeinsamen Zugriff erzwungen werden muss. Betriebssysteme stellen lokale Dateisysteme mit Sperrung und Steuerung des gemeinsamen Zugriffs für lokale Prozesse bereit. Netzdateisysteme stellen die Steuerung von Sperren und die Steuerung des gemeinsamen Zugriffs für verteilte Systeme bereit.

Historische, vernetzte Dateisysteme haben nicht schnell genug ausgeführt oder eine ausreichende Sperrung und Steuerung des gemeinsamen Zugriffs bereitgestellt, um die Anforderungen für die Protokollierung von Nachrichten zu erfüllen. Heute können vernetzte Dateisysteme eine gute Leistung bieten und Implementierungen zuverlässiger Netzdateisystemprotokolle, wie z. B. *RFC 3530, Network File System (NFS) Version 4, Protokoll* , erfüllen die Anforderungen für die zuverlässige Protokollierung von Nachrichten.

Gemeinsam genutzte Dateisysteme und IBM MQ

WS-Manager-Daten für einen WS-Manager mit mehreren Instanzen werden in einem gemeinsam genutzten Netzdateisystem gespeichert. Auf Systemen mit AIX, Linux, and Windows müssen die Datendateien und Protokolldateien des Warteschlangenmanagers in ein gemeinsam genutztes Netzdateisystem gestellt werden. IBM i Unter IBM i werden Journale anstelle von Protokolldateien verwendet, und Journale können nicht gemeinsam genutzt werden. Multi-Instanz-Warteschlangenmanager unter IBM i verwenden die Journalreplikation, oder umschaltbare Journale, um die Journale für mehrere Warteschlangenmanagerinstanzen gleichzeitig verfügbar zu machen.

IBM MQ verwendet Sperren, um zu verhindern, dass mehrere Instanzen desselben Multi-Instanz-Warteschlangenmanagers gleichzeitig aktiv sind. Dieselbe Sperre stellt auch sicher, dass zwei separate Warteschlangenmanager nicht versehentlich die gleiche Gruppe von WS-Manager-Datendateien verwenden können. Es kann immer nur eine Instanz eines Warteschlangenmanagers gleichzeitig gesperrt sein. Aus diesem Grund unterstützt IBM MQ Warteschlangenmanagerdaten, die in einem vernetzten Speicher gespeichert sind, auf den als gemeinsam genutztes Dateisystem zugegriffen wird.

Da nicht alle Sperrprotokolle von Netzdateisystemen stabil sind und ein Dateisystem möglicherweise für die Leistung und nicht für die Datenintegrität konfiguriert ist, müssen Sie den Befehl **amqmfsck** ausführen, um zu testen, ob ein Netzdateisystem den Zugriff auf Warteschlangenmanagerdaten und -Protokolle

ordnungsgemäß steuert. Dieser Befehl ist nur auf UNIX, Linux und IBM i Systeme anwendbar. Unter Windows gibt es nur ein unterstütztes Netzdateisystem, sodass der Befehl **amqmfsck** nicht benötigt wird.

Zugehörige Tasks

„Verhalten des gemeinsam genutzten Dateisystems auf mehreren Plattformen überprüfen" auf Seite 128
Führen Sie **amqmfsck** aus, um zu prüfen, ob ein geteiltes Dateisystem auf AIX, Linux , oder IBM i die Anforderungen erfüllt, die Warteschlangenmanagerdaten eines Multiinstanzwarteschlangenmanagers. (Die einzige Voraussetzung für eine Windows-Konfiguration ist, dass SMB 3 für die Bereitstellung gemeinsam genutzten Speichers verwendet wird.)

Multi Voraussetzungen für gemeinsam genutzte Dateisysteme auf Multiplatforms

Gemeinsam genutzte Dateisysteme müssen Folgendes ermöglichen: Schreibintegrität für Daten, garantiert exklusiven Zugriff auf Dateien und die Aufhebung von Sperren für den Fall, dass kein zuverlässiges Arbeiten mit IBM MQ möglich ist.

Anforderungen an ein gemeinsam genutztes Dateisystem

Für ein zuverlässiges Zusammenwirken mit IBM MQ muss ein gemeinsam genutztes Dateisystem drei grundsätzliche Voraussetzungen erfüllen:

1. Datenschreibintegrität

   Die Datenschreibintegrität wird manchmal auch als *Write through to disk on disk on flush* bezeichnet. Der Warteschlangenmanager muss in der Lage sein, mit Daten zu synchronisieren, die erfolgreich auf der physischen Einheit festgeschrieben wurden. In einem transaktionsorientierten System müssen Sie sicherstellen, dass einige Schreibvorgänge sicher festgeschrieben wurden, bevor Sie mit der anderen Verarbeitung fortfahren können.

   Spezifischer IBM MQ for AIX or LinuxPlattformen verwenden die *O_SYNC*offene Oprion und der `fsync()` Systemaufruf, um explizit Schreiben auf behebbare Medien zu erzwingen und die Schreiboperation hängt davon ab, ob diese Optionen richtig funktionieren.

   Achtung: Linux Sie sollten das Dateisystem mit der Option `async` anhängen, die weiterhin die Option synchroner Schreibvorgänge unterstützt und eine bessere Leistung bietet als die Option `sync` .

   Es ist jedoch zu beachten, dass das Dateisystem, falls es aus Linux exportiert wurde, weiterhin mit der Option `sync` exportiert werden muss.

2. Garantiert exklusiver Zugriff auf Dateien

   Damit mehrere Warteschlangenmanager synchronisiert werden können, muss ein Mechanismus für einen Warteschlangenmanager vorhanden sein, um eine exklusive Sperre für eine Datei zu erhalten.

3. Release-Sperren bei einem Ausfall

   Wenn ein Warteschlangenmanager ausfällt oder wenn ein Kommunikationsfehler mit dem Dateisystem vorliegt, müssen die vom Warteschlangenmanager gesperrten Dateien entsperrt und anderen Prozessen zur Verfügung gestellt werden, ohne zu warten, dass der Warteschlangenmanager erneut mit dem Dateisystem verbunden wird.

Damit IBM MQ zuverlässig funktioniert, muss ein gemeinsam genutztes Dateisystem diese Anforderungen erfüllen. Ist dies nicht der Fall, werden die Daten und Protokolle des Warteschlangenmanagers beschädigt, wenn das gemeinsam genutzte Dateisystem in einer Multi-Instanz-WS-Manager-Konfiguration verwendet wird.

Bei Warteschlangenmanagern mit mehreren Instanzen unter Microsoft Windowsmuss auf den Netzspeicher über das SMB-Protokoll (Server Message Block) zugegriffen werden, das von Microsoft Windows -Netzen verwendet wird. Der SMB-Client (Server Message Block) erfüllt nicht die IBM MQ -Anforderungen für die Sperrsemantik auf anderen Plattformen als Microsoft Windows. Daher dürfen Warteschlangenma-

nager mit mehreren Instanzen, die auf anderen Plattformen als Microsoft Windows ausgeführt werden, Server Message Block (SMB) nicht als gemeinsam genutztes Dateisystem verwenden.

Für WS-Manager mit mehreren Instanzen auf anderen unterstützten Plattformen muss auf den Speicher durch ein Netzdateisystemprotokoll zugegriffen werden, das mit der Position "Posix-konform" kompatibel ist, und unterstützt die lease-basierte Sperrung. Network File System 4 erfüllt diese Anforderung. Ältere Dateisysteme, wie z. B. Network File System Version 3, die keinen zuverlässigen Mechanismus zum Freigeben von Sperren nach einem Fehler aufweisen, dürfen nicht mit Warteschlangenmanagern mit mehreren Instanzen verwendet werden.

Überprüfung der Anforderungen an das gemeinsam genutzte Dateisystem

Sie müssen überprüfen, ob das gemeinsam genutzte Dateisystem, das Sie verwenden möchten, diese Anforderungen erfüllt. Außerdem müssen Sie überprüfen, ob das Dateisystem ordnungsgemäß für die Zuverlässigkeit konfiguriert ist. Gemeinsam genutzte Dateisysteme bieten manchmal Konfigurationsoptionen, um die Leistung auf Kosten der Zuverlässigkeit zu verbessern.

Weitere Informationen finden Sie unter Testing statement for IBM MQ multi-instance queue manager file systems(Test- und Unterstützungsangaben für Multi-Instanz-Warteschlangenmanager in IBM MQ).

Unter normalen Umständen funktioniert IBM MQ ordnungsgemäß mit dem Attributcaching, und es ist nicht erforderlich, das Caching zu inaktivieren, z. B. indem Sie NOAC auf einem NFS-Mount festlegen. Das Attributcaching kann Probleme verursachen, wenn mehrere Dateisystemclients für Schreibzugriff auf dieselbe Datei auf dem Dateisystemserver kontendieren, da die zwischengespeicherten Attribute, die von den einzelnen Clients verwendet werden, möglicherweise nicht mit den Attributen auf dem Server identisch sind. Ein Beispiel für Dateien, auf die auf diese Weise zugegriffen wird, sind WS-Manager-Fehlerprotokolle für einen Multi-Instanz-Warteschlangenmanager. Die WS-Manager-Fehlerprotokolle können sowohl durch eine aktive als auch durch eine Standby-Warteschlangenmanagerinstanz geschrieben werden, und die Attribute der Cachedatei können dazu führen, dass die Fehlerprotokolle größer werden als erwartet, bevor die Rollover der Dateien auftreten.

Um die Überprüfung des Dateisystems zu unterstützen, führen Sie die Task Verhalten des gemeinsam genutzten Dateisystems überprüfen aus. Diese Task prüft, ob das gemeinsam genutzte Dateisystem die Anforderungen 2 und 3erfüllt. Sie müssen die Anforderung 1 in der Dokumentation des gemeinsam genutzten Dateisystems prüfen oder indem Sie mit Protokolldaten auf der Platte experimentieren.

Plattenfehler können beim Schreiben auf Platte zu Fehlern führen, die IBM MQ als Erfassung von Fehlerdaten beim ersten Auftreten (First Failure Data Capture) meldet. Sie können das Dateisystemprüfprogramm für Ihr Betriebssystem ausführen, um das gemeinsam genutzte Dateisystem auf Plattenfehler zu überprüfen. For example:

- Linux AIX Auf AIX and Linux-Plattformen heißt das Dateisystemprüfprogramm "fsck".
- Windows Auf Windows-Plattformen heißt das Dateisystemprüfprogramm "CHKDSK" oder "SCANDISK".

Sicherheit des NFS-Servers

Anmerkungen:

- Sie können die Optionen **nosuid** oder **noexec** nicht für einen Mountpunkt verwenden, der das IBM MQ -Installationsverzeichnis enthält. Dies liegt daran, dass IBM MQ ausführbare setuid/setgid-Programme enthält, die nicht ordnungsgemäß ausgeführt werden dürfen.
- Wenn Sie WS-Manager-Daten nur auf einem Network File System-Server (NFS) einreihen, können Sie die folgenden drei Optionen mit dem Mountbefehl verwenden, um das System sicher zu machen, ohne dass die Ausführung des Warteschlangenmanagers beeinträchtigt wird:

  noexec
  Wenn Sie diese Option verwenden, stoppen Sie die Ausführung von Binärdateien auf dem NFS, wodurch verhindert wird, dass ein ferner Benutzer nicht mehr benötigten Code auf dem System ausführen kann.

nosuid
Wenn Sie diese Option verwenden, verhindern Sie die Verwendung der Bits "set-user-identifier" und "set-group-identifier bits", die verhindert, dass ein ferner Benutzer höhere Berechtigungen erhält.

nodev
Wenn Sie diese Option verwenden, stoppen Sie die Zeichen-und Blockspezial-Einheiten, die verwendet oder definiert werden, wodurch verhindert wird, dass ein ferner Benutzer aus einem chroot-Gefängnis heraus kommt.

Linux IBM i AIX *Verhalten des gemeinsam genutzten Dateisystems auf mehreren Plattformen überprüfen*

Führen Sie **amqmfsck** aus, um zu prüfen, ob ein geteiltes Dateisystem auf AIX, Linux , oder IBM i die Anforderungen erfüllt, die Warteschlangenmanagerdaten eines Multiinstanzwarteschlangenmanagers. (Die einzige Voraussetzung für eine Windows-Konfiguration ist, dass SMB 3 für die Bereitstellung gemeinsam genutzten Speichers verwendet wird.)

Vorbereitende Schritte

Sie benötigen einen Server mit vernetztem Speicher und zwei weitere Server, die mit ihm verbunden sind, auf denen IBM MQ installiert ist. Sie müssen über die Administratorberechtigung (Root) verfügen, um das Dateisystem konfigurieren zu können, und ein IBM MQ-Administrator sein, um **amqmfsck** ausführen zu können.

Informationen zu diesem Vorgang

Unter „Voraussetzungen für gemeinsam genutzte Dateisysteme auf Multiplatforms” auf Seite 126 sind die Dateisystemanforderung für die Verwendung eines gemeinsam genutzten Dateisystems mit Multi-Instanz-Warteschlangenmanagern beschrieben. In der IBM MQ-Technote Testing statement for IBM MQ multi-instance queue manager file systems werden die gemeinsam genutzten Systeme aufgeführt, mit denen IBM bereits getestet wurde. Die Prozedur in dieser Task beschreibt, wie Sie ein Dateisystem testen, um zu bewerten, ob ein nicht aufgelistete Dateisysteme die Datenintegrität aufrecht erhalten.

Der Failover eines Multi-Instanz-WS-Managers kann durch Hardware-oder Softwarefehler ausgelöst werden, einschließlich Netzproblemen, die verhindern, dass der WS-Manager in seine Daten oder Protokolldateien schreibt. Hauptsächlich sind Sie daran interessiert, Fehler auf dem Dateiserver zu verursachen. Aber Sie müssen auch Fehler auf den IBM MQ-Servern verursachen, um erfolgreich freigegebene Sperren zu testen. Damit Sie in einem gemeinsam genutzten Dateisystem vertrauen können, testen Sie alle folgenden Fehler und alle anderen Fehler, die für Ihre Umgebung spezifisch sind:

1. Das Betriebssystem auf dem Dateiserver herunterfahren, einschließlich der Synchronisierung der Platten.
2. Das Betriebssystem auf dem Dateiserver anhalten, ohne die Platten zu synchronisieren.
3. Drücken Sie die Grundstellungsschaltfläche auf jedem der Server.
4. Ausziehen des Netzkabels aus jedem der Server.
5. Ziehen Sie das Netzkabel aus jedem der Server heraus.
6. Schalten Sie die einzelnen Server aus.

Erstellen Sie das Verzeichnis im Netzspeicher, den Sie für die gemeinsame Nutzung von WS-Manager-Daten und -Protokollen verwenden werden. Der Verzeichniseigner muss ein IBM MQ-Administrator sein, oder anders gesagt, ein Mitglied der `mqm`-Gruppe in AIX and Linux sein. Der Benutzer, der die Tests ausführt, muss über die IBM MQ-Administratorberechtigung verfügen.

Verwenden Sie das Beispiel des Exports und der Montage eines Dateisystems in Einen Multiinstanzwarteschlangenmanager erstellen aufLinuxoder Einen Multiinstanzwarteschlangenmanager erstellen durch Verwendung des zeitgleichen Spiegelns eines Journals und Netserver auf IBM i, um Ihnen zu helfen, das Dateisystem zu konfigurieren. Unterschiedliche Dateisysteme erfordern unterschiedliche Konfigurationsschritte. Lesen Sie die Dokumentation zum Dateisystem.

Anmerkung: Führen Sie das IBM MQ MQI client -Beispielprogramm **amqsfhac** parallel zu **amqmfsck** aus, um zu demonstrieren, dass ein Warteschlangenmanager die Nachrichtenintegrität während eines Fehlers beibehält.

Vorgehensweise

Bei jedem der Prüfungen führen Sie alle Fehler in der vorherigen Liste durch, während die Dateisystemprüffunktion ausgeführt wird. Wenn Sie **amqsfhac** gleichzeitig mit **amqmfsck** ausführen möchten, müssen Sie die Task „amqsfhac zum Testen der Nachrichtenintegrität ausführen" auf Seite 133 parallel mit dieser Task ausführen.

1. Hängen Sie das exportierte Verzeichnis auf den beiden IBM MQ-Servern an.

   Erstellen Sie auf dem Dateisystemserver ein gemeinsam genutzes Verzeichnis `shared` und ein Unterverzeichnis zum Speichern der Daten für Multi-Instanz-Warteschlangenmanager, `qmdata`. Für ein Beispiel der Anmeldung eines freigegebenen Verzeichnisses für Multinstanzwarteschlangenmanager auf Linux, sehen Sie Einen Multiinstanzwarteschlangenmanager erstellen auf Linux
2. Überprüfen Sie das Verhalten des Basisdateisystems.

   Führen Sie auf einem der IBM MQ-Server das Dateisystemprüfprogramm ohne Parameter aus.

   Auf IBM MQ-Server 1:

   ```
   amqmfsck /shared/qmdata
   ```
3. Prüfen Sie das gleichzeitige Schreiben von beiden IBM MQ-Servern in dasselbe Verzeichnis.

   Führen Sie das Dateisystemprüfprogramm auf beiden IBM MQ-Servern gleichzeitig mit der Option `-c` aus.

   Auf IBM MQ-Server 1:

   ```
   amqmfsck -c /shared/qmdata
   ```

   Auf IBM MQ-Server 2:

   ```
   amqmfsck -c /shared/qmdata
   ```
4. Prüfen Sie auf beiden IBM MQ-Servern das Warten auf Sperren und deren Freigabe.

   Führen Sie das Dateisystemprüfprogramm auf beiden IBM MQ-Servern gleichzeitig mit der Option `-w` aus.

   Auf IBM MQ-Server 1:

   ```
   amqmfsck -w /shared/qmdata
   ```

   Auf IBM MQ-Server 2:

   ```
   amqmfsck -w /shared/qmdata
   ```
5. Überprüfen Sie die Datenintegrität.

   a) Formatieren Sie die Testdatei.

   Erstellen Sie eine große Datei in dem Verzeichnis, das getestet wird. Die Datei wird so formatiert, dass die nachfolgenden Phasen erfolgreich abgeschlossen werden können. Die Datei muss groß genug sein, dass genügend Zeit vorhanden ist, um die zweite Phase zu unterbrechen, um die Funktionsübernahme zu simulieren. Versuchen Sie, den Standardwert von 262144 Seiten (1 GB) zu verwenden. Das Programm reduziert diese Standardeinstellung bei langsamen Dateisystemen automatisch, so dass die Formatierung in ca. 60 Sekunden abgeschlossen wird.

Auf IBM MQ-Server 1:

```
amqmfsck -f /shared/qmdata
```

Der Server antwortet mit den folgenden Nachrichten:

```
Formatting test file for data integrity test.

Test file formatted with 262144 pages of data.
```

b) Schreiben Sie Daten mit Hilfe des Dateisystemprüfers in die Testdatei, und verursachen Sie einen Fehler.

Führen Sie das Testprogramm auf zwei Servern zur gleichen Zeit aus. Starten Sie das Testprogramm auf dem Server, auf dem der Fehler auftreten wird, und starten Sie dann das Testprogramm auf dem Server, das den Fehler überleben wird. Ursache des Fehlers, den Sie untersuchen.

Das erste Testprogramm stoppt mit einer Fehlernachricht. Das zweite Testprogramm ruft die Sperre für die Testdatei ab und schreibt Daten in die Testdatei, in der das erste Testprogramm abgelassen wurde. Lassen Sie das zweite Testprogramm zum Abschluss führen.

Tabelle 10. Datenintegritätsprüfung auf zwei Servern zur gleichen Zeit ausführen

IBM MQ-Server 1	**IBM MQ-Server 2**
`amqmfsck -a /shared/qmdata`	

`Please start this program on a second ma chine with the same parameters.`
 	
`File lock acquired.`
 	
`Start a second copy of this program with the same parameters on another ser ver.`
 	
`Writing data into test file.`
 	
`To increase the effectiveness of the test, interrupt the writing by ending the pro cess, temporarily breaking the network connecti on to the networked storage, rebooting the server or turning off the power.`
	`amqmfsck -a /shared/qmdata`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`
	
	`Waiting for lock...`

Turn the power off here.	

Tabelle 10. Datenintegritätsprüfung auf zwei Servern zur gleichen Zeit ausführen (Forts.)

IBM MQ-Server 1	IBM MQ-Server 2

	`File lock acquired.`
	
	`Reading test file`
	
	`Checking the integrity of the data read.`
	
	`Appending data into the test file`
	`after data already found.`
	
	`The test file is full of data.`
	`It is ready to be inspected for data in`
	`tegrity.`

Der Zeitpunkt des Tests richtet sich nach dem Verhalten des Dateisystems. Beispielsweise dauert es in der Regel 30 bis 90 Sekunden, wenn ein Dateisystem die Dateisperren freigibt, die durch das erste Programm nach einem Stromausfall erhalten wurden. Wenn Sie zu wenig Zeit haben, um den Fehler einzuführen, bevor das erste Testprogramm die Datei gefüllt hat, verwenden Sie die Option `-x` von **amqmfsck** , um die Testdatei zu löschen. Testen Sie den Test ab dem Start mit einer größeren Testdatei.

c) Überprüfen Sie die Integrität der Daten in der Testdatei.

Auf IBM MQ-Server 2:

```
amqmfsck -i /shared/qmdata
```

Der Server antwortet mit den folgenden Nachrichten:

```
File lock acquired

Reading test file checking the integrity of the data read.

The data read was consistent.

The tests on the directory completed successfully.
```

6. Löschen Sie die Testdateien.

Auf IBM MQ-Server 2:

```
amqmfsck -x /shared/qmdata
Test files deleted.
```

Der Server antwortet mit der Nachricht:

```
Test files deleted.
```

Ergebnisse

Das Programm gibt den Exit-Code 0 zurück, wenn die Tests erfolgreich abgeschlossen wurden, und andernfalls nicht null.

Beispiele

Die erste Gruppe von drei Beispielen zeigt den Befehl, der die minimale Ausgabe erzeugt.

Erfolgreicher Test der Basisdateisperrung auf einem Server

```
> amqmfsck /shared/qmdata
The tests on the directory completed successfully.
```

Fehlgeschlagener Test der Basisdateisperrung auf einem Server

```
> amqmfsck /shared/qmdata
AMQ6245: Error Calling 'write()[2]' on file '/shared/qmdata/amqmfsck.lck' error '2'.
```

Erfolgreicher Test der Sperrung auf zwei Servern

Tabelle 11. Erfolgreiches Sperren auf zwei Servern

IBM MQ-Server 1	IBM MQ-Server 2

`> amqmfsck -w /shared/qmdata`
`Please start this program on a second`
`machine with the same parameters.`
`Lock acquired.`
`Press Return`
`or terminate the program to release the lock.`	

	`> amqmfsck -w /shared/qmdata` `Waiting for lock...`
`[ Return pressed ]` `Lock released.`	

	`Lock acquired.`
	`The tests on the directory completed successful`
	`ly`

In der zweiten Gruppe von drei Beispielen werden dieselben Befehle im ausführlichen Modus angezeigt.

Erfolgreicher Test der Basisdateisperrung auf einem Server

```
> amqmfsck -v /shared/qmdata
System call: stat("/shared/qmdata")'
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fchmod(fd, 0666)
System call: fstat(fd)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: write(fd)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: close(fd)
System call: fd1 = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd1, F_SETLK, F_RDLCK)
System call: fd2 = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd2, F_SETLK, F_RDLCK)
System call: close(fd2)
System call: write(fd1)
System call: close(fd1)
The tests on the directory completed successfully.
```

Fehlgeschlagener Test der Basisdateisperrung auf einem Server

```
> amqmfsck -v /shared/qmdata
System call: stat("/shared/qmdata")
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fchmod(fd, 0666)
```

```
System call: fstat(fd)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: write(fd)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_WRLCK)
System call: close(fd)
System call: fd = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fd, F_SETLK, F_RDLCK)
System call: fdSameFile = open("/shared/qmdata/amqmfsck.lck", O_RDWR, 0666)
System call: fcntl(fdSameFile, F_SETLK, F_RDLCK)
System call: close(fdSameFile)
System call: write(fd)
AMQxxxx: Error calling 'write()[2]' on file '/shared/qmdata/amqmfsck.lck', errno 2
(Permission denied).
```

Erfolgreicher Test der Sperrung auf zwei Servern

Tabelle 12. Erfolgreiches Sperren auf zwei Servern-Modus 'verbose'

IBM MQ-Server 1	IBM MQ-Server 2

`> amqmfsck -wv /shared/qmdata`
`Calling 'stat("/shared/qmdata")'`
`Calling 'fd = open("/shared/qmda`
`ta/amqmfsck.lkw",`
`O_EXCL | O_CREAT | O_RDWR, 0666)'`
`Calling 'fchmod(fd, 0666)'`
`Calling 'fstat(fd)'`
`Please start this program on a second`
`machine with the same parameters.`
`Calling 'fcntl(fd, F_SETLK, F_WRLCK)'`
`Lock acquired.`
`Press Return`
`or terminate the program to release the lock.`	

	`> amqmfsck -wv /shared/qmdata`
	`Calling 'stat("/shared/qmdata")'`
	`Calling 'fd = open("/shared/qmda`
	`ta/amqmfsck.lkw",`
	`O_EXCL | O_CREAT | O_RDWR,0666)'`
	`Calling 'fd = open("/shared/qmdata/amqmfsck.lkw,`
	`O_RDWR, 0666)'`
	`Calling 'fcntl(fd, F_SETLK, F_WRLCK)`
	`'Waiting for lock...`

`[ Return pressed ]`
`Calling 'close(fd)'`
`Lock released.`	

	`Calling 'fcntl(fd, F_SETLK, F_WRLCK)'`
	`Lock acquired.`
	`The tests on the directory completed successful`
	`ly`

Zugehörige Verweise

Beispielprogramme zur Hochverfügbarkeit

Multi

amqsfhac zum Testen der Nachrichtenintegrität ausführen

Führen Sie das IBM MQ MQI client -Beispielprogramm **amqsfhac** parallel zu **amqmfsck** aus, um zu demonstrieren, dass ein Warteschlangenmanager die Nachrichtenintegrität während eines Fehlers beibehält.

Vorbereitende Schritte

Für diesen Test benötigen Sie vier Server. Zwei Server für den Multi-Instanz-Warteschlangenmanager, einen für das Dateisystem und einen, um **amqsfhac** als IBM MQ MQI client-Anwendung auszuführen.

Führen Sie Schritt „1" auf Seite 129 unter „Verhalten des gemeinsam genutzten Dateisystems auf mehreren Plattformen überprüfen" auf Seite 128 aus, um das Dateisystem für einen Multi-Instanz-Warteschlangenmanager einzurichten.

Informationen zu diesem Vorgang

Das IBM MQ MQI client-Beispielprogramm **amqsfhac** überprüft, ob ein Warteschlangenmanager, der den Netzspeicher verwendet, die Datenintegrität nach einem Fehler aufrechterhält. Führen Sie **amqsfhac** parallel zu **amqmfsck** aus, um zu demonstrieren, dass ein Warteschlangenmanager die Nachrichtenintegrität während eines Fehlers aufrechterhält.

Vorgehensweise

1. Erstellen Sie einen Warteschlangenmanager mit mehreren Instanzen auf einem anderen Server, QM1, und verwenden Sie dabei das Dateisystem, das Sie in Schritt „1" auf Seite 129 in Vorgehensweiseerstellt haben.

   Siehe Multi-Instanz-WS-Manager erstellen .
2. Starten Sie den Warteschlangenmanager auf beiden Servern, die ihn hoch verfügbar machen.

   Auf Server 1:

   ```
   strmqm -x QM1
   ```

   Auf Server 2:

   ```
   strmqm -x QM1
   ```
3. Richten Sie die Clientverbindung für die Ausführung von **amqsfhac**ein.
   a) Führen Sie die Vorgehensweise im Abschnitt *IBM MQ-Installation überprüfen* für die Plattform oder Plattformen aus, die in Ihrem Unternehmen zum einrichten einer Clientverbindung verwendet wird, oder die Beispielscripts im Abschnitt Clientverbindungen konfigurieren.
   b) Ändern Sie den Clientkanal so, dass zwei IP-Adressen vorhanden sind, die den beiden Servern entsprechen, auf der QM1 ausgeführt wird.

      Ändern Sie im Beispielscript Folgendes:

      ```
      DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
      CONNAME('LOCALHOST(2345)') QMNAME(QM1) REPLACE
      ```

      In:

      ```
      DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
      CONNAME('server1(2345),server2(2345)') QMNAME(QM1) REPLACE
      ```

      Dabei sind server1 und server2 die Hostnamen der beiden Server, und 2345 ist der Port, an dem der Kanal-Listener empfangsbereit ist. Gewöhnlich ist dies der Standardwert 1414. Sie können 1414 mit der Standard-Listener-Konfiguration verwenden.
4. Erstellen Sie zwei lokale Warteschlangen unter QM1 für den Test.
   Führen Sie das folgende MQSC-Script aus:

   ```
   DEFINE QLOCAL(TARGETQ) REPLACE
   DEFINE QLOCAL(SIDEQ) REPLACE
   ```

5. Testen Sie die Konfiguration mit **amqsfhac**.

```
amqsfhac QM1 TARGETQ SIDEQ 2 2 2
```

6. Testen Sie die Nachrichtenintegrität, während Sie die Integrität des Dateisystems testen.

   Führen Sie **amqsfhac** während Schritt „5” auf Seite 129 von „Verhalten des gemeinsam genutzten Dateisystems auf mehreren Plattformen überprüfen” auf Seite 128aus.

```
amqsfhac QM1 TARGETQ SIDEQ 10 20 0
```

   Wenn Sie die aktive Warteschlangenmanagerinstanz stoppen, stellt **amqsfhac** die Verbindung zur anderen Warteschlangenmanagerinstanz wieder her, sobald sie aktiv geworden ist. Starten Sie die gestoppte WS-Manager-Instanz erneut, so dass Sie den Fehler beim nächsten Test rückgängig machen können. Sie müssen wahrscheinlich die Anzahl der Iterationen auf der Basis des Experiments mit Ihrer Umgebung erhöhen, damit das Testprogramm genügend Zeit für die Übernahme von Failover ausgeführt wird.

Ergebnisse

Nachfolgend wird ein Beispiel für die Ausführung von **amqsfhac** in Schritt „6” auf Seite 135 gezeigt. In diesem Beispiel ist der Test ein Erfolg.

```
Sample AMQSFHAC start
qmname = QM1
qname = TARGETQ
sidename = SIDEQ
transize = 10
iterations = 20
verbose = 0
Iteration 0
Iteration 1
Iteration 2
Iteration 3
Iteration 4
Iteration 5
Iteration 6
Resolving MQRC_CALL_INTERRUPTED
MQGET browse side tranid=14 pSideinfo->tranid=14
Resolving to committed
Iteration 7
Iteration 8
Iteration 9
Iteration 10
Iteration 11
Iteration 12
Iteration 13
Iteration 14
Iteration 15
Iteration 16
Iteration 17
Iteration 18
Iteration 19
Sample AMQSFHAC end
```

Wenn der Test ein Problem festgestellt hat, würde die Ausgabe den Fehler melden. In einigen Testläufen kann `MQRC_CALL_INTERRUPTED` möglicherweise " `Resolving to backed out` " melden. Es macht keinen Unterschied zum Ergebnis. Das Ergebnis hängt davon ab, ob der Schreibzugriff auf die Platte durch den Netzdateispeicher vor oder nach dem Fehlschlagen der Platte festgeschrieben wurde.

Zugehörige Verweise

amqmfsck (Dateisystemprüfung)

Beispielprogramme zur Hochverfügbarkeit

Multi IBM MQ-Dateien in Multiplatforms gemeinsam nutzen

Auf einige IBM MQ-Dateien wird ausschließlich über einen aktiven Warteschlangenmanager zugegriffen, während andere Dateien gemeinsam genutzt werden.

Bei IBM MQ-Dateien wird zwischen Programmdateien und Datendateien unterschieden. Programmdateien werden normalerweise lokal auf jedem Server installiert, auf dem IBM MQ ausgeführt wird. Warteschlangenmanager nutzen den Zugriff auf Datendateien und Verzeichnisse im Standarddatenverzeichnis gemeinsam. sie benötigen exklusiven Zugriff auf die Verzeichnisstrukturen ihres eigenen Warteschlangenamanagers, die sich jeweils in den Verzeichnissen `qmgrs` und `log`, die in Abbildung 32 auf Seite 136 dargestellt sind.

Abbildung 32 auf Seite 136 ist eine Übersicht der IBM MQ-Verzeichnisstruktur. Sie zeigt die Verzeichnisse an, die von den WS-Managern gemeinsam genutzt werden können und die ferne ausgeführt werden können Die Details variieren je nach Plattform. Die gepunkteten Linien geben konfigurierbare Pfade an.

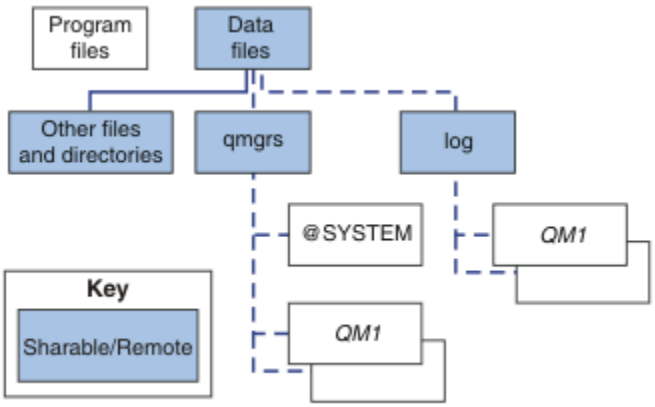


Abbildung 32. Übersicht der IBM MQ-Verzeichnisstruktur

Programm- dateien

Das Verzeichnis der Programmdateien wird in der Regel an der Standardposition belassen, ist lokal und wird von allen WS-Managern auf dem Server gemeinsam genutzt.

Daten- dateien

Das Datenverzeichnis ist in der Regel lokal in der Standardposition, `/var/mqm` auf AIX and Linux-Systemen und kann bei der Installation unter Windows konfiguriert werden. Sie wird von WS-Managern gemeinsam genutzt. Sie können eine ferne Position als Standardposition festlegen, es darf jedoch keine Position sein, die von verschiedenen IBM MQ-Installationen gemeinsam genutzt wird. Das Attribut `DefaultPrefix` in der IBM MQ-Konfiguration verweist auf diesen Pfad.

`qmgrs`

Es gibt zwei alternative Möglichkeiten, die Position der Warteschlangenmanagerdaten anzugeben:

`Prefix` verwenden

Das Attribut `Prefix` gibt die Position des `qmgrs` -Verzeichnisses an. IBM MQ erstellt für den Warteschlangenmanager im Verzeichnis `qmgrs` ein Unterverzeichnis mit dem Namen des Warteschlangenmanagers.

Das Attribut `Präfix` befindet sich in der Zeilengruppe 'QueueManager' und wird aus dem Wert im Attribut `DefaultPrefix` übernommen. Für eine einfache Verwaltung verwenden Warteschlangenmanager standardmäßig dasselbe `qmgrs`-Verzeichnis.

Die Zeilengruppe `QueueManager` befindet sich in der Datei `mqs.ini`.

Wenn Sie die Position des Verzeichnisses `qmgrs` für einen beliebigen Warteschlangenmanager ändern, müssen Sie den Wert des zugehörigen Attributs `Präfix` ändern.

Das Präfix-Attribut für das QM1-Verzeichnis in Abbildung 32 auf Seite 136 für eine AIX and Linux-Plattform ist das folgende:

```
Prefix=/var/mqm
```

DataPath verwenden

Das Attribut DataPath gibt die Position des Datenverzeichnisses des Warteschlangenmanagers an.

Das Attribut DataPath gibt den vollständigen Pfad an, einschließlich des Namens des Datenverzeichnisses des Warteschlangenmanagers. Das Attribut DataPath entspricht nicht dem Attribut Prefix , das einen unvollständigen Pfad zum Datenverzeichnis des Warteschlangenmanagers angibt.

Das Attribut DataPath befindet sich in der Zeilengruppe 'QueueManager', wenn es angegeben ist. Wenn sie angegeben wurde, hat sie Vorrang vor jedem Wert im Attribut Prefix .

Die Zeilengruppe QueueManager befindet sich in der Datei mqs.ini.

Wenn Sie die Position des Datenverzeichnisses des Warteschlangenmanagers für einen WS-Manager ändern, müssen Sie den Wert des Attributs DataPath ändern.

Das Attribut Datenpfad für das QM1-Verzeichnis in Abbildung 32 auf Seite 136 für eine AIX- oder Linux-Plattform ist

```
DataPath=/var/mqm/qmgrs/QM1
```

log

Das Protokollverzeichnis wird für jeden Warteschlangenmanager in der Zeilengruppe Log in der WS-Manager-Konfiguration separat angegeben. Die Konfiguration des WS-Managers befindet sich in qm.ini.

***DataPath*/*QmgrName*/@IPCC-Unterverzeichnisse**

Die Unterverzeichnisse von *DataPath*/*QmgrName*/@IPCC befinden sich im Pfad für gemeinsam genutzte Verzeichnisse. Sie werden verwendet, um den Verzeichnispfad für IPC-Dateisystemobjekte zu erstellen. Sie müssen den Namensbereich eines Warteschlangenmanagers unterscheiden, wenn ein Warteschlangenmanager von mehreren Systemen gemeinsam genutzt wird.

Die IPC-Dateisystemobjekte müssen vom System unterschieden werden. Für jedes System, auf dem der Warteschlangenmanager ausgeführt wird, wird dem Verzeichnispfad ein Unterverzeichnis hinzugefügt (siehe Abbildung 33 auf Seite 137).

```
DataPath/QmgrName/@IPCC/esem/myHostName/
```

Abbildung 33. Beispiel für ein IPC-Unterverzeichnis

myHostName ist bis zu den ersten 20 Zeichen des vom Betriebssystem ausgegebenen Hostnamens. Auf einigen Systemen kann der Hostname bis zu 64 Zeichen lang sein, bevor er abgeschnitten wird. Der generierte Wert von *myHostName* kann aus zwei Gründen ein Problem verursachen:

1. Die ersten 20 Zeichen sind nicht eindeutig.
2. Der Hostname wird von einem DHCP-Algorithmus generiert, der nicht immer denselben Hostnamen einem System zuordnet.

Legen Sie in diesen Fällen *myHostName* mithilfe der Umgebungsvariablen MQS_IPC_HOST fest (siehe Abbildung 34 auf Seite 138).

```
export MQS_IPC_HOST= myHostName
```

Abbildung 34. Beispiel für das Festlegen von MQS_IPC_HOST

Andere Dateien und Verzeichnisse

Andere Dateien und Verzeichnisse, wie z. B. das Verzeichnis mit den Tracedateien und das allgemeine Fehlerprotokoll, werden normalerweise gemeinsam genutzt und auf dem lokalen Dateisystem gespeichert.

Mit Unterstützung gemeinsam genutzter Dateisysteme verwaltet IBM MQ den exklusiven Zugriff auf diese Dateien mithilfe von Dateisystemsperren. Eine Dateisystemsperre erlaubt es nur einer Instanz eines bestimmten Warteschlangenmanagers, aktiv zu sein.

Wenn Sie die erste Instanz eines bestimmten Warteschlangenmanagers starten, wird das Eigentumsrecht an dem Warteschlangenmanager-Verzeichnis des Warteschlangenmanagers angezeigt. Wenn Sie eine zweite Instanz starten, kann sie nur dann das Eigentumsrecht übernehmen, wenn die erste Instanz gestoppt wurde. Wenn der erste Warteschlangenmanager noch aktiv ist, kann die zweite Instanz nicht gestartet werden, und es wird gemeldet, dass der Warteschlangenmanager an anderer Stelle ausgeführt wird. Wenn der erste Warteschlangenmanager gestoppt wurde, übernimmt der zweite Warteschlangenmanager das Eigentumsrecht an den WS-Manager-Dateien und wird zum aktiven Warteschlangenmanager.

Sie können die Prozedur des zweiten Warteschlangenmanagers, der von der ersten übernommen wird, automatisieren. Starten Sie den ersten Warteschlangenmanager mit der Option `strmqm -x` , der es einem anderen WS-Manager ermöglicht, von diesem Warteschlangenmanager zu übernehmen. Der zweite WS-Manager wartet dann, bis die WS-Manager-Dateien entsperrt sind, bevor er versucht, das Eigentumsrecht an den WS-Manager-Dateien zu übernehmen, und startet.

Linux AIX Verzeichnisstruktur auf Systemen mit AIX and Linux

Die IBM MQ-Verzeichnisstruktur auf Systemen mit AIX and Linux kann unterschiedlichen Dateisystemen zugeordnet werden, um die Verwaltung zu vereinfachen, die Leistung zu erhöhen oder die Zuverlässigkeit zu verbessern.

Nutzen Sie die flexible Verzeichnisstruktur von IBM MQ, um gemeinsam genutzte Dateisysteme für die Ausführung von Multi-Instanz-Warteschlangenmanagern zu verwenden.

Verwenden Sie den Befehl **crtmqm** *QM1* , um die in Abbildung 35 auf Seite 139 gezeigte Verzeichnisstruktur zu erstellen, wobei R das Release des Produkts ist. Dies ist eine typische Verzeichnisstruktur für einen Warteschlangenmanager, der auf einem IBM MQ -System erstellt wurde. Einige Verzeichnisse, Dateien und .ini-Attributeinstellungen werden aus Gründen der Übersichtlichkeit weggelassen, und ein anderer Name des WS-Managers kann durch das Mangeln geändert werden. Die Namen der Dateisysteme hängen von unterschiedlichen Systemen ab.

In einer Standardinstallation zeigen alle Warteschlangenmanager, die Sie erstellen, auf allgemeine `log`- und `qmgrs`-Verzeichnisse auf dem lokalen Dateisystem. In einer Konfiguration mit mehreren Instanzen befinden sich die Verzeichnisse `log` und `qmgrs` in einem Netzdateisystem, das gemeinsam mit einer anderen Installation von IBM MQ gemeinsam genutzt wird.

Abbildung 35 auf Seite 139 zeigt die Standardkonfiguration für IBM MQ V7.R unter AIX, wobei R die Releasenummer des Produkts ist. Beispiele für andere Konfigurationen mit mehreren Instanzen finden Sie unter „Beispiele für Verzeichniskonfigurationen auf Systemen mit AIX and Linux” auf Seite 144.

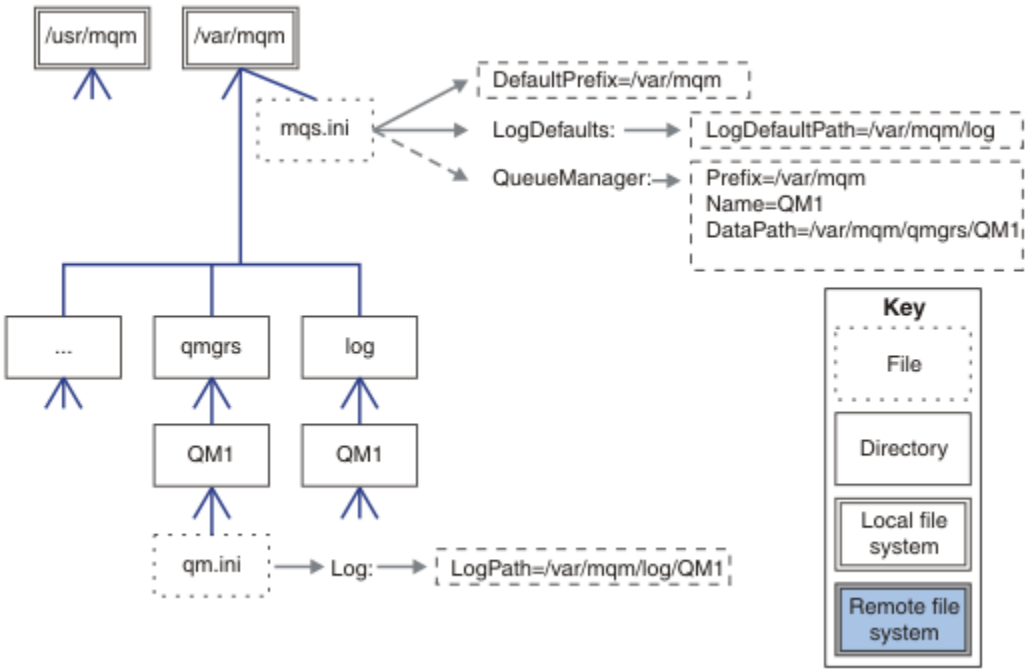


Abbildung 35. Beispiel für eine standardmäßige IBM MQ-Dateistruktur für Systeme mit AIX and Linux

Das Produkt wird standardmäßig in `/usr/mqm` unter AIX installiert, bei anderen Systemen unter `/opt/mqm`. Die Arbeitsverzeichnisse werden in das Verzeichnis `/var/mqm` installiert.

Anmerkung: Wenn Sie das `/var/mqm`-Dateisystem vor der Installation von IBM MQ erstellt haben, sollten Sie sicherstellen, dass der Benutzer 'mqm' über vollständige Verzeichnisberechtigungen verfügt, z. B. im Dateimodus '755'.

Anmerkung: Das `/var/mqm/errors`-Verzeichnis sollte ein separates Dateisystem sein, um zu verhindern, dass FFDCs, die vom Warteschlangenmanager erstellt werden, das Dateisystem füllen, das `/var/mqm` enthält.

Weitere Informationen finden Sie unter Dateisysteme auf Systemen mit AIX and Linux erstellen.

Die Verzeichnisse `log` und `qmgrs` werden an ihren Standardpositionen angezeigt, die durch die Standardwerte der Attribute `LogDefaultPath` und `Standardpräfix` in der `mqs.ini`-Datei definiert sind. Wenn ein Warteschlangenmanager erstellt wird, wird standardmäßig das Datenverzeichnis des Warteschlangenmanagers in *`DefaultPrefix`*`/qmgrs` und das Verzeichnis für die Protokolldatei in *`LogDefaultPath`*`/log` erstellt. `LogDefaultPath` und `DefaultPrefix` wirken sich nur auf die Erstellung von Warteschlangenmanagern und Protokolldateien aus. Die tatsächliche Position eines WS-Manager-Verzeichnisses wird in der Datei `mqs.ini` gespeichert, die Position des Protokolldateiverzeichnisses wird in der Datei `qm.ini` gespeichert.

Das Protokolldateiverzeichnis für einen Warteschlangenmanager ist in der Datei `qm.ini` im Attribut `Protokollpfad` definiert. Verwenden Sie die Option `-ld` im Befehl **`crtmqm`**, um das Attribut `LogPath` für einen Warteschlangenmanager festzulegen, z. B. **`crtmqm`** `-ld` *`LogPath`* `QM1`. Wenn Sie den Parameter `ld` nicht angeben, wird stattdessen der Wert von `LogDefaultPath` verwendet.

Das Datenverzeichnis des Warteschlangenmanagers wird im Attribut `Datenpfad` in der Zeilengruppe `QueueManager` in der Datei `mqs.ini` definiert. Verwenden Sie die Option `-md` im Befehl **`crtmqm`**, um `DataPath` für einen Warteschlangenmanager festzulegen, z. B. **`crtmqm`** `-md` *`DataPath`* `QM1`. Wenn Sie den Parameter `md` nicht angeben, wird stattdessen der Wert des Attributs `DefaultPrefix` oder `Prefix` verwendet. `Präfix` hat Vorrang vor `DefaultPrefix`.

In der Regel erstellen Sie QM1 , indem Sie sowohl die Protokoll-als auch die Datenverzeichnisse in einem einzigen Befehl angeben.

```
 crtmqm
-md DataPath -ld
LogPath QM1
```

Sie können die Position eines WS-Manager-Protokolls und der Datenverzeichnisse eines vorhandenen Warteschlangenmanagers ändern, indem Sie die Attribute Datenpfad und Protokollpfad in der Datei qm.ini bearbeiten, wenn der Warteschlangenmanager angehalten ist.

Der Pfad zum Verzeichnis errors ist wie die Pfade zu allen anderen Verzeichnissen in /var/mqm nicht änderbar. Die Verzeichnisse können jedoch auf verschiedenen Dateisystemen angehängt werden oder symbolisch mit verschiedenen Verzeichnissen verknüpft sein.

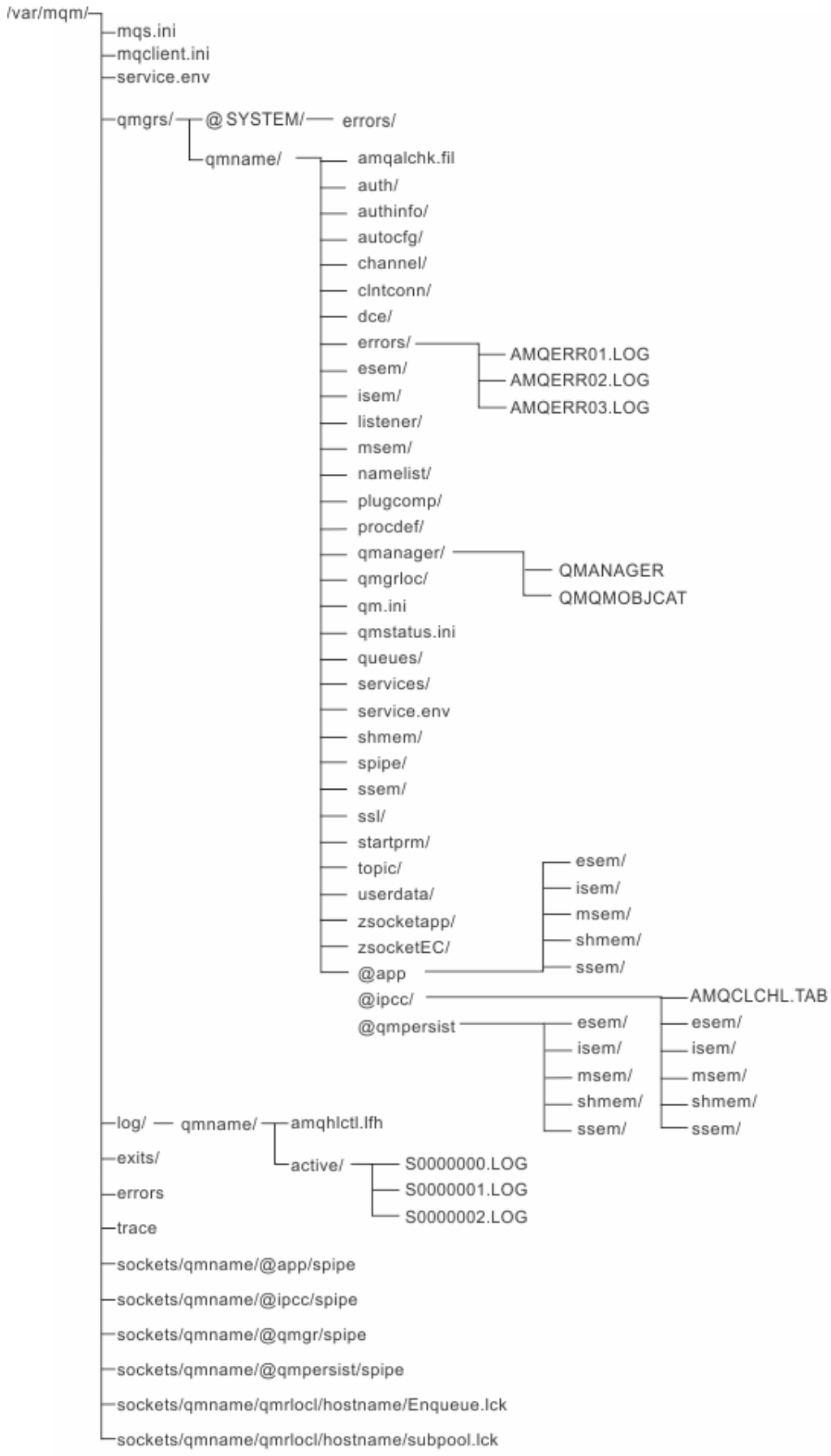
Linux AIX *Verzeichnisinhalt auf Systemen mit AIX and Linux*

Inhalt der Verzeichnisse, die einem WS-Manager zugeordnet sind.

Informationen zur Position der Produktdateien finden Sie unter Installationsposition auswählen.

Informationen zu alternativen Verzeichniskonfigurationen finden Sie unter „Unterstützung von Dateisystemen auf Multiplatforms planen” auf Seite 125.

V 9.2.0 Die folgende Verzeichnisstruktur ist repräsentativ für IBM MQ , wenn ein Warteschlangenmanager seit einiger Zeit verwendet wird. Die tatsächliche Struktur, von der Sie abhängig sind, hängt davon ab, welche Operationen auf dem Warteschlangenmanager ausgeführt wurden.


/var/mqm/
mqs.ini
mqclient.ini
service.env
qmgrs/
@SYSTEM/
errors/
qmname/
amqalchk.fil
auth/
authinfo/
autocfg/
channel/
clntconn/
dce/
errors/
AMQERR01.LOG
AMQERR02.LOG
AMQERR03.LOG
esem/
isem/
listener/
msem/
namelist/
plugcomp/
procdef/
qmanager/
QMANAGER
QMQMOBJCAT
qmgrloc/
qm.ini
qmstatus.ini
queues/
services/
service.env
shmem/
spipe/
ssem/
ssl/
startprm/
topic/
userdata/
zsocketapp/
zsocketEC/
@app
esem/
isem/
msem/
shmem/
ssem/
@ipcc/
AMQCLCHL.TAB
esem/
isem/
msem/
shmem/
ssem/
@qmpersist
esem/
isem/
msem/
shmem/
ssem/
log/
qmname/
amqhlctl.lfh
active/
S0000000.LOG
S0000001.LOG
S0000002.LOG
exits/
errors
trace
sockets/qmname/@app/spipe
sockets/qmname/@ipcc/spipe
sockets/qmname/@qmgr/spipe
sockets/qmname/@qmpersist/spipe
sockets/qmname/qmrlocl/hostname/Enqueue.lck
sockets/qmname/qmrlocl/hostname/subpool.lck

/var/mqm/

Das Verzeichnis /var/mqm enthält Konfigurationsdateien und Ausgabeverzeichnisse, die für eine IBM MQ-Installation als Ganzes gelten, und nicht für einen einzelnen Warteschlangenmanager.

Tabelle 13. Dokumentierter Inhalt des /var/mqm-Verzeichnisses unter AIX and Linux

Verzeichnis-oder Dateiname	Inhalt
mqs.ini	Für die ganze IBM MQ-Installation geltende Konfigurationsdatei, die gelesen wird, wenn ein Warteschlangenmanager gestartet wird. Der Dateipfad kann mit der Umgebungsvariablen **AMQ_MQS_INI_LOCATION** geändert werden. Stellen Sie sicher, dass dies in der Shell festgelegt und exportiert wird, in der der **strmqm** -Befehl ausgeführt wird.
mqclient.ini	Standardmäßige Clientkonfigurationsdatei, die von IBM MQ MQI client-Programmen gelesen wird. Der Dateipfad kann mit der Umgebungsvariablen **MQCLNTCF** geändert werden.
service.env	Enthält Umgebungsvariablen des Maschinenbereichs für einen Serviceprozess. Dateipfad wurde korrigiert.
Fehler/	Systemweit geltende Fehlerprotokolle und FFST-Dateien. Verzeichnispfad wurde korrigiert. Siehe auch FFST: IBM MQ for UNIX and Linux.
Sockets/	Enthält nur Informationen zu jedem Warteschlangenmanager für die Systemverwendung.
Trace/	Tracedateien. Verzeichnispfad wurde korrigiert.
web/	Verzeichnis 'mqweb server'.
exits/	Standardverzeichnis, das Benutzerkanalexitprogramme enthält. Die Position kann in ApiExit-Zeilengruppen in der Datei 'mqs.ini' geändert werden.
exits64/	

/var/mqm/qmgrs/*qmname*/

/var/mqm/qmgrs/*qmname*/ enthält Verzeichnisse und Dateien für einen Warteschlangenmanager. Das Verzeichnis ist für exklusiven Zugriff durch die aktive WS-Manager-Instanz gesperrt. Der Verzeichnispfad kann direkt in der Datei mqs.ini oder mithilfe der Option **md** des Befehls **crtmqm** geändert werden.

Tabelle 14. Dokumentierter Inhalt des /var/mqm/qmgrs/qmname-Verzeichnisses unter AIX and Linux

Verzeichnis-oder Dateiname	Inhalt
qm.ini	Warteschlangenmanagerkonfigurationsdatei, lesen, wenn ein Warteschlangenmanager gestartet wird.
Fehler/	Fehlerprotokolle des Warteschlangenmanagers. *qmname* = @system enthält kanalbezogene Nachrichten für einen unbekannten oder nicht verfügbaren WS-Manager.

Tabelle 14. Dokumentierter Inhalt des /var/mqm/qmgrs/qmname-Verzeichnisses unter AIX and Linux (Forts.)	
Verzeichnis-oder Dateiname	**Inhalt**
@ipcc/ AMQCLCHL.TAB	Standardmäßige Steuertabelle für den Clientkanal, die vom IBM MQ-Server erstellt und von IBM MQ MQI client-Programmen gelesen wird. Der Dateipfad kann mit den Umgebungsvariablen **MQCHLLIB** und **MQCHLTAB** geändert werden.
qmanager	WS-Manager-Objektdatei: QMANAGER Objektkatalog des WS-Managers: QMQMOBJCAT
authinfo/	Jedem Objekt, das im Warteschlangenmanager definiert ist, wird eine Datei in diesen Verzeichnissen zugeordnet. Der Dateiname stimmt ungefähr mit dem Definitionsnamen überein; siehe IBM MQ-Dateinamen verstehen.
Kanal/	
clntconn/	
Empfangsprogramm/	
namelist/	
procdef/	
Warteschlangen/	
Dienstleistungen/	
Themen/	
...	Andere Verzeichnisse, die von IBM MQ verwendet werden, z. B. @ipcc, und nur von IBM MQ geändert werden sollen.
V 9.2.0 **user-data/**	Kann verwendet werden, um den persistenten Status von Anwendungen zu speichern (kann vom RDQM beim Verschieben von Warteschlangenmanager an verschiedene Knoten verwendet werden - siehe Persistenten Anwendungsstatus speichern.)
V 9.2.0 ***DataPath*\autocfg**	Wird für die automatische Konfiguration verwendet

/var/mqm/log/*qmname*/

/var/mqm/log/*qmname*/ enthält die WS-Manager-Protokolldateien. Das Verzeichnis ist für exklusiven Zugriff durch die aktive WS-Manager-Instanz gesperrt. Der Verzeichnispfad kann in der Datei qm.ini oder mithilfe der Option **ld** des Befehls **crtmqm** geändert werden.

Tabelle 15. Dokumentierter Inhalt des /var/mqm/log/qmname-Verzeichnisses unter AIX and Linux	
Verzeichnis-oder Dateiname	**Inhalt**
amqhlctl.lfh	Protokollsteuerdatei.
Aktiv/	Dieses Verzeichnis enthält die Protokolldateien S0000000.LOG, S0000001.LOG, S0000002.LOG und so weiter.

/opt/mqm

/opt/mqm ist standardmäßig das Installationsverzeichnis auf den meisten Plattformen. Weitere Informationen dazu, wie viel Speicherplatz für das Installationsverzeichnis auf der Plattform oder den Plattformen benötigt wird, die Ihr Unternehmen verwendet, finden Sie unter „Erforderl. Plattenspeicherplatz auf Multiplatforms-Plattformen” auf Seite 121.

Linux AIX *Beispiele für Verzeichniskonfigurationen auf Systemen mit AIX and Linux*

Beispiele für alternative Dateisystemkonfigurationen auf Systemen mit AIX and Linux.

Sie können die Verzeichnisstruktur von IBM MQ auf verschiedene Arten anpassen, um eine Reihe von unterschiedlichen Zielsetzungen zu erreichen.

- Platzieren Sie die Verzeichnisse qmgrs und log auf gemeinsam genutzten Remote-Dateisystemen, um einen Multi-Instanz-Warteschlangenmanager zu konfigurieren.
- Verwenden Sie separate Dateisysteme für die Daten-und Protokollverzeichnisse und ordnen Sie die Verzeichnisse verschiedenen Platten zu, um die Leistung zu verbessern, indem Sie die E/A-Konkurrenzsituationen verringern.
- Verwenden Sie schnellere Speichereinheiten für Verzeichnisse, die sich stärker auf die Leistung auswirken. Die Latenzzeit der physischen Einheit ist häufig ein wichtiger Faktor bei der Leistung des persistenten Messaging, als ob eine Einheit lokal oder über Remotezugriff angehängt ist. Die folgende Liste zeigt, welche Verzeichnisse die meisten und die leistungsfähigsten Verzeichnisse sind.
  1. log
  2. qmgrs
  3. Andere Verzeichnisse, einschließlich /usr/mqm
- Erstellen Sie die Verzeichnisse qmgrs und log in Dateisystemen, die auf einem Speicher mit einer guten Ausfallsicherheit liegen, z. B. ein redundantes Plattenarray.
- Es ist besser, die allgemeinen Fehlerprotokolle in var/mqm/errors lokal und nicht in einem Netzdateisystem zu speichern, so dass der Fehler im Zusammenhang mit dem Netzdateisystem protokolliert werden kann.

Abbildung 36 auf Seite 145 ist eine Vorlage, aus der alternative IBM MQ-Verzeichnisstrukturen abgeleitet werden können. In der Schablone stellen gepunktete Linien Pfade dar, die konfiguriert werden können. In den Beispielen werden die gepunkteten Linien durch durchgezogene Linien ersetzt, die den Konfigurationsdaten entsprechen, die in der Umgebungsvariablen AMQ_MQS_INI_LOCATION und in den Dateien mqs.ini und qm.ini gespeichert sind.

Anmerkung: Die Pfadinformationen werden angezeigt, wie sie in den mqs.ini- oder qm.ini-Dateien angezeigt werden. Wenn Sie Pfadparameter im Befehl **crtmqm** angeben, lassen Sie den Namen des Warteschlangenmanagerverzeichnisses weg: Der Warteschlangenmanagername wird dem Pfad von IBM MQhinzugefügt.

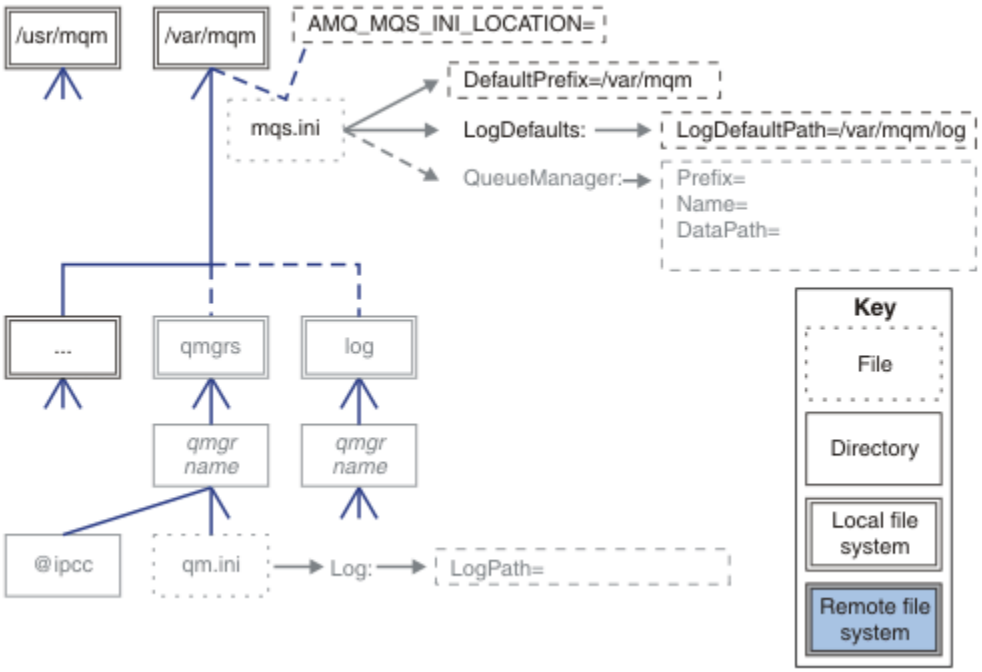


Abbildung 36. Vorlage für Verzeichnisstrukturmuster

Typische Verzeichnisstruktur für IBM MQ

Abbildung 37 auf Seite 146 zeigt die standardmäßige Verzeichnisstruktur, die in IBM MQ mit dem Befehl **crtmqm***QM1* erstellt wird.

Die Datei `mqs.ini` verfügt über eine Zeilengruppe für den QM1-Warteschlangenmanager, die unter Bezugnahme auf den Wert von `Standardpräfix` erstellt wird. Die Zeilengruppe `Protokoll` in der `qm.ini`-Datei hat einen Wert für `Protokollpfad`, der durch Verweis auf `LogDefaultPath` in `mqs.ini` festgelegt wird.

Verwenden Sie die optionalen Parameter **crtmqm** , um die Standardwerte von `DataPath` und `LogPath`zu überschreiben.

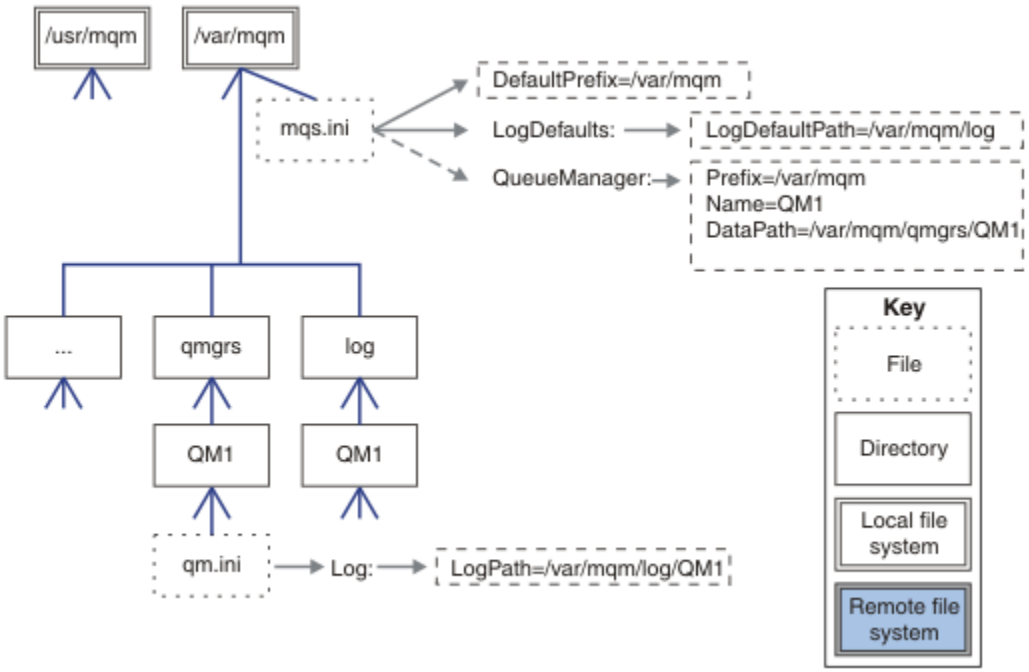


Abbildung 37. Beispiel für eine standardmäßige IBM MQ-Dateistruktur für Systeme mit AIX and Linux

Gemeinsame Nutzung der Standardverzeichnisse `qmgrs` und `log`)

Eine Alternative zu „Alles teilen” auf Seite 147ist die separate gemeinsame Nutzung der Verzeichnisse `qmgrs` und `log` (Abbildung 38 auf Seite 146). In dieser Konfiguration muss `AMQ_MQS_INI_LOCATION` nicht festgelegt werden, da die Standarddatei mqs.ini im lokalen `/var/mqm` -Dateisystem gespeichert wird. Die Dateien und Verzeichnisse, wie z. B. `mqclient.ini` und `mqserver.ini`, werden ebenfalls nicht gemeinsam genutzt.

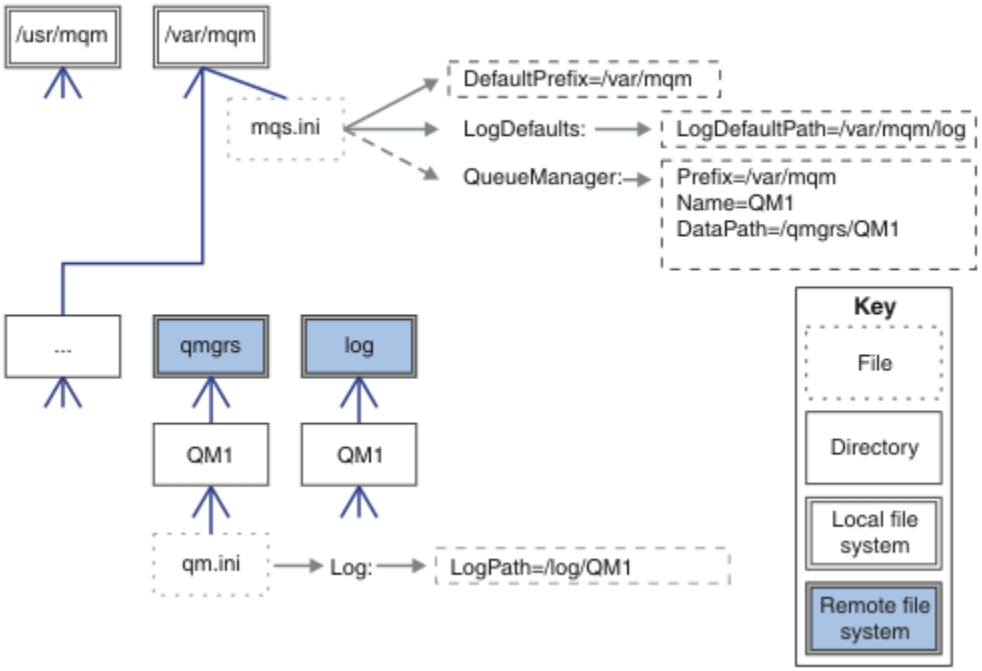


Abbildung 38. `qmgrs`- und `log`-Verzeichnisse gemeinsam nutzen

Benannte Verzeichnisse `qmgrs` und `log` gemeinsam nutzen

Bei der Konfiguration in Abbildung 39 auf Seite 147 werden `log` und `qmgrs` in einem gemeinsam genutzten Remote-Dateisystem mit dem Namen `/ha` platziert. Dieselbe physische Konfiguration kann auf zwei verschiedene Arten erstellt werden.

1. Legen Sie `LogDefaultPath=/ha` fest und führen Sie dann den Befehl **`crtmqm`** - `md` *`/ha/qmgrs`* `QM1`aus. Das Ergebnis entspricht exakt der Darstellung in Abbildung 39 auf Seite 147.
2. Lassen Sie die Standardpfade unverändert und führen Sie dann den Befehl **`crtmqm`** - `ld` *`/ha/log`* - `md` *`/ha/qmgrs`* `QM1`aus.

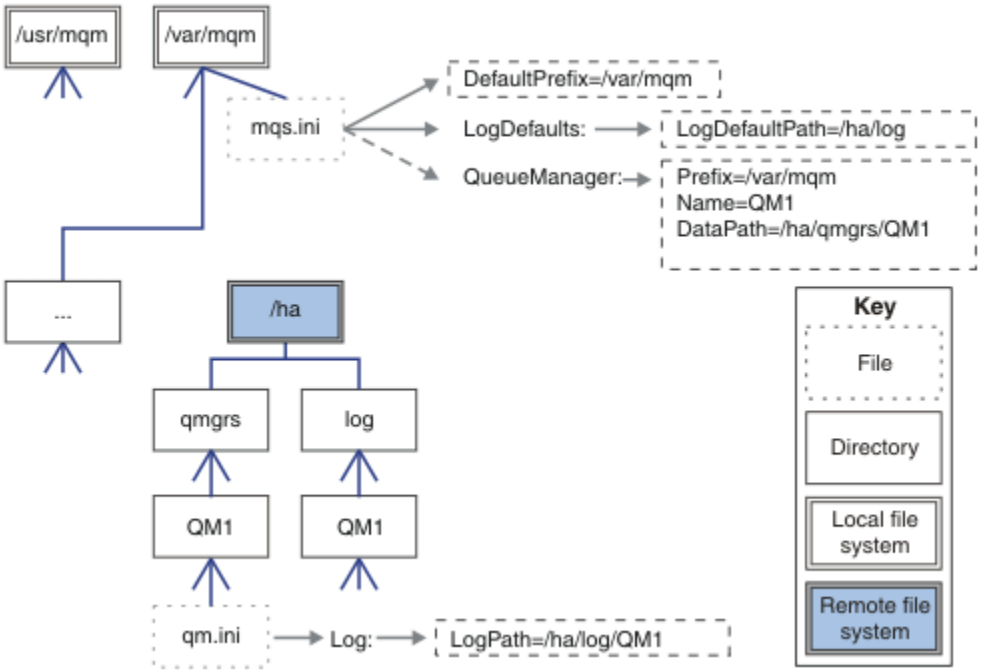


Abbildung 39. Benannte Verzeichnisse `qmgrs` und `log` gemeinsam nutzen

Alles teilen

In Abbildung 40 auf Seite 148 ist eine einfache Konfiguration für ein System mit schnellem vernetztem Dateispeicher dargestellt.

Hängen Sie `/var/mqm` als ein gemeinsam genutztes Remote-Dateisystem ein. Wenn Sie QM1 starten, sucht er standardmäßig nach `/var/mqm`, findet es auf dem gemeinsam genutzten Dateisystem und liest die `mqs.ini`-Datei in `/var/mqm`. Statt die einzige `/var/mqm/mqs.ini` -Datei für Warteschlangenmanager auf allen Ihren Servern zu verwenden, können Sie die Umgebungsvariable `AMQ_MQS_INI_LOCATION` auf jedem Server so festlegen, dass sie auf verschiedene `mqs.ini` -Dateien verweist.

Anmerkung: Der Inhalt der generischen Fehlerdatei in `/var/mqm/errors/` wird von Warteschlangenmanagern auf verschiedenen Servern gemeinsam genutzt.

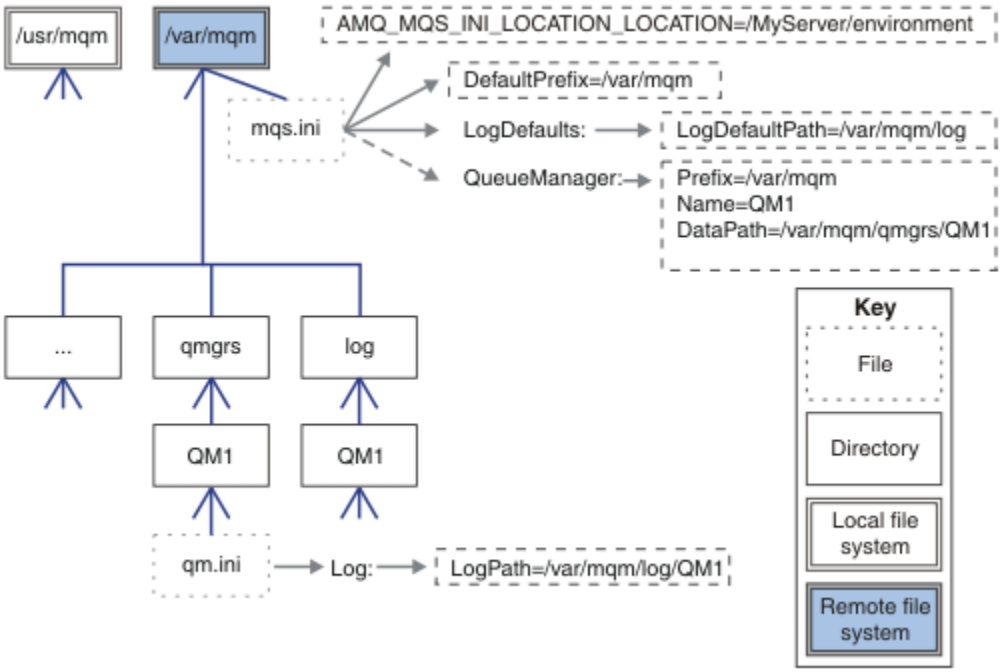


Abbildung 40. Alles teilen

Beachten Sie, dass Sie dies nicht für WS-Manager mit mehreren Instanzen verwenden können. Der Grund dafür ist, dass es für jeden Host in einem Multi-Instanz-Warteschlangenmanager erforderlich ist, über eine eigene lokale Kopie von `/var/mqm` zu verfügen, um die lokalen Daten, wie z. B. Semaphoren und gemeinsam genutzten Speicher, zu verfolgen. Diese Entitäten können nicht über Hosts hinweg gemeinsam genutzt werden.

Windows Verzeichnisstruktur auf Systemen mit Windows

Vorgehensweise zum Auffinden von Warteschlangenmanager-Konfigurationsinformationen und von Verzeichnissen unter Windows.

Folgende Standardverzeichnisse werden bei der Installation von IBM MQ for Windows erstellt:

Programmverzeichnis
`C:\Programme\IBM\MQ`

Datenverzeichnis
`C:\ProgramData\IBM\MQ`

Wichtig: Windows Für Windows-Installationen gelten die genannten Verzeichnisse, es sei denn, das Produkt wurde schon einmal installiert und die Registrierungseinträge und/oder Warteschlangenmanager dieser früheren Version sind noch vorhanden. In diesem Fall wird für die neue Installation das bereits vorhandene Datenverzeichnis verwendet. Weitere Informationen finden Sie im Abschnitt Positionen von Programm- und Datenverzeichnissen.

Wenn Sie wissen möchten, welches Installationsverzeichnis und welches Datenverzeichnis verwendet wird, führen Sie den Befehl dspmqver aus.

Das Installationsverzeichnis wird im Feld **InstPath** aufgelistet, und das Datenverzeichnis wird im Feld **DataPath** aufgelistet.

Wenn Sie den Befehl **dspmqver** ausführen, werden beispielsweise die folgenden Informationen angezeigt:

```
>dspmqver
Name:        IBM MQ
Version:     9.0.0.0
Level:       p900-L160512.4
```

```
BuildType:   IKAP - (Production)
Platform:    IBM MQ for Windows (x64 platform)
Mode:        64-bit
O/S:         Windows 7 Professional x64 Edition, Build 7601: SP1
InstName:    Installation1
InstDesc:
Primary:     Yes
InstPath:    C:\Program Files\IBM\MQ
DataPath:    C:\ProgramData\IBM\MQ
MaxCmdLevel: 900
LicenseType: Production
```

Warteschlangenmanager mit mehreren Instanzen

Zum Konfigurieren eines Warteschlangenmanagers mit mehreren Instanzen müssen die Protokoll-und Datenverzeichnisse in den Netzspeicher gestellt werden, vorzugsweise auf einem anderen Server auf einem der Server, auf denen Instanzen des Warteschlangenmanagers ausgeführt werden.

Im Befehl **crtmqm** werden zwei Parameter bereitgestellt: **-md** und **-ld**, um die Angabe der Position der Warteschlangenmanagerdaten und Protokollverzeichnisse zu vereinfachen. Die Angabe des **-md** -Parameters hat eine vierfache Auswirkung:

1. Die `mqs.ini` Zeilengruppe `QueueManager\`*QmgrName* enthält eine neue Variable *Datenpfad*, die auf das Datenverzeichnis des Warteschlangenmanagers verweist. Im Gegensatz zur Variablen *Prefix* enthält der Pfad den Namen des WS-Manager-Verzeichnisses.
2. Die Konfigurationsdaten des Warteschlangenmanagers, die in der Datei mqs.ini gespeichert sind, werden auf *Name*, *Prefix*, *Directory* und *DataPath* reduziert.

Windows *Verzeichnisinhalt*

Listet die Position und den Inhalt von IBM MQ-Verzeichnissen auf.

Zu einer IBM MQ-Konfiguration gehören drei Hauptgruppen von Dateien und Verzeichnissen:

1. Ausführbare Dateien und andere schreibgeschützte Dateien, die nur aktualisiert werden, wenn die Wartung angewendet wird. Beispiel:
   - Die Readme-Datei
   - Dateien für das IBM MQ Explorer-Plug-in und Hilfedateien
   - Lizenzdateien

   Diese Dateien werden in Tabelle 16 auf Seite 149 beschrieben.
2. Potenziell änderbare Dateien und Verzeichnisse, die für einen bestimmten WS-Manager nicht spezifisch sind. Diese Dateien und Verzeichnisse werden in Tabelle 17 auf Seite 150 beschrieben.
3. Dateien und Verzeichnisse, die für die einzelnen WS-Manager auf einem Server spezifisch sind. Diese Dateien und Verzeichnisse werden in Tabelle 18 auf Seite 151 beschrieben.

Ressourcenverzeichnisse und -dateien

Die Ressourcenverzeichnisse und -dateien enthalten den gesamten ausführbaren Code und die Ressourcen für die Ausführung eines Warteschlangenmanagers. Die Variable *FilePath* im installationsspezifischen Registrierungsschlüssel für die IBM MQ-Konfiguration enthält den Pfad zu den Ressourcenverzeichnissen.

Tabelle 16. Verzeichnisse und Dateien im Verzeichnis `FilePath`

Dateipfad	**Inhalt**
FilePath\bin	Befehle und DLLs
FilePath\bin64	Befehle und DLLs (64 Bit)
FilePath\conv	Datenkonvertierungstabellen
FilePath\doc	Hilfedateien für

Tabelle 16. Verzeichnisse und Dateien im Verzeichnis `FilePath` (Forts.)	
Dateipfad	**Inhalt**
FilePath\MQExplorer	Eclipse-Plug-ins für Explorer und Explorer
FilePath\gskit8	Globaler Sicherheitssatz
FilePath\java	Java-Ressourcen, einschließlich JRE
FilePath\licenses	Lizenzinformation
FilePath\Non_IBM_License	Lizenzinformation
FilePath\properties	Wird intern verwendet
FilePath\Tivoli	
FilePath\tools	Entwicklungsressourcen und -beispiele
FilePath\web	Beschrieben in Dateistruktur der Installationskomponente von IBM MQ Console und REST API für nicht bearbeitbare Dateien.
FilePath\Uninst	Wird intern verwendet
FilePath\README.TXT	Readme-Datei

Verzeichnisse, die nicht für einen Warteschlangenmanager spezifisch sind

Einige Verzeichnisse enthalten Dateien, wie z. B. Tracedateien und Fehlerprotokolle, die nicht spezifisch für einen bestimmten Warteschlangenmanager sind. Die Variable *DefaultPrefix* enthält den Pfad zu diesen Verzeichnissen. *Standardpräfix* ist Teil der Zeilengruppe `AllQueueManagers`.

Tabelle 17. Verzeichnisse und Dateien im Verzeichnis `DefaultPrefix`	
Dateipfad	**Inhalt**
DefaultPrefix\config	Wird intern verwendet
DefaultPrefix\conv	Konvertierungssteuerdatei für `ccsid_part2.tbl` und `ccsid.tbl data`, die in Datenkonvertierung beschrieben wird
DefaultPrefix\errors	Fehlerprotokolle des Nicht-WS-Managers, `AMQERR` *nn*`.LOG`
DefaultPrefix\exits	Kanalexitprogramme
DefaultPrefix\exits64	Kanalexitprogramme (64 Bit)
DefaultPrefix\ipc	Nicht verwendet
DefaultPrefix\qmgrs	Beschrieben in Tabelle 18 auf Seite 151
DefaultPrefix\trace	Tracedateien
DefaultPrefix\web	Beschrieben in Dateistruktur der Installationskomponente von IBM MQ Console und REST API für vom Benutzer bearbeitbare Dateien
DefaultPrefix\amqmjpse.txt	Wird intern verwendet

WS-Manager-Verzeichnisse

Wenn Sie einen WS-Manager erstellen, wird eine neue Gruppe von Verzeichnissen erstellt, die für den Warteschlangenmanager spezifisch sind.

Wenn Sie einen Warteschlangenmanager mit dem Parameter **-md** *filepath* erstellen, wird der Pfad in der Variable *DataPath* in der Zeilengruppe des Warteschlangenmanagers der Datei mqs.ini gespeichert. Wenn Sie einen Warteschlangenmanager erstellen, ohne den Parameter **-md** *filepath* festzulegen, werden die Warteschlangenmanagerverzeichnisse in dem Pfad erstellt, der in *DefaultPrefix*gespeichert ist, und der Pfad wird in die Variable *Prefix* in der Zeilengruppe des Warteschlangenmanagers in der Datei mqs.ini kopiert.

Tabelle 18. Verzeichnisse und Dateien in DataPath- und Prefix\qmgrs\QmgrName-Verzeichnissen

Dateipfad	**Inhalt**
DataPath\@ipcc	Standardposition für AMQCLCHL.TAB, die Clientverbindungstabelle.
DataPath\authinfo	Wird intern verwendet.
DataPath\channel	
DataPath\clntconn	
DataPath\errors	Fehlerprotokolle, AMQERR *nn*.LOG
DataPath\listener	Wird intern verwendet.
DataPath\namelist	
DataPath\plugcomp	
DataPath\procdef	
DataPath\qmanager	
DataPath\queues	
DataPath\services	
DataPath\ssl	
DataPath\startprm	
DataPath\topic	
DataPath\active	
DataPath\active.dat	
DataPath\amqalchk.fil	
DataPath\master	
DataPath\master.dat	
DataPath\qm.ini	WS-Manager-Konfiguration
DataPath\qmstatus.ini	Status des Warteschlangenmanagers
V 9.2.0 *DataPath*\userdata	Kann verwendet werden, um den persistenten Status von Anwendungen zu speichern.
Prefix\qmgrs*QmgrName*	Wird intern verwendet
Prefix\qmgrs\@SYSTEM	Nicht verwendet
Prefix\qmgrs\@SYSTEM\errors	
V 9.2.0 *DataPath**autocfg*	Wird für die automatische Konfiguration verwendet

IBM i Verzeichnisstruktur unter IBM i

Dieser Abschnitt enthält eine Beschreibung des integrierten Dateisystems (IFS) sowie eine Beschreibung der IFS-Verzeichnisstruktur in IBM MQ für Server, Client und Java.

Das integrierte Dateisystem (Integrated File System, IFS) als Bestandteil von IBM i unterstützt, ähnlich wie Personal Computer und Betriebssysteme wie AIX and Linux, die Datenstromeingabe/-ausgabe und Speicherverwaltung und stellt gleichzeitig eine Integrationsstruktur für alle auf dem Server gespeicherten Informationen bereit.

Bei IBM i beginnen Verzeichnisnamen mit dem Zeichen `& (ampersand)` anstelle des Zeichens `@ (at)`. Zum Beispiel: `@system` bei IBM i ist `&system`.

IFS-Stammdateisystem für einen IBM MQ-Server

Wenn Sie einen IBM MQ-Server unter IBM i installieren, werden im IFS-Stammdateisystem die folgenden Verzeichnisse erstellt.

ProdData:

Übersicht

```
QIBM
   '-- ProdData
      '-- mqm
      '-- doc
      '-- inc
      '-- lib
      '-- samp
      '-- licenses
      '-- LicenseDoc
      '-- 5724H72_V8R0M0
```

/QIBM/ProdData/mqm
Unterverzeichnisse unterhalb dieses Verzeichnisses enthalten alle Produktdaten, z. B. C + + -Klassen, Trace-Formatdateien und Lizenzdateien. Die Daten in diesem Verzeichnis werden bei jeder Installation des Produkts gelöscht und ersetzt.

/QIBM/ProdData/mqm/doc
Eine Befehlsreferenz für die CL-Befehle wird im HTML-Format bereitgestellt und hier installiert.

/QIBM/ProdData/mqm/inc
Die Headerdateien zum Kompilieren Ihrer C-oder C + + -Programme.

/QIBM/ProdData/mqm/lib
Hilfsdateien, die von MQ verwendet werden.

/QIBM/ProdData/mqm/samp
Weitere Muster.

/QIBM/ProdData/mqm/licenses
Lizenzdateien. Die beiden Dateien für jede Sprache haben die Namen LA_ *xx* und LI_ *xx* , wobei *xx* die zweistellige Sprachkennung für jede gelieferte Sprache ist.

Außerdem werden in dem folgenden Verzeichnis Lizenzvereinbarungen gespeichert:

/QIBM/ProdData/LicenseDoc/5724H72_V8R0M0
Lizenzdateien. Die Dateien tragen den Namen 5724H72_V8R0M0_ *xx* , wobei *xx* die aus 2 oder 5 Zeichen bestehende Sprachenkennung für jede bereitgestellte Sprache ist.

UserData:

Übersicht

```
QIBM
   '-- UserData
      '-- mqm
      '-- errors
      '-- trace
      '-- qmgrs
      '-- &system
      '-- qmgrname1
      '-- qmgrname2
      '-- and so on
```

/QIBM/UserData/mqm
Unterverzeichnisse unterhalb dieses Verzeichnisses enthalten alle Benutzerdaten, die sich auf Warteschlangenmanager beziehen.

Wenn Sie das Produkt installieren, wird eine Datei mqs.ini im Verzeichnis/QIBM/UserData/mqm/ erstellt (sofern sie nicht bereits von einer früheren Installation vorhanden ist).

Wenn Sie einen Warteschlangenmanager erstellen, wird eine Datei qm.ini im Verzeichnis/QIBM/UserData/mqm/qmgrs/ *QMGRNAME* /erstellt (wobei *QMGRNAME* für den Namen des Warteschlangenmanagers steht).

Die Daten in den Verzeichnissen werden beibehalten, wenn das Produkt gelöscht wird.

IFS-Stammdateisystem für einen IBM MQ MQI client

Wenn Sie einen IBM MQ MQI client for IBM i installieren, werden im IFS-Stammdateisystem die folgenden Verzeichnisse erstellt.

ProdData:

Übersicht

```
QIBM
   '-- ProdData
      '-- mqm
      '-- lib
```

/QIBM/ProdData/mqm
Unterverzeichnisse unterhalb dieses Verzeichnisses enthalten alle Produktdaten. Die Daten in diesem Verzeichnis werden gelöscht und jedes Mal ersetzt, wenn das Produkt ersetzt wird.

UserData:

Übersicht

```
QIBM
   '-- UserData
      '-- mqm
      '-- errors
      '-- trace
```

/QIBM/UserData/mqm
Unterverzeichnisse unterhalb dieses Verzeichnisses enthalten alle Benutzerdaten.

IFS-Stammdateisystem für einen IBM MQ Java

Wenn Sie IBM MQ Java unter IBM i installieren, werden im IFS-Stammdateisystem die folgenden Verzeichnisse erstellt.

ProdData:

Übersicht

```
QIBM
   '-- ProdData
      '-- mqm
      '-- java
      '--samples
      '-- bin
      '-- lib
```

/QIBM/ProdData/mqm/java
Unterverzeichnisse unterhalb dieses Verzeichnisses enthalten alle Produktdaten, einschließlich Java-Klassen. Die Daten in diesem Verzeichnis werden gelöscht und jedes Mal ersetzt, wenn das Produkt ersetzt wird.

/QIBM/ProdData/mqm/java/samples
Unterverzeichnisse unterhalb dieses Verzeichnisses enthalten alle Java-Beispielklassen und -daten.

Bibliotheken, die von Server-und Clientinstallationen erstellt

Bei der Installation des IBM MQ-Servers oder -Clients werden die folgenden Bibliotheken erstellt.

- QMQM

  Die Produktbibliothek.

- QMQMSAMP

  Die Beispielbibliothek (wenn Sie die Beispiele installieren möchten).

- QMxxxx

  Nur Server.

  Jedes Mal, wenn Sie einen Warteschlangenmanager erstellen, erstellt IBM MQ automatisch eine zugehörige Bibliothek mit einem Namen wie QMxxxx, wobei xxxx vom Namen des Warteschlangenmanagers abgeleitet ist. Diese Bibliothek enthält Objekte, die für den Warteschlangenmanager spezifisch sind, einschließlich der Journale und der zugeordneten Empfänger. Standardmäßig wird der Name dieser Bibliothek aus dem Namen des Warteschlangenmanagers abgeleitet, der mit den Zeichen QM vorangestellt ist. Für einen WS-Manager mit dem Namen TEST würde die Bibliothek beispielsweise QMTEST genannt.

  Anmerkung: Wenn Sie einen WS-Manager erstellen, können Sie den Namen seiner Bibliothek angeben, wenn Sie möchten. Beispiel:

  ```
  CRTMQM MQMNAME(TEST) MQMLIB(TESTLIB)
  ```

  Mit dem Befehl "WRKLIB" können Sie alle Bibliotheken auflisten, die von IBM MQ for IBM i erstellt wurden. Für die Bibliotheken der Warteschlangenmanager wird der Text QMGR: QMGRNAME angezeigt. Das Format des Befehls lautet wie folgt:

  ```
  WRKLIB LIB(QM*)
  ```

  Diese WS-Manager-zugeordneten Bibliotheken werden beibehalten, wenn das Produkt gelöscht wird.

Multi Dateisystemunterstützung für MFT auf Multiplatforms planen

IBM MQ Managed File Transfer MFT -Agenten können zum Übertragen von Daten an Dateien und aus Dateien in einem Dateisystem verwendet werden. Darüber hinaus können Ressourcenüberwachungen, die in einem Agenten ausgeführt werden, für die Überwachung von Dateien in einem Dateisystem konfiguriert werden.

MFT erfordert, dass diese Dateien in einem Dateisystem gespeichert werden, das Sperren unterstützt. Hierfür gibt es zwei Gründe:

- Ein Agent sperrt eine Datei, um sicherzustellen, dass sie sich nicht ändert, sobald er begonnen hat, Daten aus ihr zu lesen oder in sie zu schreiben.
- Ressourcenmonitore sperren Dateien, um sicherzustellen, dass sie von keinen anderen Prozessen verwendet werden.

Agenten und Ressourcenüberwachungen verwenden die Java-Methode **`FileChannel.tryLock()`** , um Sperren auszuführen, und das Dateisystem muss in der Lage sein, Dateien zu sperren, wenn dies mit diesem Aufruf angefordert wird.

Wichtig: Die folgenden Dateisysteme werden nicht unterstützt, da sie die technischen Anforderungen von MFTnicht erfüllen:

- GlusterFS
- NFS Version 3

Multi Kreisförmige oder lineare Protokollierung auf Multiplatforms auswählen

In IBM MQ können Sie zwischen Umlaufprotokollierung und linearer Protokollierung wählen. Die folgenden Informationen geben Ihnen einen Überblick über beide Typen.

Vorteile der Umlaufprotokollierung

Die Hauptvorteile der Umlaufprotokollierung sind, dass die Umlaufprotokollierung wie folgt lautet:

- Easier zu verwalten.

  Wenn Sie die Umlaufprotokollierung ordnungsgemäß für Ihre Workload konfiguriert haben, ist keine weitere Verwaltung erforderlich. Für die lineare Protokollierung müssen Datenträgerimages aufgezeichnet werden, und die Protokollspeicherbereiche, die nicht mehr benötigt werden, müssen archiviert oder gelöscht werden.
- Bessere Leistung

  Die Umlaufprotokollierung führt eine bessere Leistung als die lineare Protokollierung aus, da die Umlaufprotokollierung Protokollspeicherbereiche wiederverwenden kann, die bereits formatiert wurden. Während die lineare Protokollierung neue Protokollerweiterungen zuordnen und diese formatieren muss.

Weitere Informationen finden Sie im Abschnitt Protokolle verwalten .

Vorteile der linearen Protokollierung

Der Hauptvorteil der linearen Protokollierung besteht darin, dass die lineare Protokollierung einen Schutz vor mehr Fehlern bietet.

Weder die kreisförmige noch die lineare Protokollierung schützen vor einem beschädigten oder gelöschten Protokoll, oder Nachrichten oder Warteschlangen, die von Anwendungen oder vom Administrator gelöscht wurden.

Lineare Protokollierung (aber nicht kreisförmig) ermöglicht die Wiederherstellung beschädigter Objekte. Die lineare Protokollierung bietet also Schutz vor beschädigten oder gelöschten Warteschlangendateien, da diese beschädigten Warteschlangen aus einem linearen Protokoll wiederhergestellt werden können.

Sowohl kreisförmiger als auch linearer Schutz vor Stromausfall und Kommunikationsfehler wie in Wiederherstellung nach Stromausfall oder Kommunikationsfehlern beschrieben beschrieben.

Weitere Überlegungen

Ob linear oder kreisförmig gewählt wird, hängt davon ab, wie viel Redundanz Sie benötigen.

Es entstehen Kosten für die Auswahl von mehr Redundanz, d. a. der linearen Protokollierung, die durch die Leistungskosten und die Verwaltungskosten verursacht werden.

Weitere Informationen finden Sie unter Protokolltypen .

AIX gemeinsam genutzter Speicher unter AIX

Wenn bestimmte Anwendungstypen wegen einer Speicherbegrenzung unter AIX keine Verbindung herstellen können, kann dies in den meisten Fällen durch eine angepasste Einstellung der Variablen "EXTSHM=ON" behoben werden.

Bei einigen 32-Bit-Prozessen unter AIX kann eine Betriebssystembegrenzung dazu führen, dass die Prozesse keine Verbindung zu IBM MQ-Warteschlangenmanagern herstellen können. Jede Standardverbindung zu IBM MQ verwendet gemeinsam genutzten Speicher, aber im Gegensatz zu anderen UNIX-Plattformen ermöglicht AIX 32-Bit-Prozessen nur 11 gemeinsam genutzte Speichergruppen zuzuordnen.

Bei den meisten 32-Bit-Prozessen tritt dieser Grenzwert nicht auf, aber Anwendungen mit hohem Speicherbedarf können möglicherweise mit Ursachencode 2102: MQRC_RESOURCE_PROBLEM keine Verbindung zu IBM MQ herstellen. In den folgenden Anwendungstypen wird möglicherweise dieser Fehler angezeigt:

- Programme, die auf einer Java Virtual Machine mit 32-Bit-Konfiguration ausgeführt werden.
- Programme, die die großen oder sehr großen Speichermodelle verwenden
- Programme, die Verbindungen zu vielen Warteschlangenmanagern oder Datenbanken herstellen
- Programme, die an gemeinsam genutzte Speichergruppen angehängt sind

AIX bietet eine Erweiterungsfunktion an, mit der 32-Bit-Prozesse mehr gemeinsam genutzten Speicher anhängen können. Wenn Sie eine Anwendung mit dieser Funktion ausführen möchten, exportieren Sie die Umgebungsvariable EXTSHM=ON, bevor Sie Ihre Warteschlangenmanager und Ihr Programm starten. Die Funktion EXTSHM=ON verhindert in den meisten Fällen diesen Fehler, ist aber mit Programmen, die die Option SHM_SIZE der Funktion shmctl verwenden, nicht kompatibel.

IBM MQ MQI client-Anwendungen und alle 64-Bit-Prozesse sind von dieser Begrenzung nicht betroffen. Sie können unabhängig von der Einstellung der Variablen "EXTSHM" eine Verbindung zu IBM MQ-Warteschlangenmanagern herstellen.

Linux AIX IPC-Ressourcen für IBM MQ und UNIX System V

Ein WS-Manager verwendet einige IPC-Ressourcen. Verwenden Sie **`ipcs -a`** , um zu ermitteln, welche Ressourcen verwendet werden.

Diese Informationen gelten nur für IBM MQ auf Systemen mit AIX and Linux.

IBM MQ nutzt Ressourcen für Interprozesskommunikation (Interprocess Communication, IPC) von System V, also *Semaphore* und *gemeinsam genutzte Speichersegmente*, um Daten zu speichern und an Systemkomponenten zu übergeben. Diese Ressourcen werden von WS-Managerprozessen und -Anwendungen verwendet, die eine Verbindung zum Warteschlangenmanager herstellen. IBM MQ MQI clients verwenden keine IPC-Ressourcen, mit Ausnahme der IBM MQ-Tracesteuerung. Mit dem UNIX-Befehl **`ipcs -a`** können Sie vollständige Informationen zu Anzahl und Größe der aktuell auf dem System verwendeten IPC-Ressourcen abrufen.

Linux AIX Prozesspriorität von IBM MQ und UNIX

Good Practices beim Festlegen der Werte für die Prozesspriorität *nice* .

Diese Informationen gelten nur für IBM MQ auf Systemen mit AIX and Linux.

Wenn Sie einen Prozess im Hintergrund ausführen, kann diesem Prozess durch die aufrufende Shell ein höherer *nice* -Wert (und damit eine niedrigere Priorität) erteilt werden. Dies kann allgemeine Auswirkung auf die Leistung von IBM MQ haben. Wenn es in stark beanspruchten Situationen viele gebrauchsfertige Threads mit einer höheren Priorität und einigen mit einer niedrigeren Priorität gibt, können die Merkmale der Betriebssystem-Zeitplanung die Threads mit der niedrigeren Priorität der Prozessorzeit vorenthalten.

Es ist ein bewährtes Verfahren, dass unabhängig gestartete Prozesse, die Warteschlangenmanagern wie **runmqlsr**zugeordnet sind, dieselben *nice* -Werte haben wie der Warteschlangenmanager, dem sie zugeordnet sind. Stellen Sie sicher, dass die Shell diesen Hintergrundprozessen keinen höheren *nice* -Wert zuordnet. Verwenden Sie beispielsweise in 'ksh' die Einstellung "`set +o bgnice`" , um zu verhindern, dass 'ksh ' den Wert *nice* für Hintergrundprozesse erhöht. Sie können die *nice* -Werte von aktiven Prozessen überprüfen, indem Sie die Spalte *NI* einer Liste " ps -efl " prüfen.

Starten Sie außerdem IBM MQ-Anwendungsprozesse mit derselben Prioritätszahl (*nice*) wie beim Warteschlangenmanager. Wenn sie mit unterschiedlichen *nice* -Werten ausgeführt werden, blockiert ein Anwendungsthread möglicherweise einen WS-Manager-Thread, oder umgekehrt, wodurch sich die Leistung absetzt.

z/OS IBM MQ-Umgebung unter z/OS planen

Bei der Planung einer IBM MQ-Umgebung müssen Sie den Ressourcenbedarf für Datasets, Seitengruppen, Db2 und Coupling-Facilitys sowie den Bedarf an Protokollierungs- und Sicherungsfunktionen berücksichtigen. Die Informationen in diesem Thema helfen Ihnen, eine IBM MQ-Umgebung zu planen.

Bevor Sie Ihre IBM MQ-Architektur planen, müssen Sie sich mit den grundlegenden IBM MQ for z/OS-Konzepten vertraut machen. Weitere Informationen finden Sie in den Abschnitten in Konzepte von IBM MQ for z/OS.

Bei der Planung Ihres Warteschlangenmanagers müssen Sie möglicherweise mit verschiedenen Personen in Ihrem Unternehmen arbeiten. Es ist in der Regel eine gute Idee, diese Menschen frühzeitig einzubeziehen, da die Änderungskontrollverfahren sehr lange dauern können. Sie können auch die Parameter angeben, die Sie für die Konfiguration von IBM MQ for z/OS benötigen.

Sie müssen z. B. mit dem arbeiten:

- Speicheradministrator, um das übergeordnete Qualifikationsmerkmal von WS-Manager-Datensätzen zu bestimmen und genügend Speicherplatz für WS-Manager-Datensätze zuzuordnen.
- z/OS-Systemprogrammierer zum Definieren des IBM MQ-Subsystems für z/OS und APF die Autorisierung der IBM MQ for z/OS-Bibliotheken.
- Netzadministrator, um festzustellen, welcher TCP/IP-Stack und welche Ports für IBM MQ for z/OS verwendet werden sollen.
- Sicherheitsadministrator zum Festlegen des Zugriffs auf WS-Managerdatensätze, Sicherheitsprofile für IBM MQ for z/OS-Ressourcen und TLS-Zertifikate.
- Db2-Administrator für die Einrichtung von Db2-Tabellen bei der Konfiguration einer Gruppe mit gemeinsamer Warteschlange.

Zugehörige Konzepte

IBM MQ - Technische Übersicht

Zugehörige Tasks

„IBM MQ-Architektur planen” auf Seite 5

Beachten Sie bei der Planung einer IBM MQ-Umgebung die Unterstützung, die IBM MQ für Architekturen mit einzelnen oder mehreren Warteschlangenmanagern sowie für Punkt-zu-Punkt- und Publish/Subscribe-Messaging bereitstellt. Planen Sie auch den Ressourcenbedarf und die Nutzung von Protokollierungs- und Sicherheitsfunktionen.

z/OS konfigurieren

IBM MQ for z/OS verwalten

z/OS Planung des Warteschlangenmanagers

Wenn Sie einen Warteschlangenmanager einrichten, sollte Ihre Planung die Entwicklung des WS-Managers ermöglichen, damit der Warteschlangenmanager die Anforderungen Ihres Unternehmens erfüllt.

Die beste Methode zum Konfigurieren eines Warteschlangenmanagers ist in den folgenden Schritten zu finden:

1. Basiswarteschlangenmanager konfigurieren
2. Konfigurieren Sie den Kanalinitiator, der Warteschlangenmanager für die Kommunikation zwischen den WS-Managern und die Kommunikation mit der fernen Clientanwendung übernimmt.
3. Wenn Sie Nachrichten verschlüsseln und schützen möchten, konfigurieren Sie Advanced Message Security.
4. Wenn Sie die Dateiübertragung über IBM MQ verwenden möchten, konfigurieren Sie Managed File Transfer für z/OS.
5. Wenn Sie die Verwaltungs- oder Messaging-REST API oder die MQ Console verwenden möchten, um IBM MQ über einen Web-Browser zu verwalten, konfigurieren Sie den mqweb-Server.

Einige Unternehmen haben Tausende von Warteschlangenmanagern in ihrer Umgebung. Sie müssen berücksichtigen, wie Ihr IBM MQ-Netz heute ist und wie es in fünf Jahren sein wird.

Unter z/OS verarbeiten einige Warteschlangenmanager Tausende von Nachrichten pro Sekunde und protokollieren mehr als 100 MB pro Sekunde. Wenn Sie sehr hohe Volumina erwarten, müssen Sie möglicherweise mehr als einen Warteschlangenmanager verwenden.

Unter z/OS kann IBM MQ als Teil einer Gruppe mit gemeinsamer Warteschlange (QSG) ausgeführt werden, in der Nachrichten in der Coupling-Facility gespeichert werden und jeder Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange auf die Nachrichten zugreifen kann. Wenn Sie die Ausführung in einer Gruppe mit gemeinsamer Warteschlange verwenden möchten, müssen Sie überlegen, wie viele Warteschlangenmanager Sie benötigen. In der Regel gibt es für jede LPAR einen Warteschlangenmanager. Es kann auch ein Warteschlangenmanager vorhanden sein, der regelmäßig CF-Strukturen sichern soll.

Einige Änderungen an der Konfiguration sind einfach zu erledigen, z. B. die Definition einer neuen Warteschlange. Andere Änderungen sind schwieriger, wie beispielsweise das Vergrößern von Protokollen und Seitengruppen. Einige Konfigurationen können nicht geändert werden, beispielsweise der Name eines Warteschlangenmanagers oder der Name der Gruppe mit gemeinsamer Warteschlange.

Es stehen Leistungs-und Optimierungsinformationen im MP16-Leistungsunterstützungspac zur Verfügung.

Namenskonventionen

Sie müssen eine Namenskonvention für die WS-Manager-Dateigruppen haben.

Viele Unternehmen verwenden die Release-Nummer im Namen der Ladebibliotheken und so weiter. Eventuell möchten Sie ein Alias von `MQM.SCSQAUTH` nutzen, das auf die derzeit verwendete Version verweist, z. B. `MQM.V900.SCSQAUTH`. Dann müssen Sie CICS, Batch und IMS JCL nicht ändern, wenn Sie auf eine neue Version von IBM MQmigrieren.

Sie können einen symbolischen Link in z/OS UNIX System Services verwenden, um auf das Installationsverzeichnis für die aktuell verwendete Version von IBM MQ zu verweisen.

Die vom Warteschlangenmanager verwendeten Dateien (Protokolle, Seitengruppen, JCL-Bibliotheken) benötigen eine Namenskonvention, um die Erstellung von Sicherheitsprofilen zu vereinfachen, und die Zuordnung von Datensätzen zu SMS-Speicherklassen, die steuern, wo die Datensätze auf die Platte gestellt werden, und die Attribute, die sie haben.

Es ist nicht zu empfehlen, die Version von IBM MQ in den Namen von Seitengruppen oder Protokollen zu integrieren. Eines Tages können Sie eine Migration auf eine neue Version durchführen, und die Datei hat die "falschen" Namen.

Anwendungen

Sie müssen die Geschäftsanwendungen sowie die besten Methoden zum Konfigurieren von IBM MQ kennen. Wenn Anwendungen beispielsweise Logik zur Bereitstellung von Recovery und Wiederholungsfunktion haben, können nicht persistente Nachrichten gut genug sein. Wenn IBM MQ die Wiederherstellung ausführen soll, müssen Sie persistente Nachrichten verwenden und Nachrichten innerhalb eines Synchronisationspunkts einreihen und abrufen.

Sie müssen Warteschlangen von verschiedenen Geschäftstransaktionen isolieren. Wenn eine Warteschlange für eine Geschäftsanwendung voll ist, möchten Sie nicht, dass diese Auswirkungen auf andere Geschäftsanwendungen wirken. Isolieren Sie die Warteschlangen in verschiedenen Seitengruppen und Pufferpools oder Strukturen, falls möglich.

Sie müssen das Profil von Nachrichten verstehen. Für viele Anwendungen haben die Warteschlangen nur wenige Nachrichten. Andere Anwendungen können Warteschlangen während des Tages erstellt haben und über Nacht verarbeitet werden. Eine Warteschlange, die in der Regel nur wenige Nachrichten enthält, muss möglicherweise viele Stunden Nachrichten enthalten, wenn ein Problem auftritt und Nachrichten nicht verarbeitet werden. Sie müssen die CF-Strukturen und Seitengruppen so groß machen, dass die erwartete Spitzenkapazität erreicht werden kann.

Nach der Konfiguration

Nachdem Sie den WS-Manager (und die Komponenten) konfiguriert haben, müssen Sie Folgendes planen:

- Seitengruppen werden gesichert.
- Die Definitionen von Objekten werden gesichert.
- Die Sicherung von CF-Strukturen automatisieren.
- Überwachen von IBM MQ-Nachrichten und geeignete Maßnahmen bei Problemen.
- Erfassen der IBM MQ-Statistikdaten.
- Überwachen der Ressourcennutzung, wie z. B. virtueller Speicher, und Menge der protokollierten Daten pro Stunde. Mit dieser Einstellung können Sie feststellen, ob Ihre Ressourcennutzung zunimmt und Sie Maßnahmen ergreifen müssen, wie z. B. die Einrichtung eines neuen Warteschlangenmanagers.

z/OS Speicher- und Leistungsanforderung unter z/OS planen

Sie müssen realistische und erreichbare Speicher-und Leistungsziele für Ihr IBM MQ-System festlegen. Verwenden Sie dieses Thema, um die Faktoren zu verstehen, die sich auf die Speicherleistung und die Leistung auswirken.

Dieser Abschnitt enthält Informationen zu den Speicher- und Leistungsanforderungen für IBM MQ for z/OS. Es enthält die folgenden Abschnitte:

- z/OS-Leistungsoptionen für IBM MQ
- Workload-Management-Bedeutung und Geschwindigkeitsziele unter z/OS bestimmen
- „Kassettenarchivspeicher” auf Seite 160
- „System-LX-Verwendung” auf Seite 160
- „Adressraumspeicher” auf Seite 161
- „Plattenspeicher” auf Seite 165

Weitere Informationen finden Sie in „Wo Sie weitere Informationen zu Speicher-und Leistungsanforderungen finden” auf Seite 166 .

z/OS-Leistungsoptionen für IBM MQ

Mit dem Workload-Management definieren Sie Leistungsziele und ordnen jedem Ziel eine Geschäftsbedeutung zu. Sie definieren die Ziele für die Arbeit in Geschäftstermen, und das System entscheidet, wie viele Ressourcen, wie z. B. Prozessor und Speicher, an die Arbeit übergeben werden sollen, um ihr Ziel zu erreichen. Das Workload-Management steuert die Zuteilungspriorität basierend auf den Zielen, die Sie angeben. Das Workload-Management erhöht oder senkt die Priorität nach Bedarf, um das angegebene Ziel zu erreichen. Sie brauchen also nicht die genauen Prioritäten jedes Arbeitsstücks im System zu verfeinern und können sich stattdessen auf Geschäftsziele konzentrieren.

Es gibt drei Arten von Zielen:

Antwortzeit
Wie schnell die Arbeit verarbeitet werden soll

Ausführungsgeschwindigkeit
Wie schnell die Arbeit ausgeführt werden soll, wenn sie bereit ist, ohne dass die Verzögerung für Prozessor, Speicher, E/A-Zugriff und die Verzögerung der Warteschlange verzögert wird.

Diskretionär
Eine Kategorie für Arbeit mit niedriger Priorität, für die es keine Leistungsziele gibt.

Die Antwortzeitziele sind für Endbenutzeranwendungen geeignet. CICS-Benutzer können beispielsweise Workloadziele als Antwortzeitziele festlegen. Für IBM MQ-Adressräume sind Geschwindigkeitsziele besser geeignet. Eine kleine Menge der im Warteschlangenmanager geleisteten Arbeit wird zu diesem Geschwindigkeitsziel gezählt, aber diese Arbeit ist für die Leistung von entscheidender Bedeutung. Der größte Teil der Arbeit, die vom Warteschlangenmanager ausgeführt wird, zählt zu dem Leistungsziel der Endbenutzeranwendung. Der größte Teil der Arbeit, die der Adressraum des Kanalinitiators geleistet hat, zählt zu seinem eigenen Geschwindigkeitsziel. Das Empfangen und Senden von IBM MQ-Nachrichten, das der Kanalinitiator ausführt, ist normalerweise wichtig für die Leistung der Geschäftsanwendungen, die diese Nachrichten nutzen.

Workload-Management-Bedeutung und Geschwindigkeitsziele unter z/OS bestimmen

Weitere Informationen finden Sie unter „Bedeutung des z/OS-Workload-Managements bestimmen” auf Seite 160.

Kassettenarchivspeicher

V 9.2.0 Sie müssen Plattenspeicher für die Produktbibliotheken zuordnen. Die genauen Zahlen hängen von Ihrer Konfiguration ab und sollten die Ziel- und Verteilungsbibliotheken sowie die SMP/E-Bibliotheken einbeziehen.

Die von IBM MQ for z/OS genutzten Zielbibliotheken verwenden PDSE-Formate. Stellen Sie sicher, dass alle PDSE-Zielbibliotheken außerhalb eines Sysplex nicht gemeinsam genutzt werden. Weitere Informationen zu den erforderlichen Bibliotheken und ihren Größen sowie dem erforderlichen Format finden Sie im Programmverzeichnis. Download-Links für die Programmverzeichnisse finden Sie unter IBM MQ for z/OS Program Directory PDF files.

System-LX-Verwendung

Jedes definierte IBM MQ-Subsystem reserviert zum IPL-Zeitpunkt einen Systemverbindungsindex (LX) und beim Starten des Warteschlangenmanagers eine Reihe von Nicht-Systemverbindungsindizes. Der Systemverbindungsindex wird erneut verwendet, wenn der Warteschlangenmanager gestoppt und erneut gestartet wird. In ähnlicher Weise reserviert die verteilte Warteschlangensteuerung einen Nicht-Systemverbindungsindex. Im unwahrscheinlichen Fall, dass Ihr z/OS-System nicht genügend System-LXs definiert hat, müssen Sie diese reservierten System-LXs möglicherweise berücksichtigen.

Falls erforderlich, kann die Anzahl der System-LXs erhöht werden, indem der Parameter *NSYSLX* in SYS1.PARMLIB-Member IEASYSxx festgelegt wird.

z/OS *Bedeutung des z/OS-Workload-Managements bestimmen*

Vollständige Informationen zum Workload-Management und zum Definieren von Zielen über die Servicedefinition finden Sie in.Produktdokumentation zu z/OS .

In diesem Abschnitt wird beschrieben, wie Sie unter z/OS die Workload-Management-Bedeutung und die Geschwindigkeitsziele in Bezug auf andere wichtige Arbeiten in Ihrem System festlegen können. Weitere Informationen finden Sie in *z/OS MVS Planning: Workload Management* .

Der Adressraum des Warteschlangenmanagers muss mit hoher Priorität definiert werden, da er Subsystemservices bereitstellt. Der Kanalinitiator ist ein Anwendungsadressraum, der jedoch normalerweise eine hohe Priorität erhält, um sicherzustellen, dass Nachrichten, die an einen fernen Warteschlangenma-

nager gesendet werden, nicht verzögert werden. Advanced Message Security (AMS) stellt auch Subsystemdienste bereit und muss mit hoher Priorität definiert werden.

Verwenden Sie die folgenden Serviceklassen:

Die Standardserviceklasse SYSSTC

- VTAM-und TCP/IP-Adressräume
- IRLM-Adressraum (IRLMPROC)

Anmerkung: Die Adressräume für VTAM-, TCP/IP-und IRLM-Adressen müssen eine höhere Zuteilungspriorität aufweisen als alle DBMS-Adressräume, ihre zugeordneten Adressräume und die untergeordneten Adressräume. Workload-Management nicht zulassen, um die Priorität von VTAM, TCP/IP oder IRLM (oder niedriger) zu verringern, die von den anderen DBMS-Adressräumen

Ein hohes Geschwindigkeitsziel und Bedeutung von 1 für eine Serviceklasse mit einem Namen, den Sie definieren, wie z. B. PRODREGN, für Folgendes:

- IBM MQ-Warteschlangenmanager, Kanalinitiator und AMS-Adressräume
- Db2 (alle Adressräume mit Ausnahme des von Db2 eingerichteten Adressraums für gespeicherte Prozeduren)
- CICS (alle Regionstypen)
- IMS (alle Regionstypen außer Stapelnachrichtenverarbeitungsprogramme (BMPs)

Ein hohes Geschwindigkeitsziel ist gut, um zu gewährleisten, dass Startups und Neustarts so schnell wie möglich für alle diese Adressräume ausgeführt werden.

Die Geschwindigkeitsziele für CICS- und IMS-Regionen sind nur während des Starts oder Neustarts wichtig. Nachdem die Ausführung der Transaktionen begonnen hat, ignoriert das Workload-Management die Geschwindigkeitsziele für CICS oder IMS und weist Prioritäten zu, die auf den Antwortzeitzielen der Transaktionen basieren, die in den Regionen ausgeführt werden. Diese Transaktionsziele sollten die relative Priorität der Geschäftsanwendungen widerspiegeln, die sie implementieren. Sie haben in der Regel einen Wichtigkeitswert von 2. Alle Batch-Anwendungen, die IBM MQ verwenden, sollten in ähnlicher Weise Geschwindigkeitsziele und Bedeutung haben, die die relative Priorität der von ihnen verwendeten Geschäftsanwendungen widerspiegeln. Gewöhnlich sind die Bedeutung und die Geschwindigkeitsziele kleiner als die für PRODREGN.

z/OS *Adressraumspeicher*

In diesem Abschnitt finden Sie grundlegende Anleitungen zu den Adressraumanforderungen für die IBM MQ-Komponenten.

Speicheranforderungen können in die folgenden Kategorien unterteilt werden:

- Gemeinsamer Speicher
- Speicherbelegung der privaten Region des Warteschlangenmanagers
- Speicherbelegung des Kanalinitiators

In einem 64-Bit-Adressraum gibt es eine virtuelle Leitung mit dem Namen " der Balken " , die die 2-GB-Adresse markiert. Der Balken trennt den Speicher unterhalb der 2-GB-Adresse, genannt " unter der Leiste ", aus dem Speicher oberhalb der 2-GB-Adresse, die " oberhalb der Leiste " aufgerufen wird. Der Speicher unterhalb des Balkens verwendet 31-Bit-Adressierbarkeit, oberhalb des Balkens wird die 64-Bit-Adressierbarkeit verwendet.

Sie können den Grenzwert von 31-Bit-Speicher angeben, indem Sie den Parameter REGION in der JCL verwenden, und den Grenzwert oberhalb des Barspeichers mit dem Parameter MEMLIMIT verwenden. Diese angegebenen Werte können von MVS-Exits überschrieben werden.

Achtung: Es wurde eine Änderung der Funktionsweise des Systems vorgenommen. Jetzt ordnet Cross-System Extended Services (XES) für jede Verbindung 4GB Speicher in einem hohen virtuellen Speicher einer serialisierten Listenstruktur zu.

Vor dieser Änderung wurde dieser Speicher in Datenbereichen zugeordnet. Nach der Anwendung dieses APAR, basierend auf der Art und Weise, wie IBM MQ die Speichernutzung berechnet, werden möglicherweise die Nachrichten CSQY225E und CSQY224I ausgegeben, die aussagen, dass der `Warteschlangenmanager zu wenig lokalen Speicher über der Leiste.` hat.

In der Nachricht CSQY220I wird auch auf eine Erhöhung des Grenzwerts für "Speicher über der Linie" hingewiesen.

Weitere Informationen finden Sie im IBM Unterstützungsdokument 2017139 .

Empfohlene Regionsgrößen

In der folgenden Tabelle sind die vorgeschlagenen Werte für die Regionsgrößen aufgeführt.

Tabelle 19. Empfohlene Definitionen für JCL-Regionsgrößen

Definitionseinstellung	**System**
Warteschlangenmanager	REGION=0M, MEMLIMIT=3G
Kanalinitiator	REGION=0M

Gemeinsamer Speicher

Jedes Subsystem mit IBM MQ for z/OS hat ungefähr folgenden Speicherbedarf:

- CSA 4 KB
- ECSA 800KB plus die Größe der Ablaufverfolgungstabelle, die im Parameter TRACTBL des Systemparametermakros CSQ6SYSP angegeben ist. Weitere Informationen hierzu finden Sie im Abschnitt CSQ6SYSP verwenden .

Zusätzlich sind für jede gleichzeitig stattfindende logische IBM MQ-Verbindung etwa 5 KB ECSA erforderlich. Sobald eine Task beendet wird, kann dieser Speicher von anderen IBM MQ-Tasks wiederverwendet werden. IBM MQ gibt den Speicher erst beim Herunterfahren des Warteschlangenmanagers frei, d. h., Sie können den maximal erforderlichen ECSA-Speicher berechnen, indem Sie die maximale Anzahl gleichzeitiger logischer Verbindungen mit 5 KB multiplizieren. Die Anzahl der gleichzeitig ablaufenden logischen Verbindungen ist die Summe aus der Anzahl der:

- Tasks (TCBs) in Regionen für Stapelbetrieb, TSO, z/OS UNIX System Services, IMS und Db2-SPAS (Adressräume für gespeicherte Prozeduren), die mit IBM MQ verbunden sind und noch nicht nicht getrennt wurden.
- CICS-Transaktionen, die eine IBM MQ-Anforderung ausgegeben haben, aber noch nicht beendet wurden.
- JMS-Verbindungen, -Sitzungen, -TopicSessions oder -QueueSessions, die erstellt wurden (für Bindungsverbindungen), aber noch nicht gelöscht oder als fehlerhafte Daten erfasst wurden.
- Aktive IBM MQ-Kanäle.

Sie können einen Grenzwert für den gemeinsamen Speicher festlegen, der von logischen Verbindungen zum Warteschlangenmanager verwendet wird, mit dem Konfigurationsparameter ACELIM. Das Steuerelement ACELIM ist hauptsächlich für Sites interessant, in denen gespeicherte Db2-Prozeduren Operationen in IBM MQ-Warteschlangen auslösen.

Bei der Ausführung über eine gespeicherte Prozedur kann jede IBM MQ -Operation zu einer neuen logischen Verbindung zum Warteschlangenmanager führen. Umfangreiche Db2-Arbeitseinheiten, die beispielsweise auf das Laden von Tabellen zurückzuführen sind, können einen sehr hohen Bedarf an gemeinsamem Speicher zur Folge haben.

ACELIM soll die allgemeine Speicherverwendung begrenzen und das z/OS-System schützen, indem die Anzahl der Verbindungen im System begrenzt wird. Es sollte nur auf Warteschlangenmanagern gesetzt

werden, die unter Verwendung überhöhter ECSA-Speichermengen identifiziert wurden. Weitere Informationen finden Sie im Abschnitt ACELIM unter Using CSQ6SYSP .

Um einen Wert für ACELIM festzulegen, legen Sie zuerst die Menge an Speicher fest, die sich momentan im Subpool, der durch den Wert ACELIM gesteuert wird, zu ermitteln. Diese Informationen werden in den SMF 115-Sätzen des Subtyps 5, die von statistics CLASS (3) erstellt wurden, angezeigt.

IBM MQ SMF-Daten können mit SupportPac MP1B formatiert werden. Die Anzahl der Byte, die in dem von ACELIM gesteuerten Subpool verwendet werden, wird in der STGPOOL-DD in der Zeile mit dem Titel *ACE/PEB* angezeigt.

Weitere Informationen zu SMF 115-Statistikeinträgen finden Sie unter Interpretieren von IBM MQ-Leistungsstatistiken.

Erhöhen Sie den Normalwert um eine ausreichende Marge, um Platz für Wachstum und Workloadspitzen zu schaffen. Dividieren Sie den neuen Wert durch 1024, um eine maximale Speichergröße in KB für die Verwendung in der ACELIM-Konfiguration zu erzielen.

Der Kanalinitiator erfordert in der Regel eine ECSA-Belegung von bis zu 160 KB.

Speichernutzung des privaten Warteschlangenmanagers

IBM MQ for z/OS kann Speicher über der 2-GB-Linie für einige interne Steuerblöcke verwenden. In diesem Speicher können Pufferpools vorhanden sein, die Ihnen die Möglichkeit bieten, viel größere Pufferpools zu konfigurieren, wenn genügend Speicher verfügbar ist. In der Regel sind Pufferpools die wichtigsten internen Steuerblöcke, die Speicher oberhalb der 2-GB-Leiste verwenden.

Jede Pufferpoolgröße wird bei der Initialisierung des Warteschlangenmanagers bestimmt, und Speicher wird für den Pufferpool zugeordnet, wenn eine Seitengruppe, die diesen Pufferpool verwendet, verbunden ist. Es wird ein neuer Parameter LOCATION (ABOVE | BELOW) verwendet, um anzugeben, wo die Puffer zugeordnet werden. Sie können den Befehl ALTER BUFFPOOL verwenden, um die Größe von Pufferpools dynamisch zu ändern.

Zur Verwendung oberhalb des Barspeichers (64 Bit) können Sie einen Wert für den Parameter MEMLIMIT (z. B. MEMLIMIT=3G) im Parameter **EXEC PGM=CSQYASCP** in der JCL des Warteschlangenmanagers angeben. Für Ihre Installation ist möglicherweise ein Standardwertsatz festgelegt.

Geben Sie MEMLIMIT an und geben Sie statt MEMLIMIT = NOLIMIT eine sinnvolle Speichergröße an, um mögliche Probleme zu vermeiden. Wenn Sie "NOLIMIT" oder einen sehr großen Wert angeben, kann der Befehl "ALTER BUFFPOOL" bei umfangreichem Verarbeitungsaufwand den gesamten für z/OS verfügbaren, virtuellen Speicher belegen, was zu Auslagerungen in Ihrem System führt. Möglicherweise müssen Sie den Wert von MEMLIMIT mit dem z/OS -Systemprogrammierer besprechen, falls es einen systemweiten Grenzwert für die Menge des verwendbaren Speichers gibt.

Beginnen Sie mit einem MEMLIMIT = 3G und erhöhen Sie diese Größe, wenn Sie die Größe der Pufferpools erhöhen müssen.

Berechnen Sie den Wert von MEMLIMIT als 2 GB plus die Größe der Pufferpools oberhalb der Leiste, die auf die nächstgelegenen GB aufgerundet werden. Setzen Sie MEMLIMIT auf mindestens 3 GB, und erhöhen Sie diesen Wert bei Bedarf, wenn Sie die Größe der Pufferpools erhöhen müssen.

Beispiel: Für 2 Pufferpools, die mit LOCATION ABOVE konfiguriert sind, Pufferpool 1 hat 10.000 Puffer, Pufferpool 2 hat 50.000 Puffer. Die Speicherbelegung oberhalb der Leiste entspricht 60.000 (Gesamtzahl Puffer) * 4096 = 245.760.000 Byte = 234.375MB. Alle Pufferpools unabhängig von der LOCATION-Funktion verwenden 64-Bit-Speicher für Steuerstrukturen. Da die Anzahl der Pufferpools und die Anzahl der Puffer in diesen Pools zunehmen, kann dies zu einer signifikanten Zunahme führen. Jeder Puffer benötigt ca. 200 Byte (64-Bit-Speicher). Für eine Konfiguration mit 10 Pufferpools mit jeweils 20.000 Puffern, die benötigt werden: 200 * 10 * 20.000 = 40,000.000 Entsprechung von 40 MB. Sie können 3 GB für die MEMLIMIT-Größe angeben, die den Umfang für das Wachstum zulässt (40 MB + 200 MB + 2 GB, die bis zu 3 GB runden).

Bei einigen Konfigurationen kann es erhebliche Leistungsvorteile für die Verwendung von Pufferpools geben, deren Puffer permanent durch Realspeicher gesichert werden. Sie können dies erreichen, indem

Sie den Wert FIXED4KB für das Attribut PAGECLAS des Pufferpools angeben. Sie sollten dies jedoch nur tun, wenn auf der LPAR genügend Realspeicher zur Verfügung steht, da andernfalls andere Adressräume betroffen sein könnten. Informationen dazu, wann Sie den Wert FIXED4KB für PAGECLAS verwenden sollten, finden Sie im IBM MQ Support Pac MP16: IBM MQ for z/OS -Capacity planning & tuning .

Bevor Sie Speicher oberhalb der Leiste verwenden, sollten Sie mit Ihrem z/OS-Systemprogrammierer diskutieren, um sicherzustellen, dass genügend Zusatzspeicher für die maximale Zeitnutzung und ausreichende Realspeicheranforderungen vorhanden sind, um das Paging zu verhindern.

Anmerkung: Die Größe von Speicherauszugsdatensätzen muss möglicherweise erhöht werden, um den erhöhten virtuellen Speicher zu verarbeiten.

Wenn die Pufferpools so groß werden, dass ein MVS -Paging vorhanden ist, kann sich die Leistung negativ auswirken. Sie können die Verwendung eines kleineren Pufferpools in Betracht ziehen, der keine Auslagerungen ausführt, wobei IBM MQ die Nachricht in die und aus der Seitengruppe verschiebt.

Sie können die Speicherbelegung des Adressraums aus der Nachricht CSQY220I überwachen, die die Größe des privaten Regionsspeichers in der Verwendung oberhalb und unterhalb des 2-GB-Balkens angibt, und die verbleibende Menge.

Speicherbelegung durch Kanalinitiator

Es gibt zwei Bereiche für die Speicherbelegung des Kanalinitiators, die Sie in Betracht ziehen müssen:

- Private Region
- Rechnungslegung und Statistik

Speicherbelegung der privaten Region

Sie sollten REGION=0M für CHINIT angeben, damit der Wert unterhalb des Balkenspeichers maximal verwendet werden kann. Der für den Kanalinitiator verfügbare Speicher begrenzt die Anzahl der gleichzeitig ablaufenden Verbindungen, die CHINIT haben kann.

Jeder Kanal verwendet ca. 170 KB erweiterter privater Bereich im Adressraum des Kanalinitiators. Wenn Nachrichten mit einer Größe von mehr als 32 KB übertragen werden, wird der Speicher um die Nachrichtengröße erhöht. Dieser erhöhte Speicher wird freigegeben, wenn:

- Ein Sende-oder Clientkanal benötigt weniger als die Hälfte der aktuellen Puffergröße für 10 aufeinanderfolgende Nachrichten.
- Ein Überwachungssignal wird gesendet oder empfangen.

Der Speicher wird zwar innerhalb der Language Environment zur Wiederverwendung freigegeben, wird jedoch dem z/OS-Speichermanager für virtuellen Speicher nicht als freigegeben angezeigt. Dies bedeutet, dass die Obergrenze für die Anzahl der Kanäle von der Nachrichtengröße und den Eingangsmustern sowie von Einschränkungen einzelner Benutzersysteme in der Größe der erweiterten privaten Region abhängt. Die Obergrenze für die Anzahl der Kanäle dürfte auf vielen Systemen ungefähr 9000 betragen, da die Größe der erweiterten Region wahrscheinlich nicht größer als 1,6 GB ist. Die Verwendung von Nachrichtengrößen, die größer als 32 KB sind, reduziert die maximale Anzahl an Kanälen im System. Wenn z. B. Nachrichten mit einer Länge von 100 MB übertragen werden und eine erweiterte Regionsgröße von 1,6GB angenommen wird, beträgt die maximale Anzahl an Kanälen 15.

Der Kanalinitiatortrace wird in einen Datenraum geschrieben. Die Größe des Datenspeicherbereichs wird durch den Parameter **TRAXTBL** gesteuert. Siehe ALTER QMGR .

Speicherbelegung für Abrechnung und Statistik

Sie sollten den Kanalinitiatorzugriff auf mindestens 256 MB virtuellen Speicher oberhalb des Balkens zulassen. Dies kann durch die Angabe von `MEMLIMIT=256M` erreicht werden.

Wenn Sie den Parameter MEMLIMIT nicht in der Kanalinitiator-JCL setzen, können Sie die Größe des virtuellen Speichers oberhalb des Balkens mit dem Parameter MEMLIMIT im Member von `SMFPRMxx` von SYS1.PARMLIB oder über den Exit IEFUSI festlegen.

Wenn Sie MEMLIMIT so konfigurieren, dass der Speicher über der Linie auf einen Wert unter der erforderlichen Größe beschränkt wird, gibt der Kanalinitiator die Nachricht CSQX124E aus und der Abrechnungs- und Statistiktrace der Klasse 4 wird nicht verfügbar sein.

MEMLIMIT-und REGION-Größe verwalten

Andere Mechanismen, beispielsweise der Parameter **MEMLIMIT** im Member SMFPRMxx von SYS1.PARMLIB oder der Exit IEFUSI, können in Ihrer Installation verwendet werden, um eine Standardmenge an virtuellem Speicher oberhalb der Grenze für z/OS -Adressräume bereitzustellen. In Speicherverwaltung über der Leiste finden Sie ausführliche Informationen zum Begrenzen von Speicher über der Leiste.

Puffer für Shared Message Data Set (SMDS) und MEMLIMIT

Bei der Ausführung von Messaging-Workloads mit gemeinsam genutzten Nachrichtendateien gibt es zwei Optimierungsstufen, die durch Anpassung der Attribute DSBUFS und DSBLOCK erreicht werden.

Der von dem SMDS-Puffer belegte Speicher des Warteschlangenmanagers über 2 GB ist DSBUFS x DSBLOCK. Dies bedeutet, dass standardmäßig 100 x 256KB (25MB) für jede CFLEVEL (5) -Struktur im Warteschlangenmanager verwendet wird.

Obwohl dieser Wert nicht zu hoch ist, können einige von ihnen, wenn Ihr Unternehmen oder Unternehmen über viele CFSTRUCTs verfügen, einen hohen Wert für MEMLIMIT für Pufferpools zuordnen, und manchmal verfügen sie über tief indexierte Warteschlangen, sodass ihnen insgesamt nicht mehr genügend Speicher oberhalb der Grenze zur Verfügung steht.

z/OS *Plattenspeicher*

Verwenden Sie dieses Thema bei der Planung des Plattenspeicherbedarfs für Protokolldatengruppen, Db2-Speicher, Coupling-Facility-Speicher und Seitendatensätze.

Arbeiten Sie mit Ihrem Speicheradministrator, um festzustellen, wo die WS-Manager-Dateien gestellt werden sollen. Der Speicheradministrator kann Ihnen beispielsweise bestimmte DASD-Datenträger oder SMS-Speicherklassen, Datenklassen und Verwaltungsklassen für die verschiedenen Datensatztypen erteilen.

- Die Protokolldatengruppen müssen sich auf DASD befinden. Diese Protokolle können eine hohe E/A-Aktivität mit einer kleinen Antwortzeit haben und müssen nicht gesichert werden.
- Archivprotokolle können sich auf DASD oder Band befinden. Nachdem sie erstellt wurden, werden sie möglicherweise nie wieder gelesen, außer in einer abnormalen Situation, z. B. bei der Wiederherstellung einer Seitengruppe aus einer Sicherung. Sie sollten über ein langes Haltbarkeitsdatum verfügen.
- Seitengruppen können eine geringe bis mittlere Aktivität aufweisen und sollten regelmäßig gesichert werden. Bei einem hohen Nutzungssystem sollten sie zwei Mal am Tag gesichert werden.
- BSDS-Dateien sollten täglich gesichert werden; sie weisen keine hohe E/A-Aktivität auf.

Alle Datensätze sind denen ähnlich, die von Db2 verwendet werden, und es können ähnliche Wartungsprozeduren für IBM MQ verwendet werden.

In den folgenden Abschnitten finden Sie ausführliche Informationen zur Planung des Datenspeichers:

- **Protokolle und Archivierungsspeicher**

  In „Wie lange muss ich Archivierungsprotokolle aufbewahren?" auf Seite 184 wird beschrieben, wie Sie feststellen können, wie viel Speicher Ihr aktives Protokoll und Ihre Archivdatasets benötigen. Dies hängt davon ab, wie groß das von Ihrem IBM MQ-System verarbeitete Nachrichtenvolumen ist und wie häufig aktive Protokolle in die Archivdatasets ausgelagert werden.
- **Db2-Speicher**

  In „Db2-Speicher" auf Seite 204 wird beschrieben, wie Sie feststellen können, wie viel Speicher Db2 für die IBM MQ-Daten benötigt.
- **Coupling-Facility-Speicher**

In „Coupling-Facility-Ressourcen definieren” auf Seite 193 wird beschrieben, wie Sie feststellen können, wie groß Ihre Coupling-Facility-Strukturen sein müssen.

- **Seitengruppe und Nachrichtenspeicher**

  In „Seitengruppen und Pufferpools planen” auf Seite 166 wird beschrieben, wie Sie feststellen können, wie viel Speicher Ihre Datasets benötigen. Dies hängt von der Größe und Anzahl der Nachrichten ab, die Ihre Anwendungen austauschen, sowie von der Häufigkeit, mit der die Nachrichten erstellt und ausgetauscht werden.

z/OS *Wo Sie weitere Informationen zu Speicher-und Leistungsanforderungen finden*

Verwenden Sie dieses Thema als Referenz, um weitere Informationen zu Speicher-und Leistungsanforderungen zu erhalten.

Sie finden weitere Informationen aus den folgenden Quellen:

Tabelle 20. Wo Sie weitere Informationen zu Speicherbedarf finden

Thema	**Quelle**
Systemparameter	CSQ6SYSP verwenden und WS-Manager anpassen
Erforderlicher Speicher für die Installation von IBM MQ	Programmverzeichnis. Download-Links für die Programmverzeichnisse finden Sie unter IBM MQ for z/OS Program Directory PDF files.
IEALIMIT und IEFUSI beendet	*MVS-Installationsexits*, verfügbar auf der zSeries-Website: z/OS -Internetbibliothek.
Neueste Informationen	Website für IBM MQ-SupportPacs: SupportPacs für IBM MQ und andere Projektbereiche.
Workload-Management und Definition von Zielen durch die Servicedefinition	*z/OSMVS-Planung: Workload-Management*

z/OS Seitengruppen und Pufferpools planen

Informationen, die Ihnen bei der Planung der Anfangsnummer und der Größe Ihrer Seitendatensätze und Pufferpools helfen.

Dieses Thema enthält die folgenden Abschnitte:

- „Seitengruppen planen” auf Seite 167
  - Verwendung der Seitengruppen
  - Anzahl der Seitengruppen
  - Größe der Seitengruppen
  - V 9.2.0 Planung der Dataset-Verschlüsselung von z/OS
- „Berechnen Sie die Größe Ihrer Seitengruppen” auf Seite 168
  - Seitengruppe 0 (null)
  - Seitengruppe 01 - 99
  - Speicherbedarf für Nachrichten berechnen
- „Dynamische Seitenerweiterung aktivieren” auf Seite 170
- „Pufferpools definieren” auf Seite 171

Seitengruppen planen

Seitengruppe verwenden

Bei kurzlebigen Nachrichten werden normalerweise nur wenige Seiten auf der Seitengruppe verwendet und es gibt nur wenig oder keine E/A für die Dateien, außer beim Systemstart, während eines Prüfpunkts oder beim Herunterfahren.

Bei langlebigen Nachrichten werden die Seiten, die Nachrichten enthalten, normalerweise auf Platte geschrieben. Diese Operation wird vom WS-Manager ausgeführt, um die Zeit für den Neustart zu reduzieren.

Trennen Sie die kurzlebigen Nachrichten von langlebigen Nachrichten, indem Sie sie auf verschiedene Seitengruppen und in verschiedene Pufferpools stellen.

Anzahl der Seitengruppen

Die Verwendung einiger weniger großer Seitengruppen kann die Aufgabe des IBM MQ-Administrators erleichtern, weil in diesem Fall weniger Seitengruppen benötigt werden und die Zuordnung zwischen Warteschlangen und Seitengruppen vereinfacht wird.

Die Verwendung mehrerer kleinerer Seitengruppen hat eine Reihe von Vorteilen. Sie nehmen beispielsweise weniger Zeit zum Sichern ein, und die Ein-/Ausgabe kann während der Sicherung parallel ausgeführt und erneut gestartet werden. Dabei muss jedoch bedacht werden, dass dies eine erhebliche Leistungsminderung für die Rolle des IBM MQ-Administrators bedeutet, weil er jede Warteschlange einer viel größeren Anzahl von Seitengruppen zuordnen muss.

Definieren Sie mindestens fünf Seitengruppen wie folgt:

- Eine Seitengruppe, die für Objektdefinitionen reserviert ist (Seitengruppe Null)
- Eine Seitengruppe für systembezogene Nachrichten
- Eine Seitengruppe für leistungskritische, langlebige Nachrichten
- Eine Seitengruppe für leistungskritische kurzlebige Nachrichten
- Eine Seitengruppe für alle anderen Nachrichten

Im Abschnitt „Pufferpools definieren” auf Seite 171 werden die Leistungsvorteile erläutert, die durch eine solche Verteilung der Nachrichten auf Seitengruppen erreicht werden.

Größe der Seitengruppen

Definieren Sie in Ihren Seitengruppen ausreichend Speicherplatz für die erwartete Spitzennachrichtenkapazität. Berücksichtigen Sie bei einer unerwarteten Spitzenkapazität, z. B. wenn sich eine aufgelaufene Nachricht entwickelt, weil ein Warteschlangenserverprogramm nicht aktiv ist. Sie können dies tun, indem Sie die Seitengruppe mit sekundären Speicherbereichen zuordnen oder alternativ die dynamische Seitengruppenerweiterung aktivieren. Weitere Informationen finden Sie unter „Dynamische Seitenerweiterung aktivieren” auf Seite 170. Es ist schwierig, eine Seitengruppe kleiner zu machen, so dass es oft besser ist, eine kleinere Seitengruppe zuzuordnen und sie bei Bedarf zu erweitern.

Wenn Sie die Größe der Seitengruppe planen, sollten Sie alle Nachrichten berücksichtigen, die möglicherweise generiert werden, einschließlich der Nachrichtendaten der Nichtanwendungsnachricht. Auslösenachrichten, Ereignisnachrichten und alle Berichtsnachrichten, die von Ihrer Anwendung angefordert wurden, werden z. B. ausgelöst.

Die Größe der Seitengruppe bestimmt die Zeit, die zum Wiederherstellen einer Seitengruppe bei der Wiederherstellung aus einer Sicherung benötigt wird, da eine große Seitengruppe länger dauert, bis sie zurückgeschrieben wird.

Anmerkung: Die Wiederherstellung einer Seitengruppe hängt auch von der Zeit ab, die der Warteschlangenmanager benötigt, um die Protokollsätze zu verarbeiten, die seit der Sicherung geschrieben wurden. Dieser Zeitraum wird durch die Sicherungsfrequenz bestimmt. Weitere Informationen finden Sie unter „Planung von Backups und Wiederherstellung” auf Seite 206.

Anmerkung: Seitengruppen, die größer als 4 GB sind, erfordern die Verwendung der erweiterten SMS-Adressierbarkeit.

V 9.2.0 Planung der Dataset-Verschlüsselung von z/OS

Die Dataset-Verschlüsselung von z/OS kann auf Seitengruppen für Warteschlangenmanager unter IBM MQ for z/OS 9.1.4 oder höher ausgeführt werden.

Diesen Seitengruppen müssen EXTENDED-Attribute sowie ein Dataset-Schlüsselkennsatz zugeordnet werden, der sicherstellt, dass die Daten AES-verschlüsselt sind.

Weitere Informationen finden Sie im Abschnitt zur Vertraulichkeit für ruhende Daten in IBM MQ for z/OS mit der Dataset-Verschlüsselung. weitere Informationen hierzu.

Berechnen Sie die Größe Ihrer Seitengruppen

Für WS-Manager-Objektdefinitionen (z. B. Warteschlangen und Prozesse) ist es einfach, den Speicherbedarf zu berechnen, da diese Objekte eine feste Größe haben und permanent sind. Für Nachrichten ist die Berechnung jedoch aus den folgenden Gründen komplexer:

- Nachrichten variieren in der Größe.
- Nachrichten sind transitorische Nachrichten.
- Der Speicherbereich, der von Nachrichten belegt wird, die abgerufen wurden, wird in regelmäßigen Abständen durch einen asynchronen Prozess wiederhergestellt.

Große Seitengruppen mit mehr als 4 GB, die zusätzliche Kapazität für Nachrichten bereitstellen, wenn das Netz gestoppt wird, kann bei Bedarf erstellt werden. Es ist nicht möglich, die vorhandenen Seitengruppen zu ändern. Stattdessen müssen neue Seitengruppen mit erweiterter Adressierbarkeit und erweiterten Formatattributen erstellt werden. Die neuen Seitengruppen müssen die gleiche physische Größe haben wie die alten, und die alten Seitengruppen müssen dann in die neuen Seitengruppen kopiert werden. Wenn eine Rückwärtsmigration erforderlich ist, darf die Seitengruppe Null nicht geändert werden. Wenn Seitengruppen mit weniger als 4 GB ausreichend sind, ist keine Aktion erforderlich.

Seitengruppe Null

Seitengruppe Null ist für Objektdefinitionen reserviert.

Für die Seitengruppe Null ist der erforderliche Speicher:

```
   (maximum number of local queue definitions x 1010)
      (excluding shared queues)
+  (maximum number of model queue definitions x 746)
+  (maximum number of alias queue definitions x 338)
+  (maximum number of remote queue definitions x 434)
+  (maximum number of permanent dynamic queue definitions x 1010)
+  (maximum number of process definitions x 674)
+  (maximum number of namelist definitions x 12320)
+  (maximum number of message channel definitions x 2026)
+  (maximum number of client-connection channel definitions x 5170)
+  (maximum number of server-connection channel definitions x 2026)
+  (maximum number of storage class definitions x 266)
+  (maximum number of authentication information definitions x 1010)
+  (maximum number of administrative topic definitions x 15000)
+  (total length of topic strings defined in administrative topic definitions)
```

Dividieren Sie diesen Wert durch 4096, um die Anzahl der Datensätze zu ermitteln, die im Cluster für die Seitengruppe angegeben werden sollen.

Sie müssen keine Objekte zulassen, die im gemeinsam genutzten Repository gespeichert sind. Sie müssen jedoch Objekte zulassen, die gespeichert oder in die Seitengruppe null (Objekte mit der Disposition GROUP oder QMGR) kopiert werden.

Die Gesamtzahl der Objekte, die Sie erstellen können, wird durch die Kapazität der Seitengruppe null begrenzt. Die Anzahl der lokalen Warteschlangen, die Sie definieren können, ist auf 524 287 begrenzt.

Seitengruppen 01-99

Bei Seitengruppen 01-99 wird der für jede Seitengruppe erforderliche Speicher durch die Anzahl und Größe der auf dieser Seitengruppe gespeicherten Nachrichten bestimmt. (Nachrichten in gemeinsam genutzten Warteschlangen werden nicht auf Seitengruppen gespeichert.)

Dividieren Sie diesen Wert durch 4096, um die Anzahl der Datensätze zu ermitteln, die im Cluster für die Seitengruppe angegeben werden sollen.

Speicherbedarf für Nachrichten berechnen

In diesem Abschnitt wird beschrieben, wie Nachrichten auf Seiten gespeichert werden. Wenn Sie diese Informationen verstehen, können Sie berechnen, wie viel Seitensatzes Sie für Ihre Nachrichten definieren müssen. Um den ungefähren Platzbedarf für alle Nachrichten in einer Seitengruppe zu berechnen, müssen Sie die maximale Warteschlangenlänge aller Warteschlangen berücksichtigen, die der Seitengruppe zugeordnet sind, und die durchschnittliche Größe der Nachrichten in diesen Warteschlangen.

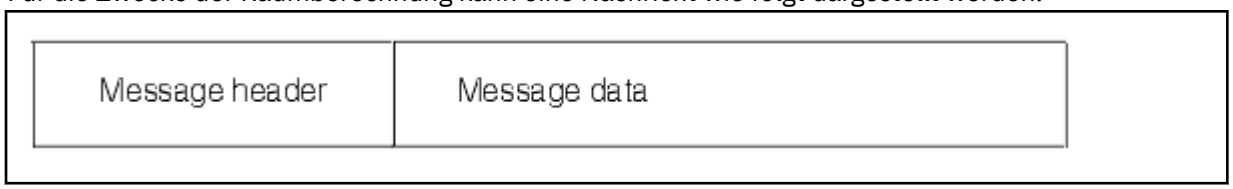
Anmerkung: Die Größe der in diesem Abschnitt enthaltenen Strukturen und Steuerinformationen kann sich zwischen den wichtigsten Releases ändern. Ausführliche Informationen zu Ihrem jeweiligen Release von IBM MQ finden Sie in den SupportPacs MP16 - WebSphere MQ for z/OS -Kapazitätsplanung und -optimierung und IBM MQ -Produktfamilie-Leistungsberichte.

Sie müssen Vorsorge dafür treffen, dass sich der Nachrichtenabruf möglicherweise verzögert, und zwar aus Gründen, die außerhalb der Kontrolle von IBM MQ liegen (z. B. bei einem Problem mit dem Kommunikationsprotokoll). In diesem Fall könnte die "put" -Rate der Nachrichten die "get" -Rate weit überschreiten. Dies kann zu einer starken Zunahme der Anzahl von Nachrichten führen, die in den Seitengruppen gespeichert sind, und einer daraus resultierenden Erhöhung der geforderten Speichergröße.

Jede Seite in der Seitengruppe ist 4096 Byte lang. Jede Seite verfügt über 4057 Byte an Speicherplatz, die für das Speichern von Nachrichten zur Verfügung stehen.

Bei der Berechnung des für die einzelnen Nachrichten erforderlichen Speicherbereichs müssen Sie zuerst prüfen, ob die Nachricht auf eine Seite (eine kurze Nachricht) passt oder ob sie auf zwei oder mehr Seiten aufgeteilt werden muss (eine lange Nachricht). Wenn Nachrichten auf diese Weise geteilt werden, müssen Sie zusätzliche Steuerinformationen in Ihren Speicherplatzberechnungen zulassen.

Für die Zwecke der Raumberechnung kann eine Nachricht wie folgt dargestellt werden:



Der Nachrichtenheaderabschnitt enthält den Nachrichtendeskriptor und andere Steuerinformationen, deren Größe in Abhängigkeit von der Größe der Nachricht variiert. Der Nachrichtendaten-Abschnitt enthält alle eigentlichen Nachrichtendaten und alle anderen Header (z. B. den Header "Transmission" oder den Header "IMS Bridge").

Für die Seitengruppe werden mindestens zwei Seiten benötigt, die in der Regel weniger als 1% des Gesamtspeicherplatzes für Nachrichten enthalten.

Kurznachrichten

Eine Kurznachricht wird als eine Nachricht definiert, die auf eine Seite passt.

Ab IBM WebSphere MQ 7.0.1 wird jede kurze Nachricht einzeln auf einer Seite gespeichert.

Lange Nachrichten

Wenn die Größe der Nachrichtendaten größer als 3596 Byte ist, jedoch nicht größer als 4 MB ist, wird die Nachricht als lange Nachricht klassifiziert. IBM MQ speichert eine solche lange Nachricht auf einer Reihe von Seiten, und auch die Steuerinformationen, die auf diese Seiten verweisen,

werden in gleicher Weise wie für kurze Nachrichten gespeichert. Dies ist in Abbildung 41 auf Seite 170 dargestellt:

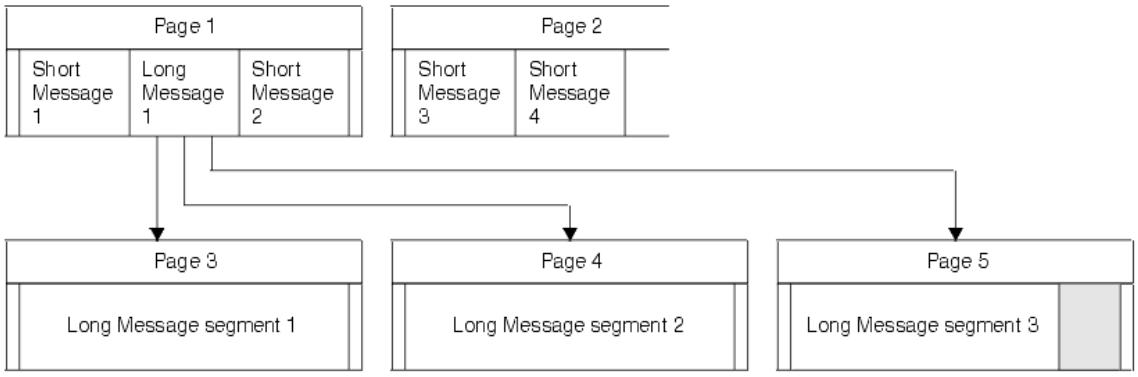


Abbildung 41. Wie IBM MQ lange Nachrichten auf Seitengruppen speichert

Sehr lange Nachrichten

Sehr lange Nachrichten sind Nachrichten mit einer Größe von mehr als 4 MB. Diese werden so gespeichert, dass jede 4 MB 1037 Seiten verwendet. Der Rest wird wie oben beschrieben auf die gleiche Weise gespeichert wie eine lange Nachricht.

z/OS *Dynamische Seitenerweiterung aktivieren*

Seitengruppen können dynamisch erweitert werden, während der WS-Manager ausgeführt wird. Eine Seitengruppe kann 123 Speicherbereiche umfassen und auf mehrere Plattendatenträger verteilt sein.

Jedes Mal, wenn eine Seitengruppe erweitert wird, wird eine neue Dateigruppe verwendet. Der Warteschlangenmanager erweitert weiterhin eine Seitengruppe, wenn dies erforderlich ist, bis die maximale Anzahl Speicherbereiche erreicht ist, oder bis kein Speicher mehr für die Zuordnung auf auswählbaren Datenträgern verfügbar ist.

Wenn die Seitenerweiterung aus einem der oben genannten Gründe fehlschlägt, markiert der WS-Manager die Seitengruppe für keine weiteren Erweiterungsversuche. Diese Markierung kann durch Ändern der Seitengruppe auf EXPAND (SYSTEM) zurückgesetzt werden.

Die Seitenerweiterung erfolgt asynchron zu allen anderen Seitensetaktivitäten, wenn 90% des vorhandenen Speicherbereichs in der Seitengruppe zugeordnet werden.

Der Erweiterungsprozess der Seitengruppe formatiert die neu zugeordnete Ausdehnung und stellt sie für die Verwendung durch den Warteschlangenmanager zur Verfügung. Es ist jedoch kein Speicherbereich für die Verwendung verfügbar, bis der gesamte Speicherbereich formatiert wurde. Dies bedeutet, dass die Erweiterung wahrscheinlich einige Zeit in Anspruch nehmen wird, und Anwendungen könnten 'blockieren', wenn sie die verbleibenden 10% der Seitengruppe füllen, bevor die Erweiterung abgeschlossen ist.

Das Beispiel thlqual.SCSQPROC (CSQ4PAGE) zeigt, wie die sekundären Speicherbereiche definiert werden.

Um die Größe neuer Speicherbereiche zu steuern, verwenden Sie eine der folgenden Optionen des Schlüsselworts EXPAND der Befehle DEFINE PSID und ALTER PSID:

- BENUTZER
- SYSTEM
- KEINE

BENUTZER

Verwendet die Größe des sekundären Extents, die bei der Zuordnung der Seitengruppe angegeben wurde. Wenn kein Wert angegeben wurde oder wenn der Wert null angegeben wurde, kann die dynamische Seitengruppe nicht erweitert werden.

Die Erweiterung der Seitengruppe tritt auf, wenn der Speicherbereich auf der Seite zu 90% verwendet wird und asynchron mit anderen Seitensetaktivitäten ausgeführt wird.

Dies kann zu einer Erweiterung um mehr als einen einzigen Speicherbereich zu einer Zeit führen.

Betrachten Sie das folgende Beispiel: Sie ordnen eine Seitengruppe mit einem Primärumfang von 100.000 Seiten und einem sekundären Umfang von 5000 Seiten zu. Es wird eine Nachricht ausgegeben, die 9999 Seiten erfordert. Wenn die Seitengruppe bereits 85.000 Seiten verwendet, überschreitet das Schreiben der Nachricht die 90% umfassende Grenze (90.000 Seiten). An dieser Stelle wird dem primären Speicherbereich von 100.000 Seiten ein weiterer sekundärer Speicherbereich zugeordnet, wobei die Seitenseitengröße auf 105.000 Seiten festgelegt wird. Die verbleibenden 4999 Seiten der Nachricht werden weiterhin geschrieben. Wenn der verwendete Seitenbereich 94.500 Seiten erreicht, was 90% der aktualisierten Seitengruppe von 105.000 Seiten entspricht, wird eine weitere 5000-Seiten-Ausdehnung zugeordnet, wobei die Seitenseitengröße auf 110.000 Seiten festgelegt wird. Am Ende des MQPUT-Befehls wurde die Seitengruppe zwei Mal erweitert, und es werden 94.500 Seiten verwendet. Keines der Seiten in der zweiten Seitenerweiterung wurde verwendet, obwohl sie zugeordnet wurden.

Wenn beim Neustart eine zuvor genutzte Seitengruppe durch einen kleineren Datenbestand ersetzt wird, wird dieser erweitert, bis er die Größe des zuvor verwendeten Datenbestands erreicht. Diese Größe erhält man bereits durch einen einzigen Speicherbereich.

SYSTEM

Ignoriert die Größe des sekundären Extents, die bei der Definition der Seitengruppe angegeben wurde. Stattdessen legt der Warteschlangenmanager einen Wert fest, der etwa 10% der aktuellen Seitengruppen-Größe entspricht. Der Wert wird auf den nächstgelegenen Zylinder der DASD-Einheit aufgerundet.

Wenn kein Wert angegeben wurde oder wenn ein Wert von null angegeben wurde, kann die dynamische Seitenerweiterung trotzdem auftreten. Der Warteschlangenmanager legt einen Wert fest, der etwa 10% der aktuellen Seitengruppen-Größe entspricht. Der neue Wert wird in Abhängigkeit von den Merkmalen der DASD-Einheit aufgerundet.

Die Erweiterung der Seitengruppe tritt auf, wenn der Speicherbereich in der Seitengruppe ungefähr 90% verwendet wird und asynchron mit anderen Seitensatzes ausgeführt wird.

Wenn beim Neustart eine zuvor genutzte Seitengruppe durch einen kleineren Datenbestand ersetzt wird, wird dieser erweitert, bis er die Größe des zuvor verwendeten Datenbestands erreicht.

KEINE

Es findet keine Seitengruppenerweiterung statt.

Zugehörige Verweise

ALTER PSID
DEFINE PSID
ANZEIGEN SYNTA

Pufferpools definieren

Verwenden Sie dieses Thema, um die Anzahl der Pufferpools zu planen, die Sie definieren sollten, und die zugehörigen Einstellungen.

Dieses Thema ist in die folgenden Abschnitte unterteilt:

Geben Sie die Anzahl der Pufferpools an, die definiert werden sollen.

Sie sollten zunächst vier Pufferpools definieren:

Pufferpool 0
Verwenden Sie für Objektdefinitionen (in Seitengruppe null) und leistungskritische, systembezogene Nachrichtenwarteschlangen, wie z. B. die Warteschlange SYSTEM.CHANNEL.SYNCQ und die Warteschlangen SYSTEM.CLUSTER.COMMAND.QUEUE und SYSTEM.CLUSTER.REPOSITORY.QUEUE.

Es ist jedoch wichtig, Punkt „7" auf Seite 174 in *Merkmale des Pufferpools anpassen* zu berücksichtigen, wenn eine große Anzahl von Kanälen oder Clustering verwendet werden soll.

Verwenden Sie die verbleibenden drei Pufferpools für Benutzernachrichten.

Pufferpool 1
Verwenden Sie für wichtige langlebige Nachrichten.

Langlebige Nachrichten sind die Nachrichten, die länger als zwei Prüfpunkte im System verbleiben, zu dem Zeitpunkt, zu dem sie auf die Seitengruppe geschrieben werden. Wenn Sie viele langlebige Nachrichten haben, sollte dieser Pufferpool relativ klein sein, sodass die Seitengruppe E/A gleichmäßig verteilt ist (ältere Nachrichten werden jedes Mal, wenn der Pufferpool zu 85% voll ist, in die DASD-Einheit geschrieben).

Wenn der Pufferpool zu groß ist und der Pufferpool nie 85% voll ist, wird die Seitengruppe E/A verzögert, bis die Prüfpunktverarbeitung ausgeführt wird. Dies kann sich auf die Antwortzeiten im gesamten System auswirken.

Wenn nur wenige langlebige Nachrichten erwartet werden, definieren Sie diesen Pufferpool so, dass er ausreichend groß ist, um alle diese Nachrichten zu speichern.

Pufferpool 2
Verwenden Sie für leistungskritische, kurzlebige Nachrichten.

Es gibt normalerweise einen hohen Grad an Pufferwiederverwendung, wobei nur wenige Puffer verwendet werden. Sie sollten diesen Pufferpool jedoch groß machen, um eine unerwartete Nachrichtenakkumulation zu ermöglichen, z. B., wenn eine Serveranwendung fehlschlägt.

Pufferpool 3
Verwenden Sie für alle anderen (normalerweise leistungsunkritischen) Nachrichten.

Warteschlangen wie die Warteschlange für nicht zustellbare Nachrichten, SYSTEM.COMMAND.* Warteschlangen und SYSTEM.ADMIN.* Warteschlangen können auch Pufferpool 3 zugeordnet werden.

Wenn die Bedingungen für virtuellen Speicher vorhanden sind und Pufferpools kleiner sein müssen, ist der Pufferpool 3 der erste Kandidat für die Verkleinerung der Größe.

Möglicherweise müssen Sie unter den folgenden Umständen zusätzliche Pufferpools definieren:

- Wenn eine bestimmte Warteschlange bekannt ist, dass sie isoliert werden muss, vielleicht weil sie zu verschiedenen Zeiten ein anderes Verhalten aufweist.
  - Eine solche Warteschlange kann unter den unterschiedlichen Umständen entweder die bestmögliche Leistung erfordern oder isoliert werden, damit sie die anderen Warteschlangen in einem Pufferpool nicht beeinträchtigt.
  - Jede solche Warteschlange kann in einen eigenen Pufferpool und eine eigene Seitengruppe eingegrenzt werden.
- Sie möchten verschiedene Gruppen von Warteschlangen aus Serviceklassengründen voneinander trennen.
  - Jede Gruppe von Warteschlangen kann dann entweder eine oder beide Typen von Pufferpools 1 oder 2 erfordern, wie in Vorgeschlagene Definitionen für Pufferpooleinstellungen beschrieben, die die Erstellung mehrerer Pufferpools eines bestimmten Typs erforderlich machen.

Legen Sie die Einstellungen für die einzelnen Pufferpools fest.

Wenn Sie die vier Pufferpools verwenden, die in „Geben Sie die Anzahl der Pufferpools an, die definiert werden sollen." auf Seite 171beschrieben sind, gibt Vorgeschlagene Definitionen für Pufferpooleinstellungen zwei Gruppen von Werten für die Größe der Pufferpools aus.

Der erste Satz eignet sich für ein Testsystem, das andere für ein Produktionssystem oder ein System, das schließlich zu einem Produktionssystem werden wird. Definieren Sie Ihre Pufferpools in allen Fällen mit dem Attribut **LOCATION**(*OBERHALB*)

Tabelle 21. Empfohlene Definitionen für Pufferpooleinstellungen

Definitionseinstellung	**Testsystem**	**Produktionssystem**
BUFFPOOL 0	1 050 Puffer	50 000 Puffer
BUFFPOOL 1	1 050 Puffer	20 000 Puffer
BUFFPOOL 2	1 050 Puffer	50 000 Puffer
BUFFPOOL 3	1 050 Puffer	20 000 Puffer

Wenn Sie mehr als die vier vorgeschlagenen Pufferpools benötigen, wählen Sie den Pufferpool (1 oder 2) aus, der das erwartete Verhalten der Warteschlangen im Pufferpool am genauesten beschreibt, und Größe des Pufferpools mit Hilfe der Informationen in Empfohlene Definitionen für Pufferpooleinstellungen .

Stellen Sie sicher, dass der Parameter MEMLIMIT hoch genug eingestellt ist, sodass alle Pufferpools oberhalb des Balkens angeordnet werden können.

Überwachen der Leistung von Pufferpools unter erwarteter Auslastung

Sie können die Verwendung von Pufferpools überwachen, indem Sie die Leistungsstatistik des Pufferpools analysieren. Insbesondere sollten Sie sicherstellen, dass die Pufferpools so groß sind, dass die Werte von QPSTSOS, QPSTSTLA und QPSTDMC auf Null bleiben.

Weitere Informationen finden Sie im Abschnitt Puffermanager-Datensätze .

Pufferpoolmerkmale anpassen

Passen Sie bei Bedarf die unter „Legen Sie die Einstellungen für die einzelnen Pufferpools fest.” auf Seite 172 genannten Pufferpooleinstellungen anhand der folgenden Punkte an.

Verwenden Sie die unter „Überwachen der Leistung von Pufferpools unter erwarteter Auslastung” auf Seite 173 angegebene Leistungsstatistik als Anleitung.

1. Wenn Sie eine Migration von einer früheren IBM MQ-Version durchführen, ändern Sie Ihre vorhandenen Einstellungen nur dann, wenn Sie nach der Migration mehr Realspeicher zur Verfügung haben.
2. Im Allgemeinen sind größere Pufferpools für die Leistung besser, und Pufferpools können viel größer sein, wenn sie über der Leiste stehen.

   Es sollte jedoch immer genügend Realspeicher verfügbar sein, damit die Pufferpools im Realspeicher resident sind. Es ist besser, kleinere Pufferpools zu haben, die nicht zu Paging führen, als die großen, die dies tun.

   Darüber hinaus gibt es keinen Punkt mit einem Pufferpool, der größer ist als die Gesamtgröße der Seitengruppen, die ihn verwenden, obwohl Sie die Erweiterung der Seitengruppe berücksichtigen sollten, wenn sie wahrscheinlich auftritt.
3. Ziel ist eine Seitengruppe pro Pufferpool, da dies eine bessere Anwendungsisolation ermöglicht.
4. Wenn genügend Realspeicher vorhanden ist, so dass Ihre Pufferpools nicht vom Betriebssystem ausgelagert werden, sollten Sie die Verwendung von seitenfesten Puffern in Ihrem Pufferpool in Betracht ziehen.

   Dies ist besonders wichtig, wenn der Pufferpool wahrscheinlich sehr viel E/A-Operationen durchläuft, da er die CPU-Kosten, die mit der Seitenfixierung der Puffer verbunden sind, vor der Ein-/Ausgabe spart und sie anschließend wieder abstellt.
5. Es gibt mehrere Vorteile, Pufferpools oberhalb der Leiste zu lokalisieren, auch wenn sie klein genug sind, um sie unter die Leiste zu passen. Diese sind:

- 31-Bit-Reliefentlastung für virtuellen Speicher-z. B. mehr Speicherbereich für gemeinsamen Speicher.
- Wenn die Größe eines Pufferpools unerwartet erhöht werden muss, während er stark genutzt wird, gibt es weniger Auswirkungen und Risiken für den Warteschlangenmanager und seine Auslastung, indem er mehr Puffer zu einem Pufferpool hinzufügt, der sich bereits oberhalb des Balkens befindet, als den Pufferpool oberhalb des Balkens zu verschieben und dann weitere Puffer hinzufügt.

6. Optimieren Sie den Pufferpool null und den Pufferpool für kurzlebige Nachrichten (Pufferpool 2), so dass die 15% freie Schwelle nie überschritten wird (d. h. QPSTCBSL dividiert durch QPSTNBUF ist immer größer als 15%). Wenn mehr als 15% der Puffer frei bleiben, können die Ein-/Ausgabe für die Seitengruppen, die diese Pufferpools verwenden, während des normalen Betriebs weitgehend vermieden werden, obwohl Nachrichten, die älter als zwei Prüfpunkte sind, in Seitengruppen geschrieben werden.

   Achtung: Der optimale Wert für diese Parameter hängt von den Merkmalen des jeweiligen Systems ab. Die angegebenen Werte sind nur als Richtlinie gedacht und sind möglicherweise für Ihr System nicht geeignet.
7. SYSTEM.* Warteschlangen, die sehr tief sind, z. B. SYSTEM.CHANNEL.SYNCQ, können davon profitieren, dass sie in ihren eigenen Pufferpool gestellt werden, wenn ausreichend Speicher verfügbar ist.

Weitere Informationen zur Optimierung von Pufferpools finden Sie im IBM MQ SupportPac MP16 - WebSphere MQ for z/OS -Kapazitätsplanung und -optimierung.

z/OS Protokollierungsumgebung planen

In diesem Abschnitt finden Sie Informationen zur Planung der Anzahl, Größe und Platzierung der Protokolle und Protokollarchive, die von IBM MQ verwendet werden.

Protokolle werden verwendet für:

- Wiederherstellungsinformationen zu persistenten Nachrichten schreiben
- Erfassen von Informationen zu Arbeitseinheiten mit persistenten Nachrichten
- Notieren Sie Informationen zu Änderungen an Objekten, wie z. B. 'define queue'.
- CF-Strukturen sichern

und für andere interne Informationen.

Die IBM MQ-Protokollierungsumgebung wird mithilfe von Systemparametermakros eingerichtet, die unter anderem folgende Optionen festlegen: sollen einzelne oder doppelte aktive Protokolle vorhanden sein, welche Datenträger sollen als Archivprotokolldatenträger verwendet werden und wie viele Protokollpuffer sollen erstellt werden.

Diese Makros werden im Abschnitt Bootstrap-und Protokolldatensätze erstellen und Tailor your system parameter module beschrieben.

Anmerkung: Wenn Sie Gruppen mit gemeinsamer Warteschlange verwenden, stellen Sie sicher, dass Sie die Bootstrap- und Protokolldatengruppen mit SHAREOPTIONS(2 3) definieren.

Dieser Abschnitt enthält Informationen zu den folgenden Themen:

z/OS *Protokolldatensatzes*

Verwenden Sie dieses Thema, um über die am besten geeignete Konfiguration für Ihre Protokolldatensätze zu entscheiden.

Dieses Thema enthält Informationen, die Sie bei der Beantwortung der folgenden Fragen unterstützen:

- Soll in der Installation einfache oder doppelte Protokollierung verwendet werden?
- Wie viele aktive Protokolldateien werden benötigt?
- „Wie groß sollten die aktiven Protokolle sein?” auf Seite 176
- Position der aktiven Protokolldatei

- V 9.2.0 „Aktive Protokollverschlüsselung mit der Dataset-Verschlüsselung von z/OS” auf Seite 177

Soll bei der Installation ein-oder zweifache Protokollierung verwendet werden?

Im Allgemeinen sollten Sie die doppelte Protokollierung für die Produktion verwenden, um das Risiko eines Datenverludes zu minimieren. Wenn Sie möchten, dass Ihr Testsystem die Produktion widerspiegelt, sollten beide die doppelte Protokollierung verwenden. Andernfalls können Ihre Testsysteme eine einzige Protokollierung verwenden.

Mit einzelnen Protokollierungsdaten werden Daten in eine Gruppe von Protokolldatengruppen geschrieben. Bei doppelten Protokolldaten werden Daten in zwei Gruppen von Protokolldateigruppen geschrieben, so dass im Falle eines Problems mit einem Protokolldatensatz, wie z. B. die Datei, die versehentlich gelöscht wird, die entsprechenden Daten in der anderen Gruppe von Protokollen verwendet werden können, um die Daten wiederherzustellen.

Bei doppelter Protokollierung benötigen Sie doppelt so viel DASD wie bei der Einzelprotokollierung.

Wenn Sie die doppelte Protokollierung verwenden, verwenden Sie auch die doppelte BSDSs und die doppelte Archivierung, um eine ausreichende Datenwiederherstellung zu gewährleisten.

Die doppelte aktive Protokollierung führt zu einem geringen Leistungsaufwand.

Achtung: Die Verwendung von Plattenspiegelungstechnologien, wie z. B. Metro Mirror, ist nicht unbedingt ein Ersatz für die doppelte Protokollierung und die doppelte BSDS. Wenn ein gespiegeltes Datenset versehentlich gelöscht wird, gehen beide Kopien verloren.

Wenn Sie persistente Nachrichten verwenden, kann die Einzelprotokollierung die maximale Kapazität um 10-30% erhöhen und auch die Antwortzeiten verbessern.

Bei der Einzelprotokollierung werden 2-310 aktive Protokolldatensätze verwendet, während die doppelte Protokollierung 4-620 aktive Protokolldateien verwendet, um dieselbe Anzahl aktiver Protokolle bereitzustellen. Daher reduziert die Einzelprotokollierung die Menge der protokollierten Daten, die für die Installation von E/A-Bedingungen von Bedeutung sein können.

Wie viele aktive Protokolldatensätze benötigen Sie?

Die Anzahl der Protokolle hängt von den Aktivitäten Ihres Warteschlangenmanagers ab. Für ein Testsystem mit niedrigem Durchsatz können drei aktive Protokolldateien geeignet sein. Für ein Produktionssystem mit hohem Durchsatz können Sie die maximale Anzahl der verfügbaren Protokolle verwenden. Wenn ein Problem beim Ausladeladen von Protokollen auftritt, haben Sie möglicherweise mehr Zeit für die Behebung der Probleme.

Es müssen mindestens drei aktive Protokolldatensätze vorhanden sein, aber es ist vorzuziehen, mehr zu definieren. Wenn zum Beispiel die Zeit, die zum Ausfüllen eines Protokolls erforderlich ist, die Zeit in Anspruch nimmt, die zum Archivieren eines Protokolls während der Spitzenauslastung verwendet wird, definieren Sie weitere Protokolle.

Anmerkung: Seitengruppen und aktive Protokolldatei Datengruppen sind berechtigt, im Speicherbereich der erweiterten Adressierung (EAS) zu residieren als Teil erweiterter Adressvolumen (EAV) und von z/OS V1.12 an kann auch ein Archivprotokolldatensatz im EAS residieren.

Sie sollten auch weitere Protokolle definieren, um mögliche Verzögerungen bei der Protokollarchivierung zu kompensieren. Wenn Sie Archivierungsprotokolle auf Band verwenden, können Sie die Zeit für die Montage des Bands berücksichtigen.

Sie sollten genügend Speicherbereich für aktive Protokolldateien haben, um die Daten eines Tages zu behalten, falls das System nicht in der Lage ist, Daten zu archivieren, weil keine DASD-Einheit vorhanden ist oder nicht auf Band geschrieben werden kann. Wenn alle aktiven Protokolle vollständig gefüllt sind, kann IBM MQ keine persistenten Nachrichten oder Transaktionen verarbeiten. Es ist sehr wichtig, genügend aktiven Protokollspeicherbereich zu haben.

Es ist möglich, neue aktive Protokolldatensätze dynamisch zu definieren, um die Auswirkungen von Archivierungsverzögerungen oder -problemen auf ein Minimum zu reduzieren. Neue Dateien können schnell online geschaltet werden, indem der Befehl **DEFINE LOG** verwendet wird, um zu verhindern, dass der Warteschlangenmanager ' stall' aufgrund von Speicherplatzmangel in der aktiven Protokolldatei verwendet wird.

Wenn Sie mehr als 31 aktive Protokolldateien definieren wollen, müssen Sie Ihre Protokollierungsumgebung so konfigurieren, dass sie ein BSDS der Version 2 verwendet. Wenn ein BSDS der Version 2 im Gebrauch ist, können bis zu 310 aktive Protokolldatensätze für jeden Protokollkopien-Ring definiert werden. Weitere Informationen zum Konvertieren in ein BSDS der Version 2 finden Sie unter „Planung für die Erhöhung des maximal adressierbaren Protokollbereichs” auf Seite 185.

Sie können angeben, ob Ihr Warteschlangenmanager eine BSDS der Version 2 oder höher verwendet, indem Sie entweder das Dienstprogramm für die Druckprotokollzuordnung (CSQJU004) oder die Nachricht CSQJ034I, die während der Initialisierung des Warteschlangenmanagers ausgegeben wurde, ausführen. Ein Ende des ProtokollrBA-Bereichs von FFFFFFFFFFFFFFFF in der Nachricht CSQJ034I gibt an, dass ein BSDS der Version 2 oder höher im Gebrauch ist. Ein Ende des ProtokollrBA-Bereichs von 0000FFFFFFFFFFFF in der Nachricht CSQJ034I zeigt an, dass ein BSDS der Version 1 im Gebrauch ist.

Wenn ein Warteschlangenmanager ein BSDS der Version 2 oder höher verwendet, ist es möglich, mit dem Befehl **DEFINE LOG** einem Protokollkopierring dynamisch mehr als 31 aktive Protokolldateien hinzuzufügen.

Wie groß sollten die aktiven Protokolle sein?

Ab IBM MQ 8.0 beträgt die maximal unterstützte Größe für aktive Protokolle bei Archivierung auf Platte 4 GB. In früheren Releases des Produkts beträgt die maximale unterstützte aktive Protokollgröße bei der Archivierung auf Platte 3 GB.

Bei der Archivierung auf Band beträgt die maximale Größe des aktiven Protokolls 4 GB.

Sie sollten aktive Protokolle mit einer Größe von mindestens 1 GB für Produktions-und Testsysteme erstellen.

Wichtig: Sie müssen bei der Zuordnung von Datensätzen vorsichtig sein, da IDCAMS die von Ihnen zuordenene Größe rundet.

Geben Sie eine der folgenden Optionen an, um ein 3-GB-Protokoll zuzuordnen:

- Zylindern (4369)
- Megabyte (3071)
- TRACKS (65535)
- RECORD (786420)

Jeder dieser Zuordnungen weist 2,99995 GB zu.

Geben Sie eine der folgenden Optionen an, um ein 4-GB-Protokoll zuzuordnen:

- Cylinders (5825)
- Megabyte (4095)
- TRACKS (87375)
- RECORD (1048500)

Jeder dieser Zuordnungen weist 3,9997 GB zu.

Wenn Sie einheitenübergreifende Dateigruppen verwenden, bei denen die Datei auf mehrere Datenträger verteilt ist, wird der angegebene Größenwert auf jedem DASD-Datenträger zugeordnet, der für das Striping verwendet wird. Wenn Sie also 4-GB-Protokolle und vier Datenträger für das Striping verwenden möchten, sollten Sie Folgendes angeben:

- CYLinder (1456)

- Megabyte (1023)

Wenn Sie diese Attribute festlegen, werden 4 * 1456 = 5824 Zylinder oder 4 * 1023 = 4092 Megabyte zugeordnet.

Anmerkung: Striping wird bei Verwendung erweiterter Formatdatensätze unterstützt. Dies wird in der Regel durch den Speichermanager festgelegt.

Siehe Die Größe der aktiven Protokolldatei erhöhen für Informationen zur Ausführung der Prozedur

Aktive Protokollposition

Sie sollten mit Ihrem Speicherverwaltungsteam zusammenarbeiten, um Speicherpools für die Warteschlangenmanager zu konfigurieren. Sie müssen Folgendes berücksichtigen:

- Eine Namenskonvention, damit die WS-Manager die korrekten SMS-Definitionen verwenden.
- Speicherbereich, der für aktive und Archivprotokolle erforderlich ist. Ihr Speicherpool sollte über ausreichend Speicherbereich für die aktiven Protokolle von einem ganzen Tag verfügen.
- Leistung und Ausfallsicherheit bei Fehlern.

Aus Leistungsgründen sollten Sie in Erwägung ziehen, Ihre aktiven Protokolldateien zu strippen. Die Ein-/Ausgabe wird auf mehrere Datenträger verteilt und reduziert die E/A-Antwortzeiten, was zu einem höheren Durchsatz führt. Informationen zum Zuordnen der Größe der aktiven Protokolle beim Verwenden von Striping finden Sie im vorherigen Text.

Sie sollten die E/A-Statistiken mit Hilfe von Berichten aus RMF oder einem ähnlichen Produkt überprüfen. Führen Sie die Überprüfung dieser Statistiken monatlich (oder häufiger) für die IBM MQ-Datensätze durch, um sicherzustellen, dass die Position der Datensätze nicht verzögert wird.

In bestimmten Situationen kann es viele Ein-/Ausgaben für die IBM MQ-Seitengruppe geben, was sich auf die IBM MQ-Protokollleistung auswirken kann, wenn sich die Protokolldateien auf demselben DASD befinden.

Wenn Sie die doppelte Protokollierung verwenden, stellen Sie sicher, dass jede Gruppe von aktiven Protokollen und Archivierungsprotokollen getrennt wird. Sie können sie z. B. auf separaten DASD-Subsystemen oder auf verschiedenen Einheiten zuordnen.

Dadurch wird das Risiko verringert, dass beide verloren gehen, wenn einer der Datenträger beschädigt oder zerstört ist. Wenn beide Kopien des Protokolls verloren gehen, ist die Wahrscheinlichkeit eines Datenverlusts hoch.

Wenn Sie eine neue aktive Protokolldatei erstellen, sollten Sie die Datei mit dem Präfix CSQJUFMT vorformatieren. Wenn das Protokoll nicht vorformatiert ist, formatiert der Warteschlangenmanager das Protokoll beim ersten Mal, was sich auf die Leistung auswirkt.

Bei älteren DASDs mit großen Spinnscheiben mussten Sie vorsichtig sein, welche Datenträger verwendet wurden, um die beste Leistung zu erhalten.

Bei modernen DASDs, bei denen Daten über viele PC-Festplatten verteilt sind, müssen Sie sich nicht so sehr um die Verwendung von Datenträgern kümmern.

Ihr Speichermanager sollte die Enterprise-DASD überprüfen, um die Leistungsprobleme zu überprüfen und zu beheben. Für die Verfügbarkeit können Sie eine Gruppe von Protokollen auf einem DASD-Subsystem und die dualen Protokolle auf einem anderen DASD-Subsystem verwenden.

Aktive Protokollverschlüsselung mit der Dataset-Verschlüsselung von z/OS

Sie können die z/OS -Funktion zur Dateiverschlüsselung auf aktive Protokolldateien für Warteschlangenmanager anwenden, die unter IBM MQ for z/OS 9.1.4 oder höher ausgeführt werden.

Sie müssen diese aktiven Protokolldateien mit EXTENDED-Attributen und einem Dateischlüsselkennsatz zuordnen, der sicherstellt, dass die Daten mit AES verschlüsselt werden.

Weitere Informationen finden Sie im Abschnitt zur Vertraulichkeit für ruhende Daten in IBM MQ for z/OS mit der Dataset-Verschlüsselung. weitere Informationen hierzu.

V 9.2.0 z/OS *Verwenden von MetroMirror mit IBM MQ*

IBM Metro Mirror, früher als "Synchronous Peer to Peer Remote Copy" (PPRC) bekannt, ist eine synchrone Replikationslösung zwischen zwei Speichersubsystemen, in der Schreiboperationen sowohl auf dem primären als auch auf dem sekundären Datenträger ausgeführt werden, bevor die Schreiboperation als abgeschlossen betrachtet wird. Metro Mirror kann in Umgebungen verwendet werden, die keine Datenverluste im Fall eines Speichersubsystemfehlers erfordern.

Unterstützte Datensatztypen

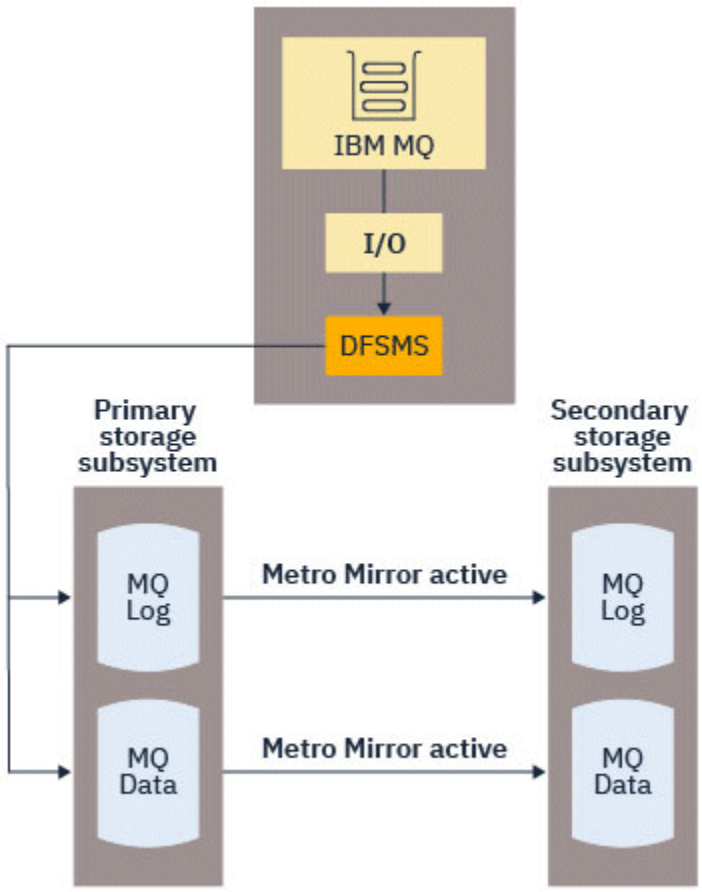
Alle der folgenden IBM MQ-Datensatztypen können mit Metro Mirror repliziert werden. Welche replizierten jedoch genau repliziert werden, hängt von den Verfügbarkeitsanforderungen Ihres Unternehmens ab:

- Aktive Protokolldateien
- Archivprotokolle
- Bootstrap-Dataset (BSDS)
- Seitengruppen
- Gemeinsam genutzte Nachrichtendatei (SMDS)
- Datensätze, die für die Konfiguration verwendet werden, z. B. in den DD-Karten CSQINP* in der MSTR-JCL

Verwenden von zHyperWrite mit aktiven IBM MQ-Protokollen

Wenn ein Schreibzugriff auf einen Datensatz erfolgt, der mit Metro Mirror repliziert wird, wird zuerst der Schreibzugriff auf den Primärdatenträger durchgeführt und anschließend auf den sekundären Datenträger repliziert. Diese Replikation wird vom Speichersubsystem ausgeführt und ist für die Anwendung transparent, die das Schreiben ausgegeben hat, z. B. IBM MQ.

Dieser Prozess wird im folgenden Diagramm dargestellt.

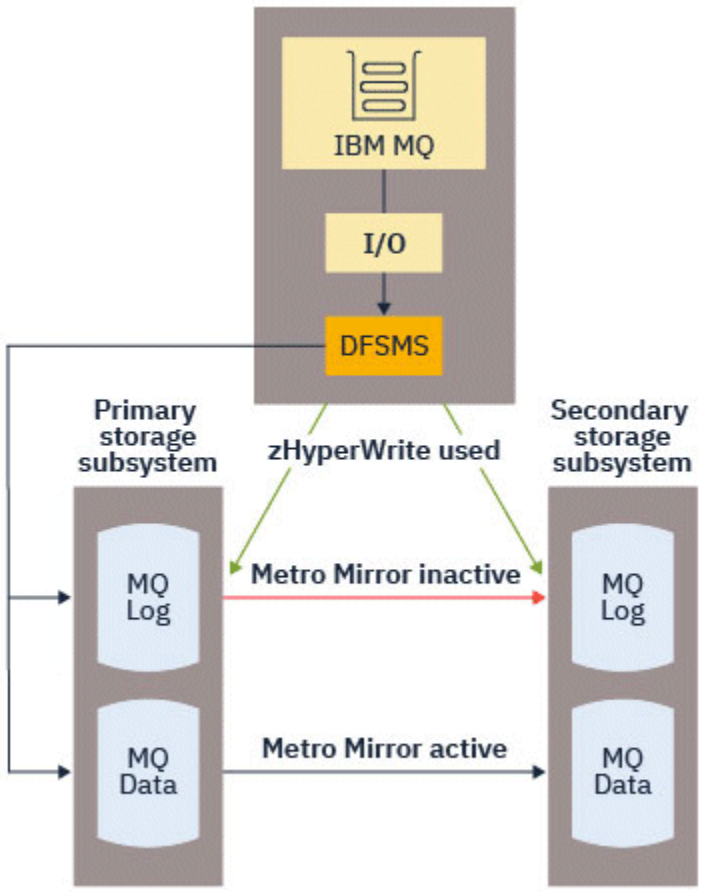


Da beide Schreibvorgänge in den primären und sekundären Speichersubsystemen abgeschlossen werden müssen, bevor der Schreibzugriff auf IBM MQ zurückkehrt, kann die Verwendung von Metro Mirror Auswirkungen auf die Leistung haben. Sie müssen diese Leistungseinwirkungen auf die Verfügbarkeitsvorteile der Verwendung von Metro Mirror abwägen.

Die aktiven IBM MQ-Protokolle sind besonders sensibel bezüglich der Leistungseinwirkungen der Verwendung von Metro Mirror. IBM MQ ermöglicht die Verwendung von zHyperWrite mit den aktiven Protokollen, um diese Leistungsbeeinträchtigung zu reduzieren.

zHyperWrite ist eine Speichersubsystemtechnologie, die mit z/OS funktioniert, um die Leistungseinwirkungen von Schreibvorgängen auf Dateien zu reduzieren, die mit Metro Mirror repliziert werden. Wenn zHyperWrite verwendet wird, wird der Schreibzugriff auf den primären und den sekundären Datenträger parallel auf der Ebene des Data Facility Storage Management-Subsystems (DFSMS) abgesetzt, statt sequenziell auf Speichersubsystemebene zu setzen, wodurch die Leistungseinwirkung verringert wird.

Das folgende Diagramm veranschaulicht zHyperWrite, das für die aktiven Protokolle verwendet wird, und Metro Mirror wird für die anderen IBM MQ-Datensatztypen verwendet. Wenn ein zHyperWrite-Schreiben fehlschlägt, gibt DFSMS den Schreibvorgang mit Metro Mirror transparent erneut aus.



zHyperWrite unter IBM MQ wird nur in den aktiven Protokolldatengruppen unterstützt.

Wenn Sie zHyperWrite mit den aktiven Protokollen verwenden möchten, müssen Sie:

- Konfigurieren Sie IBM MQ für die Verwendung von zHyperWrite und
- Die aktiven Protokolle müssen sich auf zHyperWrite-fähigen Datenträgern befinden.

Wenn beide Bedingungen erfüllt sind, werden Schreibvorgänge in aktive Protokolle für zHyperWrite aktiviert.

Sie können anhand einer der folgenden Methoden IBM MQ für die Verwendung von zHyperWrite konfigurieren:

- Geben Sie ZHYWRITE (YES) in das Systemparametermodul an.
- Geben Sie den Befehl SET LOG LOG ZHYWRITE (YES) aus.

Legen Sie die folgenden Bedingungen für aktive Protokolldateien fest, die sich auf zHyperWrite-fähigen Datenträgern befinden:

- Aktivieren Sie die Datenträger für Metro Mirror, und die Datenträger unterstützen zHyperWrite.
- Stellen Sie sicher, dass die Datenträger HyperSwap-fähig sind.
- Geben Sie HYPERWRITE=YES im Parameter IECIOSxx an.

Wenn alle vorherigen Bedingungen erfüllt sind, werden in die aktiven Protokolle für zHyperWrite geschrieben.

Wenn eine oder mehrere dieser Bedingungen nicht erfüllt sind, schreibt IBM MQ in die aktiven Protokolle als normal, und Metro Mirror repliziert die Schreibvorgänge, wenn sie konfiguriert ist.

Anmerkungen:

- IBM MQ erfordert nicht, dass alle aktiven Protokolldatensätze auf zHyperWrite-fähigen Datenträgern vorhanden sind.

  Wenn IBM MQ feststellt, dass einige aktive Protokolldateien auf zHyperWrite-fähigen Datenträgern vorhanden sind und andere nicht, gibt sie die Nachricht CSQJ166E aus und führt die Verarbeitung durch.
- IBM MQ prüft, ob aktive Protokolldatensätze zHyperWrite-fähig sind, wenn die Datensätze zum ersten Mal geöffnet werden.

  Protokolldatensätze werden entweder beim Start des Warteschlangenmanagers geöffnet oder beim dynamischen Hinzufügen mit dem Befehl DEFINE LOG. Wenn die Protokolldatensätze zHyperWrite-fähig gemacht werden, während ein Warteschlangenmanager sie geöffnet hat, erkennt der Warteschlangenmanager diese erst, wenn er erneut gestartet wurde.

Sie können die Ausgabe des Befehls DISPLAY LOG verwenden, um anzugeben, ob es sich bei den aktuellen aktiven Protokolldateien um zHyperWrite-fähig handelt. Das folgende Beispiel zeigt, dass beide Datensätze zHyperWrite-fähig sind. Wenn der Warteschlangenmanager mit ZHYWRITE (YES) konfiguriert wurde, werden in diese Protokolle Schreibvorgänge für zHyperWrite aktiviert:

```
Copy %Full zHyperWrite DSName
 1      4  CAPABLE     MQTST.SUBSYS.MQDL.LOGCOPY1.DS001
 2      4  CAPABLE     MQTST.SUBSYS.MQDL.LOGCOPY2.DS001
```

z/OS *Planen des Protokollarchivierungsspeichers*

Verwenden Sie dieses Thema, um die verschiedenen Methoden zum Verwalten der Archivprotokolldateien zu verstehen.

Sie können Archivprotokolldateien auf Standard-Label-Bändern oder auf DASD-Einheiten stellen, und Sie können sie durch den hierarchischen Speichermanager (DFHSM) der Dateneinrichtung verwalten. Jeder logische z/OS-Satz in einer Archivprotokolldatei entspricht einem VSAM-Steuerintervall (Virtual Storage Access Method) aus der aktiven Protokolldatei. Die Blockgröße beträgt ein Vielfaches von 4 KB.

Archivprotokolldateien werden dynamisch zugeordnet, wobei die Namen von IBM MQ ausgewählt werden. Das Präfix, die Blockgröße, der Einheitenname und die DASD-Größen, die für solche Zuordnungen benötigt werden, werden im Systemparametermodul angegeben. Sie können bei der Installation auch angeben, dass IBM MQ dem Namen der Archivprotokolldatei ein Datum und eine Uhrzeit hinzufügen soll.

Es ist nicht möglich anzugeben, dass IBM MQ bestimmte Datenträger für neue Archivprotokolle verwenden soll, aber dies können Sie mithilfe von Speichermanagementroutinen erreichen. Wenn Zuordnungsfehler auftreten, wird die Ausladung verschoben, bis die nächste Auslastung ausgelöst wird.

Wenn Sie während der Installation doppelte Archivprotokolle angeben, wird jedes Protokollsteuerintervall, das aus dem aktiven Protokoll abgerufen wird, in zwei Archivierungsprotokolldateien geschrieben. Die Protokollsätze, die im Paar von Archivierungsprotokolldatensätzen enthalten sind, sind identisch, aber die Datenträgerende-Punkte werden nicht für Datensätze mit mehreren Datenmengen synchronisiert.

Sollen die Archivprotokolle auf Band oder auf DASD gespeichert werden?

Bei der Entscheidung, ob das Band oder die DASD-Einheit für Ihre Archivprotokolle verwendet werden soll, müssen Sie eine Reihe von Faktoren berücksichtigen:

- Überprüfen Sie die Betriebsprozeduren, bevor Sie über ein Band oder eine Platte entscheiden. Wenn Sie beispielsweise auswählen, dass auf Band archiviert werden soll, muss genügend Bandlaufwerk vorhanden sein, wenn sie benötigt werden. Nach einem Katastrophenfall können alle Subsysteme Bandlaufwerke haben, und Sie haben möglicherweise nicht so viele freie Bandlaufwerke wie erwartet.
- Während der Wiederherstellung sind Archivprotokolle auf Band verfügbar, sobald das Band geladen ist. Wenn DASD-Archive verwendet wurden und die Datensätze mit Hilfe des hierarchischen Speichermanagers (HSM) auf Band umgelagert wurden, gibt es eine Verzögerung, während HSM jede Datei auf die

Platte zurückweist. Sie können die Datensätze zurückrufen, bevor das Archivprotokoll verwendet wird. Es ist jedoch nicht immer möglich, die korrekte Reihenfolge vorherzusagen, in der sie erforderlich sind.

- Wenn bei der Verwendung von Archivprotokollen auf der DASD-Einheit viele Protokolle erforderlich sind (dies kann der Fall sein, wenn eine Seitengruppe nach der Wiederherstellung aus einer Sicherung wiederhergestellt wird), benötigen Sie möglicherweise eine beträchtliche Menge an DASD, um alle Archivprotokolle aufnehmen zu können.
- In einem System mit geringer Auslastung oder einem Testsystem kann es günstiger sein, Archivprotokolle auf DASD zu haben, um den Bedarf an Bandladevorgänge zu vermeiden.
- Wenn Sie den Befehl RECOVER CFSTRUCT ausgeben und eine persistente UOW (Unit of Work) sichern, wird das Protokoll rückwärts gelesen. Bandlaufwerke mit Hardwarekomprimierung führen schlecht für Operationen aus, die rückwärts gelesen werden. Planen Sie ausreichend Protokolldaten auf DASD, um zu vermeiden, dass die Daten von Band rückwärts gelesen werden.

Das Archivieren auf DASD bietet eine schnellere Wiederherstellbarkeit, ist aber teurer als die Archivierung auf Band. Wenn Sie die doppelte Protokollierung verwenden, können Sie angeben, dass die primäre Kopie des Archivprotokolls in der DASD-Einheit enthalten ist und die sekundäre Kopie auf Band. Dies erhöht die Wiederherstellungsgeschwindigkeit, ohne dabei so viel DASD zu verwenden, und Sie können das Band als Sicherung verwenden.

Im Abschnitt „Speichermedium für Archivprotokolle ändern” auf Seite 183 finden Sie Details dazu, wie Sie Ihre Protokolle nicht mehr auf Band, sondern in DASD archivieren und den umgekehrten Prozess ausführen.

Archivierung auf Band

Wenn Sie sich für die Archivierung auf einer Bandeinheit entscheiden, kann IBM MQ auf maximal 20 Datenträger erweitert werden.

Wenn Sie erwägen, die Größe der aktiven Protokolldatei so zu ändern, dass die Gruppe auf einen Banddatenträger passt, ist zu beachten, dass eine Kopie des BSDS auf denselben Banddatenträger gestellt wird wie die Kopie der aktiven Protokolldatei. Passen Sie die Größe der aktiven Protokolldatei nach unten an, um den für die BSDS auf dem Banddatenträger erforderlichen Speicherbereich zu versetzen.

Wenn Sie Doppelarchivierungsprotokolle auf Band verwenden, ist es typisch, dass eine Kopie lokal gehalten wird und die andere Kopie für die Verwendung in der Disaster Recovery (Disaster Recovery) ausgelagert wird.

Archivieren auf DASD-Datenträger

IBM MQ erfordert, dass Sie alle Archivprotokolldateien katalogisieren, die Nicht-Bandeinheiten (DASD) zugeordnet sind. Wenn Sie die Archivierung auf DASD auswählen, muss der Parameter CATALOG des Makros CSQ6ARVP YES sein. Wenn dieser Parameter auf "NO" (Nein) festgelegt ist und Sie sich dafür entscheiden, Archivprotokolldateien auf einem DASD (Direct Access Storage Device) zu speichern, erhalten Sie bei jeder Zuordnung einer Archivprotokolldatei die Nachricht CSQJ072E, obwohl IBM MQ die Datei dennoch katalogisiert.

Wenn die Archivprotokolldatei auf DASD gehalten wird, können die Archivierungsprotokolldatensätze auf einen anderen Datenträger erweitert werden. Mehrvolumen wird unterstützt.

Wenn Sie sich für die Verwendung von DASD entscheiden, stellen Sie sicher, dass die primäre Speicherbereichszuordnung (sowohl die Größe als auch die Blockgröße) groß genug ist, um die Daten zu enthalten, die aus der aktiven Protokolldatei stammen, oder aus dem entsprechenden BSDS, je nachdem, welcher der beiden größer ist.

Dadurch wird die Möglichkeit minimiert, dass während des Auslagerungsprozesses die unerwünschten z/OS-Abbruchcodes X'B37' oder X'E37' auftreten. Die primäre Bereichszuordnung wird mit dem Parameter PRIQTY (Primärmenge) des Makros CSQ6ARVP festgelegt.

Ab IBM MQ for z/OS 8.0 können Archivprotokolldateien in sequenziellen Dateien mit großem oder erweitertem Format vorhanden sein. SMS-ACS-Routinen können jetzt DSNTYPE (LARGE) oder DSNTYPE (EXT) verwenden. Diese wurden vor IBM MQ for z/OS 8.0 nicht unterstützt.

IBM MQ unterstützt die Zuordnung von Archivprotokollen als Dateien mit erweitertem Format. Wenn das erweiterte Format verwendet wird, wird die maximale Größe des Archivierungsprotokolls von 65535 Spuren auf die maximale Größe des aktiven Protokolls von 4 GB erhöht. Archivprotokolle können für die Zuordnung im erweiterten Adressraum (EAS) von erweiterten Adressdatenträgern (EAV) ausgewählt werden.

Wenn die erforderlichen Hardware- und Softwarestufen verfügbar sind, kann die Zuordnung von Archivprotokollen zu einer Datenklasse, die mit COMPACTION unter Verwendung von zEDC definiert ist, den Plattenspeicher reduzieren, der für die Aufbewahrung von Archivprotokollen erforderlich ist. Weitere Informationen finden Sie in IBM MQ for z/OS: Reducing storage occupancy with IBM zEnterprise Data Compression (zEDC) .

Weitere Informationen zu Hardware- und Softwareebenen finden Sie im Artikel Funktionale Erweiterungen für zEnterprise Data Compression (zEDC) verwenden, dort finden sich ebenfalls Beispiele für RACF-Profiländerungen.

Die Dateiverschlüsselungsfunktion von z/OS kann auf Archivprotokolle für Warteschlangenmanager angewendet werden, die mit IBM MQ 8.0 oder höher ausgeführt werden. Diese Archivprotokolle müssen über ACS-Routinen (Automatic Class Selection) zu einer Datenklasse zugeordnet werden, die mit EXTENDED-Attributen definiert ist, und mit einem Datensatzschlüsselkennsatz, der sicherstellt, dass die Daten AES-verschlüsselt sind.

SMS mit Archivierungsprotokolldateien verwenden

Wenn Sie MVS/DFP Storage Management Subsystem (DFSMS) installiert haben, können Sie einen Benutzerexitfilter für die automatische Klassenauswahl (ACS) für Ihre Archivierungsprotokolldateien schreiben, der Sie bei der Konvertierung in die SMS-Umgebung unterstützt.

Ein solcher Filter kann die Ausgabe beispielsweise an eine DASD-Datei weiterleiten, die von DFSMS verwaltet werden kann. Sie müssen vorsichtig sein, wenn Sie auf diese Weise einen ACS-Filter verwenden. Da für SMS DASD-Datensets katalogisiert werden müssen, müssen Sie sicherstellen, dass das Feld CATALOG DATA des Makros CSQ6ARVP JA enthält. Wenn dies nicht der Fall ist, wird die Nachricht CSQJ072E zurückgegeben. Dennoch wird die Datei von IBM MQ katalogisiert.

Weitere Informationen zu ACS-Filtern finden Sie unter Datensätze, die DFSMShsm dynamisch zuordnet .

z/OS *Speichermedium für Archivprotokolle ändern*

Die Prozedur zum Ändern des Speichermediums, das von Archivprotokollen verwendet wird.

Informationen zu diesem Vorgang

In dieser Task wird beschrieben, wie das Speichermedium, das für Archivprotokolle verwendet wird, geändert werden kann, z. B. bei einer Archivierungsumstellung von Band auf DASD.

Sie haben die Wahl, wie Sie die Änderungen vornehmen möchten:

1. Nehmen Sie die Änderungen nur mit dem Makro CSQ6ARVP vor, so dass sie ab dem nächsten Neustart des Warteschlangenmanagers angewendet werden.
2. Nehmen Sie die Änderungen mit dem Makro CSQ6ARVP und dynamisch mit dem Befehl SET ARCHIVE vor. Dies bedeutet, dass die Änderungen ab dem nächsten Mal, wenn der Warteschlangenmanager eine Protokolldatei archiviert, gelten und nach dem Neustart des Warteschlangenmanagers bestehen bleiben.

Vorgehensweise

1. Änderung, damit Archivprotokolle auf DASD statt auf Band gespeichert werden:

a) Lesen Sie den Abschnitt „Archivieren auf DASD-Datenträger” auf Seite 182 und überprüfen Sie die Parameter CSQ6ARVP.

b) Nehmen Sie Änderungen an den folgenden Parametern in CSQ6ARVP vor.

- Aktualisieren Sie den Parameter UNIT und, falls erforderlich, auch UNIT2.
- Aktualisieren Sie den Parameter BLKSIZE, da sich die optimale Einstellung für DASD-Datenträger von der optimalen Einstellung für Bänder unterscheidet.
- Setzen Sie die Parameter PRIQTY und SECQTY auf einen Wert, der ausreicht, um das größte der aktiven Protokolle oder BSDS speichern zu können.
- Setzen Sie den Parameter CATALOG auf YES.
- Vergewissern Sie sich, dass die Einstellung ALCUNIT das ist, was Sie möchten. Sie sollten BLK verwenden, da sie unabhängig vom Einheitentyp ist.
- Setzen Sie den Parameter ARCWTOR auf NO, wenn dies nicht bereits der Fall ist.

2. Änderung, damit Archivprotokolle auf Band statt in DASD gespeichert werden:

a) Lesen Sie den Abschnitt „Archivierung auf Band” auf Seite 182 und überprüfen Sie die Parameter CSQ6ARVP.

b) Nehmen Sie Änderungen an den folgenden Parametern in CSQ6ARVP vor:

- Aktualisieren Sie den Parameter UNIT und, falls erforderlich, auch UNIT2.
- Aktualisieren Sie den Parameter BLKSIZE, da sich die optimale Einstellung für Bänder von der optimalen Einstellung für DASD-Datenträger unterscheidet.
- Vergewissern Sie sich, dass die Einstellung ALCUNIT das ist, was Sie möchten. Sie sollten BLK verwenden, da sie unabhängig vom Einheitentyp ist.
- Überprüfen Sie die Einstellung des Parameters ARCWTOR.

z/OS *Wie lange muss ich Archivierungsprotokolle aufbewahren?*

Verwenden Sie die Informationen in diesem Abschnitt, um Sie bei der Planung Ihrer Sicherungsstrategie zu unterstützen.

Sie geben an, wie lange Archivprotokolle in Tagen aufbewahrt werden sollen. Verwenden Sie dazu den Parameter ARCRETN in USING CSQ6ARVP oder den Befehl SET SYSTEM . Nach diesem Zeitraum können die Dateien von z/OS gelöscht werden.

Sie können Archivierungsprotokolldatensätze manuell löschen, wenn sie nicht mehr benötigt werden.

- Der WS-Manager benötigt möglicherweise die Archivprotokolle für die Wiederherstellung.

  Der WS-Manager kann nur die letzten 1000 Archive im BSDS beibehalten, wenn die Archivprotokolle nicht im BSDS enthalten sind, können sie nicht für die Wiederherstellung verwendet werden und dienen nur zur Prüfung, Analyse oder Wiedergabetypenverwendung.
- Möglicherweise möchten Sie die Archivprotokolle so halten, dass Sie Informationen aus den Protokollen extrahieren können. Beispiel: Extrahieren von Nachrichten aus dem Protokoll und Überprüfen der Benutzer-ID, die die Nachricht enthält oder erhalten hat.

Das BSDS enthält Informationen zu Protokollen und anderen Wiederherstellungsinformationen. Diese Datei ist eine feste Größe. Wenn die Anzahl der Archivprotokolle den Wert von MAXARCH in CSQ6LOGP erreicht oder wenn das BSDS voll ist, werden die ältesten Archivprotokolldaten überschrieben.

Es gibt Dienstprogramme zum Entfernen von Archivierungsprotokolleinträgen aus dem BSDS, aber im Allgemeinen wird der älteste Archivprotokollsatz von BSDS umgebrochen und überlagert.

Wann ist ein Archivprotokoll erforderlich?

Sie müssen Ihre Seitengruppen regelmäßig sichern. Die Häufigkeit von Sicherungen bestimmt, welche Archivprotokolle im Fall des Verlues einer Seitengruppe benötigt werden.

Sie müssen Ihre CF-Strukturen regelmäßig sichern. Die Häufigkeit von Sicherungen bestimmt, welche Archivprotokolle für den Verlust von Daten in der CF-Struktur benötigt werden.

Das Archivprotokoll kann für die Wiederherstellung benötigt werden. Die folgenden Informationen erläutern, wann das Archivprotokoll benötigt wird, wenn es Probleme mit den verschiedenen IBM MQ-Ressourcen gibt.

Verlust einer Seitengruppe
Sie müssen Ihr System von der Sicherung wiederherstellen und den Warteschlangenmanager erneut starten.

Sie benötigen die Protokolle von, wenn die Sicherung ausgeführt wurde, sowie bis zu drei Protokolldatensätze, bevor die Sicherung ausgeführt wird.

Alle LPARs verlieren die Verbindung zu einer CF-Struktur, oder die Struktur ist nicht verfügbar.
Verwenden Sie den Befehl RECOVER CFSTRUCT , um die Struktur wiederherzustellen.

Die Strukturwiederherstellung erfordert die Protokolle aller WS-Manager, die seit der letzten Sicherung auf die Struktur zugegriffen haben (zurück zu dem Zeitpunkt, zu dem die Sicherung ausgeführt wurde) sowie die Struktursicherung selbst im Protokoll des Warteschlangenmanagers, der die Sicherung übernommen hat.

Wenn Sie häufige Sicherungen der CF-Strukturen ausgeführt haben, sollten sich die Daten in aktiven Protokollen befinden, und Sie sollten keine Archivprotokolle benötigen.

Wenn es keine aktuelle Sicherung der CF-Struktur gibt, benötigen Sie möglicherweise Archivprotokolle.

Anmerkung: Alle nicht persistenten Nachrichten gehen verloren. Alle persistenten Nachrichten werden erneut erstellt, indem Sie die folgenden Tasks ausführen:

1. Letzte CF-Struktursicherung aus dem Protokoll lesen
2. Protokolle aus allen Warteschlangenmanagern lesen, die die Struktur verwendet haben
3. Aktualisierungen seit der Sicherung zusammenführen

Wiederherstellung der Verwaltungsstruktur
Wenn Sie die Verwaltungsstruktur erneut erstellen müssen, werden die Informationen aus dem letzten Prüfpunkt des Protokolls für jeden Warteschlangenmanager in der QSG gelesen.

Wenn ein Warteschlangenmanager nicht aktiv ist, liest ein anderer WS-Manager in der QSG das Protokoll.

Archivierungsprotokolle sollten nicht benötigt werden.

Verlust einer SMDS-Datei
Wenn Sie eine SMDS-Datei verlieren oder die Datei beschädigt wird, wird die Datei unbrauchbar, und der Status für diese Datei ist auf FAILED gesetzt. Die CF-Struktur ist unverändert.

Um die SMDS-Datei zurückschreiben zu können, müssen Sie:

1. Definieren Sie die SMDS-Datei neu.
2. Sie können die CF-Struktur wiederherstellen, indem Sie den Befehl RECOVER CFSTRUCT ausgeben.

   Anmerkung: Alle nicht persistenten Nachrichten in der CF-Struktur gehen verloren. Alle persistenten Nachrichten werden wiederhergestellt.

Die Voraussetzung für WS-Manager-Protokolle ist die gleiche wie bei der Wiederherstellung nach einer Struktur, die nicht verfügbar ist.

z/OS *Planung für die Erhöhung des maximal adressierbaren Protokollbereichs*

Sie können den maximal adressierbaren Protokollbereich erhöhen, indem Sie Ihren Warteschlangenmanager so konfigurieren, dass er eine größere relative Byteadresse (RBA) verwendet.

Die Größe der relativen Byteadresse für das Protokoll wurde erhöht von IBM MQ for z/OS 8.0. Eine Übersicht über diese Änderung finden Sie unter Relative Byteadresse für größere Protokolle.

V 9.2.0 Wenn sich der Warteschlangenmanager nicht in einer Gruppe mit gemeinsamer Warteschlange befindet, können Sie ihn so konvertieren, dass er zu jedem beliebigen Zeitpunkt 8-Byte-Protokoll-RBA-Werte verwendet. Wenn Sie anschließend eine Migration auf IBM MQ for z/OS 9.0.0durchführen, stellen Sie sicher, dass Sie **OPMODE**=(*NEWFUNC,900*) verwenden, da andernfalls der Warteschlangenmanager nicht gestartet wird.

V 9.2.5 Wenn der Warteschlangenmanager unter IBM MQ 9.2.5 oder höher erstellt wurde, ist die 8-Byte-Protokoll-RBA bereits standardmäßig aktiviert und erfordert daher keine Konvertierung.

Bevor WS-Manager in einer Gruppe mit gemeinsamer Warteschlange in die 8-Byte-Protokoll-RBA konvertiert werden können, müssen alle Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange eine der folgenden Stufen haben:

- IBM MQ for z/OS 9.0.n CD, IBM MQ for z/OS 9.1.0 LTS oder höher
- IBM MQ for z/OS 9.0.0 und gestartet mit **OPMODE**=(*NEWFUNC,800*) oder **OPMODE**=(*NEWFUNC,900*)

Sie können dann jeden WS-Manager ändern, um die 8-Byte-Protokoll-RBA-Werte zu verwenden. Es ist nicht unbedingt erforderlich, alle WS-Manager gleichzeitig zu ändern.

Wenn ein Warteschlangenmanager in einer Gruppe mit gemeinsamer Warteschlange konvertiert wurde, um 8-Byte-Protokoll-RBA-Werte zu verwenden, können andere Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange die Protokolle des konvertierten Warteschlangenmanagers verwenden, auch wenn sie noch nicht in die Verwendung von 8 Byte-RBA-Werten für Byteprotokoll konvertiert wurden. Dies ist beispielsweise nützlich für die Peer-Wiederherstellung.

Änderung rückgängig machen

Die Änderung kann nicht zurückgesetzt werden.

Wie lange dauert es?

Für die Änderung ist ein Neustart des Warteschlangenmanagers erforderlich. Stoppen Sie den Warteschlangenmanager, führen Sie das Dienstprogramm CSQJUCNV für die Bootstrap-Datei (BSDS) oder die Datensätze aus, um neue Dateien zu erstellen, diese Bootstrap-Dateigruppen umzubenennen und den Warteschlangenmanager erneut zu starten. Das Dienstprogramm CSQJUCNV benötigt in der Regel einige Sekunden, um ausgeführt zu werden.

Welche Auswirkungen hat das?

- Bei Verwendung von 8-Byte-Protokoll-RBA im Gebrauch enthält jedes Schreiben von Daten in die Protokolldatengruppen zusätzliche Byte. Aus diesem Grund ist für eine Arbeitslast, die aus persistenten Nachrichten besteht, die Menge der Daten, die in die Protokolle geschrieben werden, gering.
- Daten, die in eine Seitengruppe oder Coupling Facility (CF) -Struktur geschrieben werden, sind nicht betroffen.

Zugehörige Tasks

Relative Byteadresse für größere Protokolle implementieren

z/OS Kanalinitiator planen

Der Kanalinitiator stellt die Kommunikation zwischen Warteschlangenmanagern zur Verfügung und wird in einem eigenen Adressraum ausgeführt.

Es gibt zwei Arten von Verbindungen:

1. Anwendungsverbindungen zu einem WS-Manager über ein Netz. Diese werden als Clientkanäle bezeichnet.

2. Warteschlangenmanager für WS-Manager-Verbindungen. Diese werden als MCA-Kanäle bezeichnet.

Empfangsprogramme

Ein Kanal-Listener-Programm ist für eingehende Netzanforderungen empfangsbereit und startet den entsprechenden Kanal, wenn dieser Kanal benötigt wird. Für die Verarbeitung eingehender Verbindungen benötigt der Kanalinitiator mindestens eine konfigurierte IBM MQ-Listener-Task. Ein Listener kann entweder ein TCP-Listener oder ein LU 6.2-Listener sein.

Für jedes Empfangsprogramm ist ein TCP-Port oder ein LU-Name erforderlich. IBM MQ for Multiplatforms verwendet häufig den TCP/IP-Port 1414 (Standardeinstllung).

Beachten Sie, dass Sie für jeden Kanalinitiator mehr als einen Listener haben können.

TCP/IP

Ein Kanalinitiator kann mehr als einen TCP-Stack in demselben z/OS-Image betreiben. Beispiel: Ein TCP-Stack könnte für interne Verbindungen und ein anderer TCP-Stack für externe Verbindungen sein.

Wenn Sie einen Ausgabekanal definieren:

1. Sie legen den Zielhost und den Zielport der Verbindung fest. Dies kann Folgendes sein:
   - eine IP-Adresse, z. B. `10.20.4.6`
   - einen Hostnamen, z. B. `mvs-prod.myorg.com`

   Wenn Sie als Ziel einen Hostnamen angeben, verwendet IBM MQ zum Auflösen der Ziel-IP-Adresse das Domain Name System (DNS).
2. Wenn Sie mehrere TCP-Stacks verwenden, können Sie den Parameter **LOCLADDR** in der Kanaldefinition angeben, in der die zu verwendende IP-Stack-Adresse angegeben ist.

Sie sollten einen hoch verfügbaren DNS-Server oder DNS-Server planen. Wenn der DNS nicht verfügbar ist, können abgehende Kanäle möglicherweise nicht gestartet werden, und Kanalauthentifizierungsregeln, die eine eingehende Verbindung mit einem Hostnamen zuordnen, können nicht verarbeitet werden.

APPC und LU 6.2

Wenn Sie APPC verwenden, benötigt der Kanalinitiator einen LU-Namen und eine Konfiguration in APPC.

Gruppen mit gemeinsamer Warteschlange

Wenn Sie ein einzelnes Systemimage bereitstellen und gleichzeitig zulassen möchten, dass eine eingehende IBM MQ-Verbindungsanforderung an jeden Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange zugestellt wird, müssen Sie einige Konfigurationsschritte ausführen. Beispiel:

1. Ein Hardware-Netzwerk-Router. Dieser Router verfügt über eine IP-Adresse, die vom Unternehmen angezeigt wird, und kann die ursprüngliche Anforderung an jeden Warteschlangenmanager weiterleiten, der mit dieser Hardware verbunden ist.
2. Eine virtuelle IP-Adresse (VIPA). Es wird eine unternehmensweite IP-Adresse angegeben, und diese Adresse kann an jeden der TCP-Stacks in einem Sysplex weitergeleitet werden. Der TCP-Stack kann ihn dann an einen beliebigen Empfangswarteschlangenmanager im Sysplex weiterleiten.

IBM MQ-Datenverkehr schützen

Zum Schutz der Daten während der Übertragung können Sie IBM MQ für die Verwendung von TLS-Verbindungen (oder SSL-Verbindungen) konfigurieren. Um TLS verwenden zu können, müssen Sie digitale Zertifikate und Schlüsselringe verwenden.

Außerdem müssen Sie sich mit den Administratoren am fernen Ende des Kanals abstimmen, um sicherzustellen, dass Sie an beiden Enden kompatible IBM MQ-Definitionen und kompatible Zertifikate haben.

Sie können anhand der folgenden Merkmale steuern, welche Verbindungen zu IBM MQ und zur Benutzer-ID zulässig sind:

- IP-Adresse
- Clientbenutzer-ID
- Ferner Warteschlangenmanager oder
- Digitales Zertifikat (siehe Kanalauthentifizierungsdatensätze)

Es ist auch möglich, Clientanwendungen zu beschränken, indem sichergestellt wird, dass sie eine gültige Benutzer-ID und ein gültiges Kennwort angeben (siehe Verbindungsauthentifizierung).

Sie können den Kanalinitiator abrufen und anschließend jeden Kanal so konfigurieren, dass er TLS verwendet, jeweils eine nach einem anderen.

Kanalinitiator überwachen

Es gibt MQSC-Befehle, die Informationen zum Kanalinitiator und zu Kanälen geben:

- Mit dem Befehl DISPLAY CHINIT werden Informationen zum Kanalinitiator und aktiven Empfangsprogrammen angezeigt.
- Mit dem Befehl DISPLAY CHSTATUS wird die Aktivität und der Status eines Kanals angezeigt.

Der Kanalinitiator kann auch SMF-Datensätze mit Informationen über die Kanalinitiatortasks und die Kanalaktivität erstellen. Weitere Informationen finden Sie unter „SMF-Daten des Kanalinitiators planen” auf Seite 189.

Der Kanalinitiator gibt Nachrichten an das Jobprotokoll aus, wenn Kanäle gestartet und gestoppt werden. Die Automatisierung in Ihrem Unternehmen kann diese Nachrichten verwenden, um den Status zu erfassen. Da einige Kanäle für nur wenige Sekunden aktiv sind, können viele Nachrichten erzeugt werden. Sie können diese Nachrichten unterdrücken, indem Sie entweder die z/OS -Nachrichtenverarbeitungsfunktion verwenden oder indem Sie **EXCLMSG** mit dem Befehl SET SYSTEM festlegen.

IBM MQ-Kanaldefinitionen konfigurieren

Wenn viele WS-Manager miteinander verbunden sind, kann es schwierig sein, alle Objektdefinitionen zu verwalten. Dies kann durch IBM MQ-Clustering vereinfacht werden.

Sie geben zwei WS-Manager als vollständige Repositorys an. Andere Warteschlangenmanager benötigen eine Verbindung zu einem der Repositorys und eine Verbindung von. Wenn Verbindungen zu anderen Warteschlangenmanagern benötigt werden, erstellt und startet der Warteschlangenmanager Kanäle automatisch.

Wenn Sie planen, eine große Anzahl von Warteschlangenmanagern in einem Cluster zu haben, sollten Sie planen, Warteschlangenmanager als dedizierte Repositorys zu verwenden und keinen Anwendungsdatenverkehr zu haben.

Weitere Informationen finden Sie unter „Verteilte Warteschlangen und Cluster planen” auf Seite 21.

Aktionen vor der Konfiguration des Kanalinitiators

1. Entscheiden Sie, ob Sie TCP/IP oder APPC verwenden.
2. Wenn Sie TCP verwenden, ordnen Sie mindestens einen Port für IBM MQ zu.
3. Wenn Sie einen DNS-Server benötigen, konfigurieren Sie den Server, falls erforderlich, hoch verfügbar.
4. Wenn Sie APPC verwenden, ordnen Sie einen LU-Namen zu, und konfigurieren Sie APPC.

Aktionen, nachdem Sie den Kanalinitiator konfiguriert haben, bevor Sie in die Produktion gehen

1. Planen Sie die Verbindungen, die Sie haben:

a. Clientverbindungen von fernen Anwendungen.

b. MCA-Kanäle zu und von anderen Warteschlangenmanagern. In der Regel verfügen Sie über einen Kanal zu und von jedem fernen Warteschlangenmanager.

2. Richten Sie Clustering ein oder schließen Sie eine vorhandene Clustering-Umgebung an.
3. Überlegen Sie, ob Sie mehrere TCP-Stacks, VIPA oder einen externen Router für die Verfügbarkeit vor dem Kanalinitiator verwenden müssen.
4. Wenn Sie TLS planen, gehen Sie wie folgt vor:

   a. Konfigurieren Sie den Schlüsselring.

   b. Zertifikate konfigurieren

5. Gehen Sie wie folgt vor, wenn Sie die Kanalauthentifizierung planen:

   a. Festlegen der Kriterien für die Zuordnung eingehender Sitzungen zu MCA-Benutzer-IDs

   b. Aktivieren Sie die Funktion Reverse-DNS-Lookup, indem Sie den Warteschlangenmanagerparameter **REVDNS** entsprechend festlegen.

   c. Überprüfen Sie die Sicherheit. Löschen Sie z. B. die Standardkanäle, und geben Sie Benutzer-IDs mit nur der erforderlichen Berechtigung im Attribut **MCAUSER** für einen Kanal an.

6. Erfassen Sie die Accounting-und Statistikdaten-SMF-Datensätze, die von dem Kanalinitiator erstellt wurden, und veröffentlichen Sie sie.
7. Automatisieren Sie die Überwachung von Jobprotokollnachrichten.
8. Optimieren Sie bei Bedarf die Netzumgebung, um den Durchsatz zu verbessern. Mit TCP verbessern große Sende-und Empfangspuffer den Durchsatz. Sie können MQ erzwingen, dass bestimmte TCP-Puffergrößen mit den folgenden Befehlen verwendet werden:

   ```
   RECOVER QMGR(TUNE CHINTCPRBDYNSZ nnnnn)
   RECOVER QMGR(TUNE CHINTCPSBDYNSZ nnnnn)
   ```

   die die Kanäle SO_RCVBUF und SO_SNDBUF für die Kanäle auf die Größe in Byte setzen, die in nnnnn angegeben ist.

Zugehörige Konzepte

„Planung des Warteschlangenmanagers” auf Seite 157
Wenn Sie einen Warteschlangenmanager einrichten, sollte Ihre Planung die Entwicklung des WS-Managers ermöglichen, damit der Warteschlangenmanager die Anforderungen Ihres Unternehmens erfüllt.

z/OS SMF-Daten des Kanalinitiators planen

Sie müssen die Implementierung der Erfassung von SMF-Daten für den Kanalinitiator planen.

Der Kanalinitiator erzeugt zwei Typen von Satz:

- Statistikdaten mit Informationen zum Kanalinitiator und zu den Tasks, die in ihm ausgeführt werden.
- Kanalabrechnungsdaten mit Informationen, die dem Befehl DISPLAY CHSTATUS ähneln.

Die Erfassung von Statistikdaten wird mit dem folgenden Befehl gestartet:

```
START TRACE(STAT) CLASS(4)
```

und stoppen Sie ihn mit dem folgenden Befehl:

```
STOP TRACE(STAT) CLASS(4)
```

Abrechnungsdaten werden mit dem folgenden Befehl erfasst:

```
START TRACE(ACCTG) CLASS(4)
```

und stoppen Sie ihn mit dem folgenden Befehl:

```
STOP TRACE(ACCTG) CLASS(4)
```

Sie können steuern, für welche Kanäle Abrechnungsdaten erfasst werden, die für die Verwendung des Attributs **STATCHL** in der Kanaldefinition oder in dem Warteschlangenmanager erfasst werden.

- Für Clientkanäle müssen Sie **STATCHL** auf der WS-Managerebene festlegen.
- Für automatisch definierte Clustersenderkanäle können Sie die Erfassung von Abrechnungsdaten mit dem WS-Manager-Attribut **STATACLS** steuern.

Der Standardwert für **STATCHL** für den Warteschlangenmanager ist OFF . Um Kanalabrechnungsdaten erfassen zu können, müssen Sie zusätzlich zum Abrechnungs-Trace der Klasse 4 den Wert von **STATCHL** aus dem Standardwert in der WS-Manager-oder Kanaldefinition ändern.

Die SMF-Datensätze werden erstellt, wenn:

- LTS Von IBM MQ for z/OS 9.2.0 zu 9.2.3 der Zeitintervall, dass durch den CSQ6SYSP **STATIME** Parameter angegeben wurde, ist verstrichen oder **STATIME** ist Null auf dem Datenerfassungsbroadcast. Die Anforderungen zum Erfassen von SMF-Daten für den Kanalinitiator und den Warteschlangenmanager wird synchronisiert.
- V 9.2.4 Von IBM MQ for z/OS 9.2.4 an ist der Zeitintervall, angegeben durch die CSQ6SYSP **STATIME** oder **ACCTIME** Parameter abgelaufen oder, wenn **STATIME** oder **ACCTIME** gleich null ist auf dem SMF Datenerfassungsbroadcast. Die Anforderungen zum Erfassen von SMF-Daten für den Kanalinitiator und den Warteschlangenmanager wird synchronisiert.
- Ein STOP TRACE(ACCTG) CLASS(4)- oder STOP TRACE(STAT) CLASS(4)-Befehl wird ausgegeben oder
- Der Kanalinitiator wird heruntergefahren. An diesem Punkt werden alle SMF-Daten geschrieben.

Wenn ein Kanal während des SMF-Intervalls gestoppt wird, werden die Abrechnungsdaten beim nächsten SMF-Verarbeitungslauf in SMF geschrieben. Wenn ein Client eine Verbindung herstellt, einige Arbeiten und die Verbindung trennt, dann die Verbindung herstellt und die Verbindung trennt, werden zwei Sätze von Kanalabrechnungsdaten erzeugt.

Die Statistikdaten passen normalerweise in einen SMF-Datensatz, es können jedoch mehrere SMF-Datensätze erstellt werden, wenn eine große Anzahl von Tasks im Gebrauch ist.

Abrechnungsdaten werden für jeden Kanal erfasst, für den sie aktiviert ist, und passt normalerweise in einen SMF-Datensatz. Es können jedoch mehrere SMF-Datensätze erstellt werden, wenn eine große Anzahl an Kanälen aktiv ist.

Die Kosten für die Erfassung der SMF-Daten des Kanalinitiators sind gering. Der Anstieg der CPU-Belastung ist in der Regel unter ein paar Prozent und häufig innerhalb des Messfehlers.

Bevor Sie diese Funktion verwenden, müssen Sie sich mit dem zuständigen z/OS-Systemprogrammierer abstimmen, um sicherzustellen, dass SMF über genügend Kapazität für die zusätzlichen Datensätze verfügt und dass die Prozesse dahingehend angepasst werden, dass bei der Extraktion der SMF-Datensätze die neuen SMF-Daten eingeschlossen werden.

Für Kanalinitiatorstatistikdaten ist der SMF-Satztyp 115 und sub-type 231.

Für die Kanalinitiatorabrechnungsdaten ist der SMF-Satztyp 116 und der Subtyp 10.

Sie können eigene Programme schreiben, um diese Daten zu verarbeiten, oder verwenden Sie das SupportPac MP1B , das ein Programm, MQSMF, zum Drucken der Daten und zum Erstellen von Daten im CSV-Format (Comma Separated Values) enthält, die für den Import in eine ausgebreite Tabelle geeignet sind.

Wenn Sie Probleme mit dem Erfassen von SMF-Daten des Kanalinitiators haben, lesen Sie die Informationen im Abschnitt Probleme beim Erfassen von SMF-Daten für den Kanalinitiator (CHINIT) für weitere Informationen.

Zugehörige Tasks

IBM MQ-Leistungsstatistik interpretieren

Fehlerbehebung für Kanalabrechnungsdaten

z/OS TCP/IP-Umgebung unter z/OS planen

Um den besten Durchsatz über Ihr Netz zu erhalten, müssen Sie TCP/IP-Sende-und -Empfangspuffer mit einer Größe von 64 KB oder mehr verwenden. Mit dieser Größe optimiert das System seine Puffergrößen.

Siehe What is Dynamic Right Sizing for High Latency Networks? weitere Informationen hierzu.

Sie können die Größe des Systempuffers überprüfen, indem Sie den folgenden Netstat-Befehl verwenden. Beispiel:

```
TSO NETSTAT ALL (CLIENT csq1CHIN
```

In den Ergebnissen werden viele Informationen angezeigt, einschließlich der folgenden beiden Werte:

```
ReceiveBufferSize: 0000065536
SendBufferSize: 0000065536
```

65536 ist 64 KB. Wenn Ihre Puffergrößen kleiner als 65536 sind, müssen Sie mit Ihrem Netzwerkteam zusammenarbeiten, um die Werte für **TCPSENDBFRSIZE** und **TCPRCVBUFRSIZE** in der `PROFILE DDName` in der TCP/IP-Prozedur zu erhöhen. Sie können z. B. den folgenden Befehl verwenden:

```
TCPCONFIG TCPSENDBFRSZE 65536 TCPRCVBUFRSIZE 65536
```

Wenn Sie die systemweiten Einstellungen für **TCPSENDBFRSIZE** oder **TCPRCVBUFRSIZE** nicht ändern können, wenden Sie sich an das IBM Software Support Center.

z/OS Gruppe mit gemeinsamer Warteschlange planen (QSG)

Die einfachste Möglichkeit, eine gemeinsam genutzte Warteschlangenumgebung zu implementieren, besteht darin, einen Warteschlangenmanager zu konfigurieren, den WS-Manager zu einer QSG hinzuzufügen und anschließend weitere Warteschlangenmanager zu der Gruppe mit gemeinsamer Warteschlange hinzuzufügen.

Eine Gruppe mit gemeinsamer Warteschlange speichert die Konfigurationsinformationen in Db2-Tabellen. Es gibt eine Gruppe von Tabellen, auf die alle Gruppen mit gemeinsamer Warteschlange (QSG) zugreifen, die dieselbe Gruppe mit gemeinsamer Nutzung der Db2-Daten verwenden.

Gemeinsam genutzte Warteschlangennachrichten werden in einer Struktur in einer Coupling Facility (CF) gespeichert. Jede QSG verfügt über eine eigene Gruppe von CF-Strukturen. Sie müssen die Strukturen so konfigurieren, dass sie Ihren Anforderungen entsprechen.

Nachrichten können auch in gemeinsam genutzten Nachrichtendatengruppen (Shared Message Data Sets, SMDS) gespeichert werden. Nachricht mit einer Größe von mehr als 63 KB kann nicht in der CF gespeichert werden. Sie müssen SMDS verwenden, um diese Nachrichten in gemeinsam genutzten Warteschlangen zu speichern.

Nachrichtenprofile und Kapazitätsplanung

Sie sollten das Nachrichtenprofil Ihrer gemeinsam genutzten Warteschlangennachrichten verstehen. Im Folgenden finden Sie Beispiele für Faktoren, die Sie berücksichtigen müssen:

- Durchschnittliche und maximale Nachrichtenlänge
- Die typische Länge der Warteschlangenlänge und die Länge der Ausnahmewarteschlange. Beispiel: Sie müssen möglicherweise genügend Kapazität haben, um Nachrichten für einen ganzen Tag zu halten, und die typische Warteschlangenlänge unter 100 Nachrichten.

Wenn sich das Nachrichtenprofil ändert, können Sie die Größe der Strukturen erhöhen oder SMDS zu einem späteren Zeitpunkt implementieren.

Wenn Sie die Möglichkeit haben möchten, eine hohe Spitzenauslastung mit Nachrichten zu verarbeiten, können Sie IBM MQ so konfigurieren, dass Nachrichten an SMDS ausgelagert werden, wenn die Auslastung der Struktur die benutzerdefinierten Grenzwerte erreicht.

Sie müssen entscheiden, ob die CF-Strukturen duplexverwendet werden sollen. Dies wird durch die CF-Strukturdefinition in der CFRM-Richtlinie gesteuert:

1. Eine duplizierte Struktur verwendet zwei Coupling-Facilities. Wenn bei einem CF ein Fehler auftritt, wird der Service nicht unterbrochen, und die Struktur kann auf einem dritten CF wiederhergestellt werden, falls ein Fehler verfügbar ist. Duplizierte Strukturen können die Leistung von Operationen in gemeinsam genutzten Warteschlangen erheblich beeinflussen.
2. Wenn die Struktur nicht dupliziert wird, bedeutet ein Problem mit der CF, dass gemeinsam genutzte Warteschlangen auf Strukturen in dieser CF nicht mehr verfügbar werden, bis die Struktur in einer anderen CF wiederhergestellt werden kann.

   IBM MQ kann so konfiguriert werden, dass in diesem Fall die Strukturen automatisch in einer anderen CF erneut erstellt werden. Persistente Nachrichten werden aus den Protokollen der WS-Manager wiederhergestellt.

Beachten Sie, dass es leicht ist, die CF-Definitionen zu ändern.

Sie können eine Struktur so definieren, dass sie nur nicht persistente Nachrichten enthalten kann, oder so dass sie persistente und nicht persistente Nachrichten enthalten kann.

Strukturen, die persistente Nachrichten enthalten können, müssen in regelmäßigen Abständen gesichert werden. Sichern Sie Ihre CF-Strukturen mindestens jede Stunde, um die Zeit zu minimieren, die für die Wiederherstellung der Struktur im Falle eines Fehlers benötigt wird. Die Sicherung wird in der Protokolldatengruppe des Warteschlangenmanagers gespeichert, der die Sicherung ausführt.

Wenn Sie einen hohen Durchsatz von Nachrichten in Ihren gemeinsam genutzten Warteschlangen erwarten, ist es am besten, wenn ein dedizierter Warteschlangenmanager für die Sicherung der CF-Strukturen vorhanden ist. Dadurch wird die Zeit reduziert, die für die Wiederherstellung der Strukturen benötigt wird, da weniger Daten aus WS-Manager-Protokollen gelesen werden müssen.

Kanäle

Um ein einzelnes Systemimage für Anwendungen bereitzustellen, die eine Verbindung zu einer Gruppe mit gemeinsamer IBM MQ-Warteschlange haben, können Sie gemeinsame Eingabekanäle definieren. Wenn diese konfiguriert werden, kann eine Verbindung, die in die Gruppe mit gemeinsamer Warteschlange eingeht, zu jedem WS-Manager in der QSG wechseln.

Möglicherweise müssen Sie für diese Kanäle einen Netzrouter oder eine virtuelle IP-Adresse (VIPA) konfigurieren.

Sie können gemeinsam genutzte Ausgabekanäle definieren. Eine gemeinsam genutzte Ausgabekanalinstanz kann von jedem WS-Manager in der QSG aus gestartet werden.

Weitere Informationen finden Sie unter Gemeinsam genutzte Kanäle.

Sicherheit

Sie können IBM MQ-Ressourcen mithilfe eines externen Sicherheitsmanagers schützen. Bei Verwendung von RACF erhalten die RACF-Profile den Warteschlangenmanagernamen als Präfix. Beispiel: Eine Warteschlange mit dem Namen APPLICATION.INPUT würde unter Verwendung eines Profils in der Klasse MQQUEUE mit dem Namen `qmgrName.APPLICATION.INPUT.` geschützt.

Wenn Sie eine Gruppe mit gemeinsamer Warteschlange verwenden, können Sie weiterhin Ressourcen mit Profilen schützen, die dem Namen des Warteschlangenmanagers vorangestellt sind, oder Sie können Profile mit dem Namen der Gruppe mit gemeinsamer Warteschlange voranstellen. Beispiel: `qsgName.APPLICATION.INPUT`.

Sie sollten das Profile-Präfix mit dem Namen der Gruppe mit gemeinsamer Warteschlange verwenden, da dies bedeutet, dass es eine einzige Definition für alle Warteschlangenmanager gibt, wodurch Sie die Arbeit speichern und eine Diskrepanz bei den Definitionen zwischen den Warteschlangenmanagern verhindern.

Zugehörige Konzepte

„Planung des Warteschlangenmanagers" auf Seite 157
Wenn Sie einen Warteschlangenmanager einrichten, sollte Ihre Planung die Entwicklung des WS-Managers ermöglichen, damit der Warteschlangenmanager die Anforderungen Ihres Unternehmens erfüllt.

z/OS Planen der Coupling-Facility und der Auslagerung der Speicherumgebung

Dieses Thema enthält Informationen für die Planung der Anfangsgrößen und -formate der CF-Strukturen (CF = Coupling Facility) sowie der Umgebung für gemeinsam genutzte Nachrichtendateien (SMDS) oder für Db2.

Dieser Abschnitt enthält Informationen zu den folgenden Themen:

Coupling-Facility-Ressourcen definieren

Wenn gemeinsam genutzte Warteschlangen verwendet werden sollen, müssen Sie die Coupling-Facility-Strukturen definieren, die IBM MQ in Ihrer CFRM-Richtlinie (Coupling Facility Resource Management) verwenden soll. Dazu müssen Sie zuerst Ihre CFRM-Richtlinie mit Informationen zu den Strukturen aktualisieren und dann die Richtlinie aktivieren.

Ihre Installation verfügt wahrscheinlich über eine vorhandene CFRM-Richtlinie, in der die verfügbaren Coupling-Facilitys beschrieben werden. Das Dienstprogramm für Verwaltungsdaten wird verwendet, um den Inhalt der Richtlinie auf der Basis der von Ihnen angegebenen Textanweisungen zu ändern. Sie müssen der Richtlinie Anweisungen hinzufügen, in denen die Namen der neuen Strukturen, die Coupling-Facilitys, in denen sie definiert sind, und die Größe der Strukturen definiert sind.

Die CFRM-Richtlinie bestimmt außerdem, ob die IBM MQ-Strukturen dupliziert werden und wie sie in Fehlerszenarios neu zugeordnet werden. Wiederherstellung der gemeinsam genutzten Warteschlange enthält Empfehlungen zum Konfigurieren von CFRM für Ausfallsicherheit bei Fehlern, die sich auf die Coupling-Facility auswirken.

Auslagerung der Speicherumgebung festlegen

Die Nachrichtendaten für gemeinsam genutzte Warteschlangen können aus der Coupling-Facility ausgelagert und entweder in einer Db2-Tabelle oder in einer von IBM MQ verwalteten Datei, die als *gemeinsam genutzte Nachrichtendatei* (Shared Message Data Set, SMDS) bezeichnet wird, gespeichert werden. Nachrichten, die zu groß sind, um in der Coupling-Facility gespeichert zu werden (d. h. größer als 63 KB), müssen immer ausgelagert werden. Kleinere Nachrichten können optional ausgelagert werden, um die Speicherbelegung der Coupling-Facility zu verringern.

Weitere Informationen finden Sie unter Offload-Optionen für gemeinsam genutzte Nachrichten angeben.

Strukturen planen

Für eine Gruppe mit gemeinsamer Warteschlange (Queue Sharing Group, QSG) müssen mindestens zwei Strukturen definiert werden. Mit der ersten Struktur, die als Verwaltungsstruktur bezeichnet wird, wird die interne IBM MQ-Aktivität in der Gruppe mit gemeinsamer Warteschlange koordiniert. In dieser Struktur sind keine Benutzerdaten enthalten. Sie hat den festgelegten Namen *Name_der_QSG*CSQ_ADMIN (dabei ist *Name_der_QSG* der Name Ihrer Gruppe mit gemeinsamer Warteschlange). Nachfolgende Strukturen werden als Anwendungsstrukturen bezeichnet und zum Speichern der Nachrichten in gemeinsam genutzten IBM MQ -Warteschlangen verwendet. Jede Struktur kann bis zu 512 gemeinsam genutzte Warteschlangen aufnehmen.

Eine Anwendungsstruktur mit der Bezeichnung *Name_der_QSG*CSQSYSAPPL wird für Systemwarteschlangen verwendet. Die Definition dieser Struktur ist optional, sie ist aber für bestimmte Funktionen erforderlich. Standardmäßig sind die Warteschlangen SYSTEM.QSG.CHANNEL.SYNCQ und SYSTEM.QSG.UR.RESOLUTION.QUEUE in der Struktur *Name_der_QSG*CSQSYAPPL definiert.

Mehrere Strukturen verwenden

Eine Gruppe mit gemeinsamer Warteschlange kann Verbindungen mit bis zu 64 Coupling Facility-Strukturen herstellen. Eine dieser Strukturen muss die Verwaltungsstruktur sein. Wenn diese definiert ist, kann *Name_der_QSG*CSQSYSAPPL eine der anderen Strukturen sein. Sie können bis zu 63 Strukturen (62, wenn *Name_der_QSG*CSQSYSAPPL definiert ist) für Nachrichtendaten verwenden. Sie können mehrere Anwendungsstrukturen in einer der folgenden Situationen auswählen:

- Sie verfügen über einige Warteschlangen, die wahrscheinlich eine große Anzahl an Nachrichten enthalten, und erfordern daher alle Ressourcen einer gesamten Coupling-Facility.
- Sie müssen eine große Anzahl gemeinsam genutzter Warteschlangen verwenden, sodass sie auf mehrere Strukturen verteilt werden müssen, da jede Struktur nur 512 Warteschlangen enthalten kann.
- In RMF-Berichten zu den Nutzungsmerkmalen einer Struktur wird die Verteilung der darin enthaltenen Warteschlangen auf eine Reihe von Coupling-Facilitys empfohlen.
- Sie möchten, dass einige Warteschlangendaten aus anderen Warteschlangendaten aus Gründen der Datenisolation in einer physisch unterschiedlichen Coupling-Facility gehalten werden.
- Die Wiederherstellung persistenter gemeinsam genutzter Nachrichten wird unter Verwendung von Attributen und Befehlen auf Strukturebene ausgeführt, z. B. BACKUP CFSTRUCT. Um die Sicherung und Wiederherstellung zu vereinfachen, können Sie Warteschlangen, die nicht persistente Nachrichten enthalten, anderen Strukturen von diesen Strukturen zuordnen, die persistente Nachrichten enthalten.

Bei der Entscheidung, in welchen Coupling-Facilitys die Strukturen zugeordnet werden sollen, beachten Sie die folgenden Punkte:

- Ihre Datenisolationsanforderungen.
- Die Flüchtigkeit der Coupling Facility (d. a. ihre Fähigkeit, Daten über einen Stromausfall zu erhalten).
- Ausfallunabhängigkeit zwischen dem zugreifenden System und der Coupling-Facility oder zwischen Coupling-Facilitys.
- Die Stufe des CFCC (Coupling Facility Control Code), der auf der Coupling-Facility installiert ist (für IBM MQ ist Stufe 9 oder höher erforderlich).

Planen der Größe Ihrer Strukturen

Verwaltungsstruktur

Die Verwaltungsstruktur (*Name_der_QSG*CSQ_ADMIN) muss groß genug sein, um 1000 Listeneinträge für jeden Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange enthalten zu

können. Beim Start eines Warteschlangenmanagers wird die Struktur geprüft, um zu ermitteln, ob sie groß genug für die Anzahl der aktuell *definierten* Warteschlangenmanager für die Gruppe mit gemeinsamer Warteschlange ist. Warteschlangenmanager sind für die Gruppe mit gemeinsamer Warteschlange definiert, wenn sie mit dem Dienstprogramm CSQ5PQSG hinzugefügt wurden. Mit dem MQSC-Befehl DISPLAY GROUP können Sie prüfen, welche Warteschlangenmanager für die Gruppe definiert sind.

Anmerkung: Bei der Berechnung der Größe der Struktur sollten Sie zusätzlich zur Anzahl der Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange die Größe großer Arbeitseinheiten berücksichtigen.

In Tabelle 22 auf Seite 195 wird die erforderliche Mindestgröße der Verwaltungsstruktur für eine unterschiedliche Anzahl an Warteschlangenmanagern angezeigt, die in der Gruppe mit gemeinsamer Warteschlange definiert sind. Diese Größen wurden für eine Coupling Facility-Struktur der CFCC-Stufe 14 festgelegt; für höhere Stufen von CFCC müssen sie wahrscheinlich größer sein.

Tabelle 22. Mindestgröße der Verwaltungsstruktur

Anzahl der Warteschlangenmanager, die in der Gruppe mit gemeinsamer Warteschlange definiert sind	**Erforderlicher Speicher**
1	6144 KB
2	6912 KB
3	7976 KB
4	8704 KB
5	9728 KB
6	10496 KB
7	11520 KB
8	12288 KB
9	13056 KB
10	14080 KB
11	14848 KB
12	15616 KB
13	16640 KB
14	17408 KB
15	18176 KB
16	19200 KB
17	19968 KB
18	20736 KB
19.	21760 KB
20	22528 KB
21	23296 KB
22	24320 KB
23	25088 KB
24	25856 KB

Tabelle 22. Mindestgröße der Verwaltungsstruktur (Forts.)	
Anzahl der Warteschlangenmanager, die in der Gruppe mit gemeinsamer Warteschlange definiert sind	**Erforderlicher Speicher**
25	27136 KB
26	27904 KB
27	28672 KB
28	29696 KB
29	30464 KB
30	31232 KB
31	32256 KB

Wenn Sie einen Warteschlangenmanager einer vorhandenen Gruppe mit gemeinsamer Warteschlange hinzufügen, hat der Speicherbedarf möglicherweise die in Tabelle 22 auf Seite 195 empfohlene Größe überschritten. Ist dies der Fall, verwenden Sie die folgende Prozedur, um den erforderlichen Speicher für die Struktur *Name_der_QSG*CSQ_ADMIN zu schätzen:

1. Geben Sie den MQSC-Befehl **DISPLAY CFSTATUS(CSQ_ADMIN)** für ein vorhandenes Mitglied der Gruppe mit gemeinsamer Warteschlange aus.
2. Extrahieren Sie die ENTSMAX-Informationen für die CSQ_ADMIN-Struktur.
3. Wenn diese Zahl kleiner ist als 1000-mal die Gesamtzahl der Warteschlangenmanager, die Sie in der Gruppe mit gemeinsamer Warteschlange definieren möchten, erhöhen Sie die Größe der Struktur.

Anwendungsstrukturen

Die Größe der Anwendungsstruktur, die für die Aufnahme von IBM MQ-Nachrichten erforderlich ist, hängt von der voraussichtlichen Anzahl und Größe der Nachrichten ab, die gleichzeitig in einer Struktur enthalten sein sollen.

Das Diagramm in Abbildung 42 auf Seite 197 zeigt, wie groß die Coupling-Facility-Strukturen sein sollten, um die Nachrichten in den gemeinsam genutzten Warteschlangen speichern zu können. Für die Berechnung der Zuordnungsgröße benötigen Sie die folgenden Informationen:

- Die Durchschnittsgröße der Nachrichten in Ihren Warteschlangen.
- Die Gesamtzahl der Nachrichten, die voraussichtlich in der Struktur gespeichert werden.

Suchen Sie die Anzahl der Nachrichten entlang der horizontalen Achse. Wählen Sie die Kurve aus, die Ihrer Nachrichtengröße entspricht, und bestimmen Sie den erforderlichen Wert aus der vertikalen Achse. Beispiel: Bei 200.000 Nachrichten mit einer Länge von 1 KB ergibt sich ein Wert zwischen 256 und 512 MB.

In Tabelle 23 auf Seite 197 werden dieselben Informationen in tabellarischer Form bereitgestellt.

Abbildung 42. Berechnen der Größe einer Coupling-Facility-Struktur

Verwenden Sie diese Tabelle, um zu berechnen, wie groß die Coupling Facility-Strukturen sind:

Tabelle 23. Berechnen der Größe einer Coupling-Facility-Struktur

Anzahl der Nachrichten	**1 KB**	**2 KB**	**4 KB**	**8 KB**	**16 KB**	**32 KB**	**63 KB**
100	6 MB	6 MB	7 MB	7 MB	8 MB	10 MB	14 MB
1000	8 MB	9 MB	12 MB	17 MB	27 MB	48 MB	88 MB
10000	25 MB	38 MB	64 MB	115 MB	218 MB	423 MB	821 MB
100000	199 MB	327 MB	584 MB	1097 MB	2124 MB	4177 MB	8156 MB

Ihre CFRM-Richtlinie muss die folgenden Anweisungen enthalten:

- `INITSIZE` ist die Größe in KB, mit der die Struktur zugeordnet wird, wenn der erste Warteschlangenmanager eine Verbindung herstellt.
- `SIZE` ist die maximale Größe, die die Struktur erreichen kann.
- `FULLTHRESHOLD` legt den Prozentwert für den Schwellenwert fest, an dem z/OS die Nachricht IXC585E ausgibt, in der angezeigt wird, dass die Struktur fast voll ist.

Ein bewährstes Verfahren ist, sicherzustellen, dass INITSIZE und SIZE innerhalb eines Faktors von 2 sind. Beispielsweise können Sie mit den zuvor ermittelten Werten die folgenden Anweisungen in die folgenden Angaben aufnehmen:

```
STRUCTURE NAME(structure-name)
INITSIZE(value from graph in KB, that is, multiplied by 1024)
SIZE(something larger)
FULLTHRESHOLD(85)
```

```
STRUCTURE NAME(QSG1APPLICATION1)
INITSIZE(262144) /* 256 MB */
SIZE(524288)     /* 512 MB */
FULLTHRESHOLD(85)
```

Wenn die Strukturverwendung den Schwellenwert erreicht, in dem Warnungen ausgegeben werden, ist ein Eingriff erforderlich. Sie können IBM MQ verwenden, um MQPUT-Operationen in einigen Warteschlangen in der Struktur zu blockieren, um Anwendungen daran zu hindern, weitere Nachrichten zu schreiben, um weitere Anwendungen zum Abrufen von Nachrichten aus den Warteschlangen zu starten oder um einige Anwendungen, die Nachrichten in die Warteschlange einreihen, in den Wartemodus (Quiesce) zu versetzen.

Alternativ können Sie mit z/OS-Funktionen die Strukturgröße direkt an der Stelle verändern. Führen Sie folgenden z/OS-Befehl aus:

```
SETXCF START,ALTER,STRNAME=structure-name,SIZE=newsize
```

Ändert die Größe der Struktur in *newsize*, wobei *newsize* ein Wert ist, der kleiner als der Wert von SIZE ist, der in der CFRM-Richtlinie für die Struktur angegeben ist, aber größer als die aktuelle Coupling-Facility-Größe ist.

Sie können die Verwendung der Coupling-Facility-Struktur mit dem MQSC-Befehl DISPLAY CFSTATUS überwachen.

Wenn keine Aktion ausgeführt wird und eine Warteschlangenstruktur voll ist, wird ein MQRC_STORAGE_MEDIUM_FULL-Rückkehrcode an die Anwendung zurückgegeben. Wenn die Verwaltungsstruktur voll wird, hängen die genauen Symptome davon ab, welche Prozesse den Fehler erfahren, aber sie können die folgenden Probleme enthalten:

- Keine Antworten auf Befehle.
- Der Warteschlangenmanager ist aufgrund von Problemen während der COMMIT-Verarbeitung fehlgeschlagen.

Die Struktur CSQSYSAPPL

Die Struktur *Name_der_QSG*CSQSYSAPPL ist eine Anwendungsstruktur für Systemwarteschlangen. In Tabelle 3 finden Sie ein Beispiel für die Schätzung der Nachrichtendatengröße für die Standardwarteschlangen, die in der Struktur *Name_der_QSG*CSQSYSAPPL definiert sind.

Tabelle 24. Tabelle, die die CSQSYSAPPL-Verwendung für die Dimensionierung zeigt.

***qsg-name* CSQSYSAPPL-Verwendung**	**Größe**
SYSTEM.QSG.CHANNEL.SYNCQ	2 Nachrichten mit einer Länge von 500 Byte pro aktive Instanz eines gemeinsam genutzten Kanals
SYSTEM.QSG.UR.RESOLUTION.QUEUE	1000 Nachrichten von 2 KB

Die vorgeschlagenen Anfangswerte für die Strukturdefinition lauten wie folgt:

```
STRUCTURE NAME(qsg-nameCSQSYSAPPL)
INITSIZE(20480)        /* 20 MB */
```

```
SIZE(30720)            /* 30 MB */
FULLTHRESHOLD(85)
```

Diese Werte können abhängig von der Verwendung gemeinsam genutzter Kanäle und Gruppeneinheiten der Wiederherstellung angepasst werden.

Gemeinsam genutzte Warteschlangen zu Strukturen zuordnen

Definieren Sie eine Anwendungsstruktur für IBM MQ mit dem Befehl DEFINE CFSTRUCT. Schließen Sie beim Definieren einer Struktur für IBM MQ das Präfix für den Namen der Gruppe mit gemeinsamer Warteschlange nicht in den Strukturnamen ein. Wenn Sie beispielsweise eine Anwendungsstruktur für IBM MQ definieren, die in der CFRM-Richtlinie die Bezeichnung *Name_der_QSG*APPLICATION1 hat, geben Sie den folgenden Befehl aus:

```
DEFINE CFSTRUCT(APPLICATION1)
```

Das Attribut CFSTRUCT der Warteschlangendefinition wird zum Zuordnen der Warteschlange zu einer Struktur verwendet. Geben Sie den Namen der CF-Struktur ohne das Präfix für den Namen der Gruppe mit gemeinsamer Warteschlange in diesem Attribut an. Beispielsweise definiert der folgende Befehl eine gemeinsam genutzte Warteschlange in der Struktur APPLICATION1:

```
DEFINE QLOCAL(myqueue) QSGDISP(SHARED) CFSTRUCT(APPLICATION1)
```

z/OS *SMDS-Umgebung (SMDS = Shared Message Data Set) planen*

Wenn Sie eine Gruppe mit gemeinsamer Warteschlange mit SMDS-Auslagerung verwenden, muss IBM MQ eine Verbindung zu einer Gruppe mit gemeinsam genutzten Nachrichtendateien herstellen. In diesem Abschnitt finden Sie Informationen zu den Datasetanforderungen und zur Konfiguration, die zum Speichern von IBM MQ-Nachrichtendaten erforderlich ist.

Eine *gemeinsam genutzte Nachrichtendatei* (beschrieben durch das Schlüsselwort SMDS) ist eine Datei, die von einem Warteschlangenmanager verwendet wird, um ausgelagerte Nachrichtendaten für gemeinsam genutzte Nachrichten zu speichern, die in einer Coupling-Facility-Struktur gespeichert sind.

Anmerkung: Wenn Sie SMDS-Dateien für eine Struktur definieren, muss es für jeden Warteschlangenmanager eine Datei geben.

Wenn diese Form der Datenauslagerung aktiviert ist, ist für **CFSTRUCT** eine zugehörige Gruppe gemeinsam genutzter Nachrichtendateien erforderlich, eine Datei für jeden Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange. Die Gruppe der gemeinsam genutzten Nachrichtendateien wird für IBM MQ mit dem Parameter **DSGROUP** in der Definition **CFSTRUCT** festgelegt. Zusätzliche Parameter können verwendet werden, um weitere optionale Informationen zu liefern, wie z. B. die Anzahl der Puffer, die verwendet werden sollen, und Erweiterungsattribute für die Datensätze.

Jeder WS-Manager kann in die Datei schreiben, die er besitzt, um gemeinsam genutzte Nachrichtendaten für Nachrichten zu speichern, die über diesen Warteschlangenmanager geschrieben werden, und kann alle Datensätze in der Gruppe lesen.

Eine Liste, die den Status und die Attribute für jeden Datensatz beschreibt, der der Struktur zugeordnet ist, wird intern als Teil der Definition von **CFSTRUCT** verwaltet, sodass jeder WS-Manager die Definition überprüfen kann, um zu ermitteln, welche Datensätze derzeit verfügbar sind.

Diese Dateiinformationen können mit dem Befehl **DISPLAY CFSTATUS TYPE(SMDS)** angezeigt werden, um den aktuellen Status und die Verfügbarkeit anzuzeigen, und mit dem Befehl **DISPLAY SMDS** können die Parametereinstellungen für die Dateien angezeigt werden, die einem angegebenen **CFSTRUCT**zugeordnet sind.

Einzelne gemeinsam genutzte Nachrichtendatensätze werden durch die Kombination aus dem Namen des Eignungswarteschlangenmanagers (normalerweise unter Verwendung des Schlüsselworts **SMDS**) und dem Namen der **CFSTRUCT** -Struktur effektiv identifiziert.

In diesem Abschnitt werden die folgenden Themen beschrieben:

- Parameter "DSGROUP"
- Parameter "DSBLOCK"
- Merkmale gemeinsam genutzter Nachrichtendateien
- Speicherplatzverwaltung für gemeinsam genutzte Nachrichtendateien
- Zugriff auf gemeinsam genutzte Nachrichtendateien
- Gemeinsam genutzte Nachrichtendateien erstellen
- Überlegungen zur Leistung und Kapazität von gemeinsam genutzten Nachrichtendateien
- Gemeinsam genutzte Nachrichtendateien aktivieren

Weitere Informationen zu diesen Parametern finden Sie in DEFINE CFSTRUCT .

Weitere Informationen zum Verwalten Ihrer gemeinsam genutzten Nachrichtendateien finden Sie im Artikel Gemeinsam genutzte Nachrichtendateien verwalten.

Parameter DSGROUP

Der Parameter **DSGROUP** in der Definition **CFSTRUCT** gibt die Gruppe von Datensätzen an, in denen große Nachrichten für diese Struktur gespeichert werden sollen. Zusätzliche Parameter können verwendet werden, um die logische Blockgröße anzugeben, die für die Speicherbereichszuweisungszwecke und die Werte für die Pufferpoolgröße und die Optionen für die automatische Dateierweiterung verwendet werden soll.

Der Parameter **DSGROUP** muss konfiguriert werden, bevor die Ausladung in Datensätze aktiviert werden kann.

- Wenn ein neuer **CFSTRUCT** unter **CFLEVEL(5)** definiert wird und die Option **OFFLOAD(SMDS)** angegeben oder angenommen wird, muss der Parameter **DSGROUP** in demselben Befehl angegeben werden.
- Wenn ein vorhandener **CFSTRUCT** geändert wird, um den **CFLEVEL** auf **CFLEVEL(5)** zu erhöhen, und die Option **OFFLOAD(SMDS)** angegeben oder angenommen wird, muss der Parameter **DSGROUP** in demselben Befehl angegeben werden, wenn er noch nicht festgelegt ist.

Parameter DSBLOCK

Der Speicherbereich in jedem Datensatz wird als logische Blöcke einer festen Größe (normalerweise 256 KB), die mit dem Parameter **DSBLOCK** in der Definition **CFSTRUCT** angegeben wurde, als logische Blöcke zugeordnet, die dann einzelnen Nachrichten als Bereiche von Seiten von 4 KB zugeordnet werden (entsprechend der physischen Blockgröße und der Steuerintervallgröße) in jedem logischen Block. Die logische Blockgröße bestimmt auch die maximale Größe von Nachrichtendaten, die in einer einzelnen E/A-Operation gelesen oder geschrieben werden können, die mit der Puffergröße für den SMDS-Pufferpool identisch ist.

Ein größerer Wert des Parameters **DSBLOCK** kann die Leistung für sehr große Nachrichten verbessern, indem die Anzahl der separaten E/A-Operationen reduziert wird. Ein kleinerer Wert verringert jedoch die Größe des Pufferspeichers, der für jede aktive Anforderung erforderlich ist. Der Standardwert für den Parameter **DSBLOCK** ist 256 KB, wodurch ein angemessenes Gleichgewicht zwischen diesen Anforderungen bereitgestellt wird, sodass die Angabe dieses Parameters normalerweise nicht erforderlich sein könnte.

Merkmale der gemeinsam genutzten Nachrichtendatei

Ein gemeinsam genutzter Nachrichtensatz wird als lineare VSAM-Datei (LDS) definiert. Jede ausgelagerte Nachricht wird in einem oder mehreren Blöcken in der Datei gespeichert. Die gespeicherten Daten werden direkt durch Informationen in den Coupling Facility-Einträgen adressiert, wie eine erweiterte Form des virtuellen Speichers. Es gibt keinen separaten Index oder ähnliche Steuerinformationen, die in der Datei selbst gespeichert sind.

Das direkte Adressierungsschema bedeutet, dass für Nachrichten, die in einen Block passen, nur eine einzige E/A-Operation zum Lesen oder Schreiben des Blocks benötigt wird. Wenn eine Nachricht mehr als einen Block umfasst, können die E/A-Operationen für die einzelnen Blöcke vollständig überlappt werden, um die abgelaufene Zeit zu minimieren, vorausgesetzt, dass genügend Puffer verfügbar sind.

Die gemeinsam genutzte Nachrichtendatei enthält außerdem eine kleine Menge an allgemeinen Steuerinformationen, die aus einem Header auf der ersten Seite bestehen, die Informationen zum Wiederherstellungs-und Neustartstatus enthält, sowie einen Prüfpunktbereich für die Speicherbereichszuordnung, der zum Speichern der freien Blockspeicherbereichszuordnung bei normaler Beendigung des Warteschlangenmanagers verwendet wird.

Speicherverwaltung für gemeinsam genutzte Nachrichtendaten

Als Hintergrundinformationen zu Kapazität, Leistung und Betriebsüberlegungen kann es nützlich sein, die Konzepte zu verstehen, wie der Speicherbereich in gemeinsam genutzten Nachrichtendatengruppen von den Warteschlangenmanagern verwaltet wird.

Der freie Speicherbereich in den einzelnen gemeinsam genutzten Nachrichtendatensatzes wird von seinem Eigner-Warteschlangenmanager überwacht, der eine Speicherbereichszuordnung verwendet, die die Anzahl der Seiten angibt, die in jedem logischen Block verwendet werden. Die Speicherbereichszuordnung wird im Hauptspeicher verwaltet, während die Datei geöffnet und in der Datei gespeichert wird, wenn sie normal geschlossen wird. (In den Wiederherstellungssituationen wird die Speicherzuordnung automatisch wiederhergestellt, indem die Nachrichten in der Coupling-Facility-Struktur durchsucht werden, um zu ermitteln, welche Datenseiten momentan verwendet werden.)

Wenn eine gemeinsam genutzte Nachricht mit ausgelagerten Nachrichtendaten geschrieben wird, ordnet der Warteschlangenmanager einen Seitenbereich für jeden Nachrichtenblock zu. Wenn ein teilweise belegter aktueller logischer Block für die angegebene Warteschlange vorhanden ist, ordnet der Warteschlangenmanager Speicherplatz auf der nächsten freien Seite in diesem Block zu, andernfalls ordnet er einen neuen logischen Block zu. Wenn die gesamte Nachricht nicht in den aktuellen logischen Block passt, teilt der WS-Manager die Nachrichtendaten am Ende des logischen Blocks auf und ordnet einen neuen logischen Block für den nächsten Nachrichtenblock zu. Dies wird wiederholt, bis der Speicherbereich für die gesamte Nachricht zugeordnet wurde. Der nicht belegte Speicherbereich im letzten logischen Block wird als neuer aktueller logischer Block für die Warteschlange gespeichert. Wenn die Datei normal geschlossen wird, werden alle nicht verwendeten Seiten in den aktuellen logischen Blöcken an die Speicherbereichszuordnung zurückgegeben, bevor sie gespeichert werden.

Wenn eine gemeinsam genutzte Nachricht mit ausgelagerten Nachrichtendaten gelesen wurde und zum Löschen bereit ist, verarbeitet der Warteschlangenmanager die Löschanforderung, indem er den Coupling-Facility-Eintrag für die Nachricht in eine Bereinigungsliste überträgt, die vom Eigner-Warteschlangenmanager überwacht wird (der möglicherweise derselbe Warteschlangenmanager sein kann). Wenn Einträge in dieser Liste ankommen, liest und löscht der Eigner-WS-Manager die Einträge und gibt die freigegebenen Bereiche von Seiten an die Speicherbereichszuordnung zurück. Wenn alle verwendeten Seiten in einem logischen Block freigegeben wurden, steht der Block zur Wiederverwendung zur Verfügung.

Zugriff auf gemeinsam genutzte Nachrichtendatensätze

Jede gemeinsam genutzte Nachrichtendatei muss sich in einem gemeinsamen Direktzugriffsspeicher befinden, auf den alle Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange zugreifen können.

Während der normalen Ausführung öffnet jeder Warteschlangenmanager seine eigene gemeinsam genutzte Nachrichtendatei für den Schreib-/Lesezugriff und öffnet alle aktiven gemeinsam genutzten Nachrichtendatensätze für andere Warteschlangenmanager für schreibgeschützten Zugriff, so dass sie Nachrichten lesen kann, die von diesen Warteschlangenmanagern gespeichert werden. Dies bedeutet, dass jede Warteschlangenmanager-Benutzer-ID mindestens UPDATE-Zugriff auf ihre eigene gemeinsam genutzte Nachrichtendatei und Lesezugriff auf alle anderen gemeinsam genutzten Nachrichtendaten für die Struktur erfordert.

Wenn gemeinsam genutzte Nachrichtendateien mithilfe von **RECOVER CFSTRUCT** wiederhergestellt werden müssen, kann der Wiederherstellungsprozess auf jedem Warteschlangenmanager in der Gruppe mit

gemeinsamer Warteschlange ausgeführt werden. Ein Warteschlangenmanager, der zur Ausführung der Wiederherstellungsverarbeitung verwendet werden kann, erfordert UPDATE-Zugriff auf alle Datensätze, die er möglicherweise wiederherstellen muss.

Gemeinsam genutzte Nachrichtendatei erstellen

Jede gemeinsam genutzte Nachrichtendatei sollte normalerweise erstellt werden, bevor die entsprechende **CFSTRUCT** -Definition erstellt oder geändert wird, um die Verwendung dieser Form von Nachrichtenauslagern zu aktivieren, da die Änderungen der **CFSTRUCT** -Definition normalerweise sofort wirksam werden, und die Datei erforderlich ist, sobald ein Warteschlangenmanager versucht, auf eine gemeinsam genutzte Warteschlange zuzugreifen, die dieser Struktur zugeordnet wurde. In SCSQPROC (CSQ4SMDS) wird ein Beispieljob zum Zuordnen und Vorformatieren eines gemeinsam genutzten Nachrichtensatzes bereitgestellt. Der Job muss angepasst und ausgeführt werden, um für jeden Warteschlangenmanager, der einen CFSTRUCT mit OFFLOAD (SMDS) verwendet, eine gemeinsam genutzte Nachrichtengruppe zuzuordnen.

Wenn der Warteschlangenmanager feststellt, dass die Auslastungs-Unterstützung aktiviert wurde und versucht, seine gemeinsam genutzte Nachrichtendatei zu öffnen, die aber noch nicht erstellt wurde, wird die gemeinsam genutzte Nachrichtengruppe als nicht verfügbar markiert. Der Warteschlangenmanager kann dann keine großen Nachrichten speichern, bis die Datei erstellt wurde und der Warteschlangenmanager erneut benachrichtigt wurde, z. B. mit dem Befehl **START SMDSCONN** .

Eine gemeinsam genutzte Nachrichtendatei wird als lineare VSAM-Datei mit einem **DEFINE CLUSTER** -Befehl von Access Method Services erstellt. Die Definition muss **SHAREOPTIONS(2 3)** angeben, damit ein Warteschlangenmanager ihn für den Schreibzugriff öffnen kann und eine beliebige Anzahl von Warteschlangenmanagern ihn gleichzeitig lesen kann. Es muss die Standardgröße des Steuerintervalls von 4 KB verwendet werden. Wenn die Datei möglicherweise mehr als 4 GB erweitern muss, muss sie mit Hilfe einer SMS-Datenklasse definiert werden, die das VSAM-Attribut für die erweiterte Adressierbarkeit aufweist. Eine gemeinsam genutzte Nachrichtendatei kann sich im EAS-Teil (EAS = Extended Addressing Space) eines EAV (Extended Address Volumes) befinden.

Jede gemeinsam genutzte Nachrichtendatei kann vor ihrer ersten Verwendung entweder leer oder vorformatiert als binäre Nullen sein (mit **CSQJUFMT** oder einem ähnlichen Dienstprogramm wie dem Beispieljob SCSQPROC (CSQ4SMDS)). Wenn es leer ist oder nur teilweise formatiert ist, wenn es geöffnet wird, formatiert der Warteschlangenmanager den verbleibenden Speicherbereich automatisch in binäre Nullen.

Aspekte der Leistung und Kapazität von gemeinsam genutzten Nachrichtendatensatzes

Jede gemeinsam genutzte Nachrichtengruppe wird verwendet, um ausgelagerte Daten für gemeinsam genutzte Nachrichten zu speichern, die vom Eigner-WS-Manager in den zugehörigen **CFSTRUCT** geschrieben werden, von Regionen innerhalb desselben Systems. Die gespeicherten Daten für jede Nachricht enthalten einen Deskriptor (derzeit ca. 350 Byte), die Nachrichtenheader und den Nachrichtenhauptteil. Jede ausgelagerte Nachricht wird in einer oder mehreren Seiten (physische Blöcke mit einer Größe von 4 KB) in der Datei gespeichert.

Der für eine bestimmte Anzahl ausgelagerte Nachrichten erforderliche Datensatzspeicherbereich kann daher geschätzt werden, indem die Gesamtnachrichtengröße (einschließlich des Deskriptors) auf das nächste Vielfache von 4 KB aufgerundet und dann mit der Anzahl der Nachrichten multipliziert wird.

Wie bei einer Seitengruppe, wenn ein gemeinsam genutztes Nachrichtensatzes fast voll ist, kann es optional automatisch erweitert werden. Das Standardverhalten für diese automatische Erweiterung kann mit dem Parameter **DSEXPAND** in der Definition **CFSTRUCT** festgelegt werden. Diese Einstellung kann für jeden Warteschlangenmanager mit dem Parameter **DSEXPAND** im Befehl **ALTER SMDS** überschrieben werden. Die automatische Erweiterung wird ausgelöst, wenn der Datensatz 90% voll erreicht und mehr Speicherplatz benötigt wird. Wenn die Erweiterung zulässig ist, aber ein Erweiterungsversuch durch VSAM zurückgewiesen wird, da beim Definieren der Datei keine sekundäre Bereichszuordnung angegeben wurde, wird die Erweiterung mit einer sekundären Zuordnung von 20% der aktuellen Größe des Datensatzes erneut versucht.

Wenn die gemeinsam genutzte Nachrichtengruppe mit dem Attribut "Erweiterte Adressierbarkeit" definiert ist, wird die maximale Größe nur durch VSAM-Aspekte auf maximal 16 TB oder 59 Datenträger begrenzt. Dieser Wert ist erheblich größer als die maximale Größe einer lokalen Seitengruppe (64 GB).

Gemeinsam genutzte Nachrichtendatei aktivieren

Wenn ein Warteschlangenmanager erfolgreich eine Verbindung zu einer Struktur der Anwendungs-Coupling-Facility hergestellt hat, prüft er, ob diese Strukturdefinition die Ausladung unter Verwendung eines zugeordneten **DSGROUP** -Parameters angibt. Wenn dies der Fall ist, ordnet der Warteschlangenmanager seine eigene gemeinsam genutzte Nachrichtengruppe für den Schreibzugriff zu und öffnet für den Lesezugriff alle vorhandenen gemeinsam genutzten Nachrichtendatensätze, die anderen Warteschlangenmanagern gehören.

Wenn eine gemeinsam genutzte Nachrichtendatei das erste Mal geöffnet wird (bevor sie in der Gruppe mit gemeinsamer Warteschlange als aktiv erfasst wurde), enthält die erste Seite noch keinen gültigen Header. Der Warteschlangenmanager füllt die Headerinformationen aus, mit denen die Gruppe mit gemeinsamer Warteschlange, der Strukturname und der zugehörige Warteschlangenmanager angegeben wird.

Nach Abschluss des Headers registriert der Warteschlangenmanager die neue gemeinsam genutzte Nachrichtendatei als aktiv und sendet ein Ereignis, um alle anderen aktiven Warteschlangenmanager über den neuen Datensatz zu benachrichtigen.

Jedes Mal, wenn ein Warteschlangenmanager eine gemeinsam genutzte Nachrichtendatei öffnet, prüft er die Headerdaten, um sicherzustellen, dass die richtige Datei weiterhin verwendet wird und dass sie nicht beschädigt wurde.

z/OS *Db2-Umgebung planen*

Wenn Sie Gruppen mit gemeinsamer Warteschlange verwenden, muss IBM MQ eine Verbindung zu einem Db2-Subsystem herstellen, dass Mitglied einer Gruppe mit gemeinsamer Datennutzung ist. In diesem Abschnitt finden Sie Informationen zu den Db2-Anforderungen, die für die Aufnahme von IBM MQ-Daten erforderlich sind.

IBM MQ muss den Namen der Gruppe mit gemeinsamer Datennutzung kenne, zu der eine Verbindung hergestellt werden soll, und den Namen eines Db2-Subsystems (oder einer Db2-Gruppe), zu dem eine Verbindung hergestellt werden soll, um diese Gruppe mit gemeinsamer Datennutzung zu erreichen. Diese Namen werden im Parameter QSGDATA des Systemparametermakros CSQ6SYSP (beschrieben in CSQ6SYSP) angegeben.

In der Gruppe mit gemeinsamer Datennutzung werden gemeinsam genutzte Db2-Tabellen verwendet, um Folgendes zu speichern:

- Konfigurationsinformationen für die Gruppe mit gemeinsamer Warteschlange
- Eigenschaften von gemeinsam genutzten Objekten und Gruppenobjekten von IBM MQ.
- Optional können Daten in Bezug auf ausgelagerte IBM MQ-Nachrichten verwendet werden.

V 9.2.0 IBM MQ stellt eine einzelne Gruppe mit Beispieljobs für die Definition der erforderlichen Db2-Tabellenbereiche, -Tabellen und -Indizes bereit. Diese Jobs verwenden Universal Table Spaces (UTS). Frühere Versionen des Produkts enthielten zwei Gruppen mit Jobs, eine für UTS und eine für ältere Typen von Tabellenbereichen, die in den aktuellsten Versionen von Db2 nicht mehr verwendet werden.

V 9.2.0 IBM MQ kann weiterhin mit älteren Typen von Tabellenbereichen verwendet werden, was auch sinnvoll sein kann, wenn bereits eine Gruppe mit gemeinsamer Warteschlange vorhanden ist. Wenn Sie allerdings eine neue Gruppe mit gemeinsamer Warteschlange erstellen, sollten Sie UTS verwenden.

V 9.2.0 Db2 V12 Funktionsebene 508 bietet nun einen einen unterbrechungsfreien Migrationsprozess, um Tabellenbereiche mit mehreren Tabellen in universelle Tabellenbereiche umzuwandeln. Sie können diesen Ansatz verwenden, um die Tabellenbereiche mit mehreren Tabellen, die von vorhandenen Gruppen mit gemeinsamer Warteschlange verwendet werden, zu universellen Tabellenbereichen zu migrieren, ohne einen Ausfall der Gruppe mit gemeinsamer Warteschlange zu riskieren.

Db2 verwendet die Benutzer-ID der Person, die die Jobs ausführt, standardmäßig als Eigner der Db2-Ressourcen. Wenn diese Benutzer-ID gelöscht wird, werden die ihr zugeordneten Ressourcen gelöscht, und die Tabelle wird gelöscht. Verwenden Sie eine Gruppen-ID als Eigner der Tabellen und nicht als eine einzelne Benutzer-ID. Fügen Sie dazu `GROUP=groupname` auf der Jobkarte hinzu und geben Sie `SET CURRENT SQLID='groupname'` vor allen SQL-Anweisungen an.

IBM MQ verwendet die RRS-Anschlussfunktion von Db2. Dies bedeutet, dass Sie den Namen einer Db2-Gruppe angeben können, zu der eine Verbindung hergestellt werden soll. Der Vorteil einer Verbindung zu einem Db2-Gruppenanschlussnamen (anstatt zu einem bestimmten Db2-Subsystem) besteht darin, dass IBM MQ in diesem Fall eine Verbindung (oder erneute Verbindung) zu jedem verfügbaren Db2-Subsystem in dem z/OS-Image herstellen kann, das ein Mitglied dieser Gruppe ist. Es muss ein Db2 -Subsystem vorhanden sein, das Mitglied der Gruppe mit gemeinsamer Datennutzung ist, die auf jedem z/OS -Image aktiv ist, auf dem Sie ein IBM MQ -Subsystem mit gemeinsamer Warteschlange ausführen, und RRS muss aktiv sein.

Db2-Speicher

Bei den meisten Installationen beträgt der erforderliche Db2-Speicher etwa 20 oder 30 Zylinder auf einer 3390-Einheit. Zur genaueren Berechnung Ihres Speicherbedarfs ist in der folgenden Tabelle aufgeführt, wie viel Speicherplatz Db2 für die jeweiligen IBM MQ-Daten benötigt. Die Tabelle gibt an, wie lang die jeweilige Db2-Zeile ist und wann eine Zeile in der relevanten Db2-Tabelle eingefügt oder gelöscht wird. Verwenden Sie diese Informationen zusammen mit den Informationen zur Berechnung der Speicherplatzanforderungen für die Db2-Tabellen und deren Indizes in der *Db2 für z/OS Installationsanleitung*.

Tabelle 25. Db2-Speicherbedarf planen

Db2-Tabellenname	Länge der Zeile	Eine Zeile wird hinzugefügt, wenn:	Eine Zeile wird gelöscht, wenn:
CSQ.ADMIN_B_QSG	252 Byte	Eine Gruppe mit gemeinsamer Warteschlange wird mit der Funktion ADD QSG des Dienstprogramms CSQ5PQSG der Tabelle hinzugefügt.	Eine Gruppe mit gemeinsamer Warteschlange wird mit der Funktion REMOVE QSG des Dienstprogramms CSQ5PQSG aus der Tabelle entfernt. (Alle Zeilen, die zu dieser Gruppe mit gemeinsamer Warteschlange gehören, werden automatisch aus allen anderen Db2-Tabellen entfernt, wenn der Eintrag für die Gruppe mit gemeinsamer Warteschlange gelöscht wird.)
CSQ.ADMIN_B_QMGR	Bis zu 3828 Byte	Ein WS-Manager wird der Tabelle mit der Funktion ADD QMGR des Dienstprogramms CSQ5PQSG hinzugefügt.	Ein WS-Manager wird mit der Funktion REMOVE QMGR des Dienstprogramms CSQ5PQSG aus der Tabelle entfernt.
CSQ.ADMIN_B_STRUCTURE	1454 Byte	Die erste lokale Warteschlange wird definiert, die das Attribut QSGDISP(SHARED) angibt, das eine zuvor unbekannte Struktur in der Gruppe mit gemeinsamer Warteschlange benennt.	Die letzte lokale Warteschlangendefinition wird gelöscht, die das Attribut QSGDISP(SHARED) angibt, das eine Struktur in der Gruppe mit gemeinsamer Warteschlange benennt.
CSQ.ADMIN_B_SCST	342 Byte	Ein gemeinsam genutzter Kanal wird gestartet.	Ein gemeinsam genutzter Kanal wird inaktiv.

Tabelle 25. Db2-Speicherbedarf planen (Forts.)

Db2-Tabellenname	Länge der Zeile	Eine Zeile wird hinzugefügt, wenn:	Eine Zeile wird gelöscht, wenn:
CSQ.ADMIN_B_SSKT	254 Byte	Ein gemeinsam genutzter Kanal, der das Attribut NPMSPEED (NORMAL) hat, wird gestartet.	Ein gemeinsam genutzter Kanal, der das Attribut NPMSPEED (NORMAL) hat, wird inaktiv.
CSQ.ADMIN_B_STRBACKUP	514 Byte	Es wird eine neue Zeile zur Tabelle CSQ.ADMIN_B_STRUCTURE hinzugefügt. Jeder Eintrag ist ein Pseudoeintrag, bis der Befehl BACKUP CFSTRUCT ausgeführt wird, der die Dummyeinträge überschreibt.	Eine Zeile wird aus der Tabelle CSQ.ADMIN_B_STRUCTURE gelöscht.
CSQ.OBJ_B_AUTHINFO	3400 Byte	Es ist ein Authentifizierungsinformationsobjekt mit QSGDISP (GROUP) definiert.	Ein Authentifizierungsinformationsobjekt mit QSGDISP (GROUP) wird gelöscht.
CSQ.OBJ_B_QUEUE	Bis zu 3707 Byte	• Es ist eine Warteschlange mit dem Attribut QSGDISP (GROUP) definiert. • Es ist eine Warteschlange mit dem Attribut QSGDISP (SHARED) definiert. • Es wird eine Modellwarteschlange mit dem Attribut DEFTYPE (SHAREDYN) geöffnet.	• Eine Warteschlange mit dem Attribut QSGDISP (GROUP) wird gelöscht. • Eine Warteschlange mit dem Attribut QSGDISP (SHARED) wird gelöscht. • Eine dynamische Warteschlange mit dem Attribut DEFTYPE (SHAREDYN) wird mit der Option DELETE geschlossen.
CSQ.OBJ_B_NAMELIST	Bis zu 15127 Byte	Es ist eine Namensliste mit dem Attribut QSGDISP (GROUP) definiert.	Eine Namensliste mit dem Attribut QSGDISP (GROUP) wird gelöscht.
CSQ.OBJ_B_CHANNEL	Bis zu 14127 Byte	Es ist ein Kanal mit dem Attribut QSGDISP (GROUP) definiert.	Ein Kanal mit dem Attribut QSGDISP (GROUP) wird gelöscht.
CSQ.OBJ_B_STGCLASS	Bis zu 2865 Byte	Es ist eine Speicherklasse mit dem Attribut QSGDISP (GROUP) definiert.	Eine Speicherklasse mit der Attributklasse QSGDISP (GROUP) wird gelöscht.
CSQ.OBJ_B_PROCESS	Bis zu 3347 Byte	Es wird ein Prozess mit dem Attribut QSGDISP (GROUP) definiert.	Ein Prozess mit dem Attribut QSGDISP (GROUP) wird gelöscht.
CSQ.OBJ_B_TOPIC	Bis zu 14520 Byte	Es ist ein Themenobjekt mit dem Attribut QSGDISP (GROUP) definiert.	Ein Themenobjekt mit dem Attribut QSGDISP (GROUP) wird gelöscht.
CSQ.EXTEND_B_QMGR	Kleiner als 430 Byte	Ein WS-Manager wird der Tabelle mit der Funktion ADD QMGR des Dienstprogramms CSQ5PQSG hinzugefügt.	Ein WS-Manager wird mit der Funktion REMOVE QMGR des Dienstprogramms CSQ5PQSG aus der Tabelle entfernt.
CSQ.ADMIN_B_MESSAGES	87 Byte	Für große Nachricht PUT (1 pro BLOB).	Für große Nachrichten GET (1 pro BLOB).

Tabelle 25. Db2-Speicherbedarf planen (Forts.)			
Db2-Tabellenname	**Länge der Zeile**	**Eine Zeile wird hinzugefügt, wenn:**	**Eine Zeile wird gelöscht, wenn:**
CSQ.ADMIN_MSGS_BAUX1 CSQ.ADMIN_MSGS_BAUX2 CSQ.ADMIN_MSGS_BAUX3 CSQ.ADMIN_MSGS_BAUX4		Diese vier Tabellen enthalten Nachrichtennutzdaten für große Nachrichten, die in einer dieser vier Tabellen für jedes BLOB der Nachricht hinzugefügt werden. Da BLOBs eine maximale Länge von 511 KB haben, müssen bei einer Nachrichtenlänge von mehr als 711 KB auf jeden Fall mehrere BLOBs vorhanden sein.	

Die Verwendung einer großen Anzahl von Nachrichten in gemeinsam genutzten Warteschlangen mit einer Größe von mehr als 63 KB kann erhebliche Auswirkungen auf die Leistung eines IBM MQ-Systems haben. Weitere Informationen finden Sie im Abschnitt 'SupportPac MP16, Capacity Planning and Tuning for IBM MQ for z/OS' unter SupportPacs for IBM MQ and other project areas.

z/OS Planung von Backups und Wiederherstellung

Die Entwicklung von Sicherungs-und Wiederherstellungsprozeduren an Ihrem Standort ist wichtig, um kostspielige und zeitaufwendige Datenverluste zu vermeiden. IBM MQ stellt Funktionen bereit, mit denen sowohl Warteschlangen als auch Nachrichten nach einem Systemausfall in ihrem aktuellen Zustand wiederhergestellt werden können.

Dieses Thema enthält die folgenden Abschnitte:

Wiederherstellungsprozeduren

Entwickeln Sie folgende Prozeduren für IBM MQ:

- Es wird ein Wiederherstellungspunkt erstellt.
- Seitengruppen werden gesichert.
- CF-Strukturen sichern.
- Seitengruppen werden wiederhergestellt.
- Wiederherstellung bei Vorliegen der Bedingung 'Zu wenig Speicherbereich' (für IBM MQ-Protokolle und -Seitengruppen).
- CF-Strukturen wiederherstellen.

Weitere Informationen hierzu finden Sie unter IBM MQ for z/OS verwalten.

Machen Sie sich mit den Prozeduren vertraut, die auf Ihrer Site für die folgenden Schritte verwendet werden:

- Wiederherstellung nach einem Hardware-oder Stromausfall.
- Wiederherstellung nach einem z/OS-Komponentenfehler.
- Wiederherstellung nach einer Standortunterbrechung mit Offsite-Wiederherstellung.

z/OS Tipps für die Sicherung und Wiederherstellung

Verwenden Sie dieses Thema, um einige Sicherungs-und Wiederherstellungstasks zu verstehen.

Der Neustartprozess des Warteschlangenmanagers erfasst Ihre Daten in einem konsistenten Zustand, indem er Protokollinformationen auf die Seitengruppen anwendet. Wenn Ihre Seitengruppen beschädigt sind oder nicht verfügbar sind, können Sie das Problem mithilfe Ihrer Sicherungskopien Ihrer Seitengruppen lösen (wenn alle Protokolle verfügbar sind). Wenn Ihre Protokolldatensätze beschädigt oder nicht verfügbar sind, ist es möglicherweise nicht möglich, die Daten vollständig wiederherzustellen.

Beachten Sie die folgenden Punkte:

- Sicherungskopien in regelmäßigen Abständen erstellen
- Archivierungsprotokolle, die Sie möglicherweise noch benötigen, nicht verwerfen
- Zuordnung von DDname zu Seitengruppe nicht ändern

Sicherungskopien in regelmäßigen Abständen erstellen

Der Begriff *Wiederherstellungspunkt* bezeichnet ein Gruppe von Sicherungskopien von IBM MQ-Seitengruppen und den entsprechenden Protokolldateien, die zum Wiederherstellen dieser Seitengruppen erforderlich sind. Die Sicherungskopien stellen den potenziellen Wiederanlaufpunkt für den Fall von Seitengruppenverlusten dar (z. B. bei einem E/A-Fehler für die Seitengruppe). Wenn Sie den Warteschlangenmanager unter Verwendung dieser Sicherungskopien erneut starten, sind die Daten in IBM MQ bis zu dem Punkt konsistent, in dem diese Kopien ausgeführt wurden. Wenn alle Protokolle ab diesem Punkt verfügbar sind, kann IBM MQ zurück bis zum Fehlerpunkt wiederhergestellt werden.

Je aktueller Ihre Sicherungskopien sind, desto schneller kann IBM MQ die Daten in den Seitengruppen wiederherstellen. Die Wiederherstellung der Seitengruppen hängt von allen verfügbaren Protokolldatensätzen ab, die verfügbar sind.

Bei der Planung der Wiederherstellung müssen Sie festlegen, wie oft Sicherungskopien ausgeführt werden sollen und wie viele vollständige Sicherungszyklen zu halten sind. Diese Werte geben an, wie lange Ihre Protokolldateien und Sicherungskopien der Seitengruppen für die IBM MQ-Wiederherstellung beibehalten werden müssen.

Bei der Entscheidung, wie oft Sicherungskopien durchgeführt werden sollen, ist die Zeit zu berücksichtigen, die für die Wiederherstellung einer Seitengruppe erforderlich ist. Die benötigte Zeit wird wie folgt bestimmt:

- Die Menge des zu durchsetzenden Protokolls.
- Die Zeit, die ein Bediener benötigt, um Archivierungsbanddatenträger zu laden und zu entfernen.
- Die Zeit, die benötigt wird, um den Teil des Protokolls zu lesen, der für die Wiederherstellung benötigt wird.
- Die Zeit, die zum erneuten Verarbeiten geänderter Seiten benötigt wird.
- Das Speichermedium, das für die Sicherungskopien verwendet wird.
- Die Methode, die zum Erstellen und Zurückschreiben von Sicherungskopien verwendet wird.

Im Allgemeinen werden Sicherungskopien häufiger durchgeführt, wenn die Wiederherstellung weniger Zeit dauert, aber die Zeit für die Erstellung von Kopien verwendet wird.

Für jeden WS-Manager sollten Sie Sicherungskopien der folgenden Schritte ausführen:

- Die Archivprotokolldateien
- Die BSDS-Kopien, die zum Zeitpunkt des Archivs erstellt wurden
- Die Seitengruppen
- Ihre Objektdefinitionen
- Ihre CF-Strukturen

Gehen Sie wie folgt vor, um das Risiko zu verringern, dass Ihre Sicherungskopien verloren gehen oder beschädigt sind:

- Sicherungskopien auf verschiedenen Speicherdatenträgern in den Originalkopien speichern.
- Das Speichern der Sicherungskopien an einer anderen Site in den Originalkopien.
- Erstellen Sie mindestens zwei Kopien jeder Sicherung Ihrer Seitengruppen und, wenn Sie eine einzelne Protokollierung oder eine einzelne BSDS verwenden, zwei Kopien Ihrer Archivierungsprotokolle und BSDS. Wenn Sie die doppelte Protokollierung oder BSDS verwenden, erstellen Sie eine einzige Kopie beider Archivprotokolle oder BSDS.

Bevor Sie IBM MQ in eine Produktionsumgebung verschieben, sollten Sie Ihre Sicherungsprozeduren vollständig testen und dokumentieren.

Ihre Seitengruppen sichern

Sie müssen die Seitengruppen regelmäßig sichern. Einige Unternehmen sichern die Seitengruppen zweimal pro Tag.

Sie benötigen die aktiven und archivierbaren Protokolle seit einer Sicherung, um die Wiederherstellung mit Hilfe der Sicherung wiederherstellen zu können. Sie benötigen genügend Protokolldaten, um vier Prüfpunkte zu sichern, wenn die Sicherung beim Ausführen des Warteschlangenmanagers ausgeführt wurde.

Sie können ADRDSSU FastReplication verwenden, um Seitengruppen zu sichern, und Sie können dies tun, während der WS-Manager aktiv ist. Beachten Sie, dass Sie sicherstellen müssen, dass genügend Speicherplatz im Speicherpool vorhanden ist.

Objektdefinitionen sichern

Erstellen Sie Sicherungskopien Ihrer Objektdefinitionen. Verwenden Sie hierfür die Funktion MAKEDEF der Funktion COMMAND des Dienstprogramms (siehe COMMAND-Funktion von CSQUTIL verwenden).

Dies sollten Sie immer dann tun, wenn Sie Sicherungskopien Ihrer WS-Manager-Dateien erstellen und die aktuelle Version beibehalten.

Coupling Facility-Strukturen sichern

Wenn Sie Gruppen mit gemeinsamer Warteschlange eingerichtet haben, müssen Sie regelmäßige Sicherungen Ihrer CF-Strukturen ausführen, selbst wenn Sie diese nicht verwenden. Führen Sie dazu den Befehl IBM MQ BACKUP CFSTRUCT aus. Sie können diesen Befehl nur für CF-Strukturen verwenden, die mit dem Attribut RECOVER (YES) definiert sind. Wenn CF-Einträge für persistente gemeinsam genutzte Nachrichten auf ausgelagerte Nachrichtendaten verweisen, die in einer gemeinsam genutzten Nachrichtendatei (SMDS) oder in Db2 gespeichert sind, werden die ausgelagerten Daten zusammen mit den CF-Einträgen abgerufen und gesichert. Gemeinsam genutzte Nachrichtendatengruppen sollten nicht separat gesichert werden.

Es wird empfohlen, eine Sicherung aller CF-Strukturen zu jeder Stunde zu erstellen, um die Zeit zu minimieren, die zum Wiederherstellen einer CF-Struktur benötigt wird.

Sie können alle Sicherungen der CF-Struktur auf einem einzigen Warteschlangenmanager ausführen, was den Vorteil hat, die Erhöhung der Protokollverwendung auf einen einzigen Warteschlangenmanager zu begrenzen. Alternativ können Sie Sicherungskopien auf allen Warteschlangenmanagern in der Gruppe mit gemeinsamer Warteschlange erstellen, was den Vorteil hat, dass die Auslastung auf die

Gruppe mit gemeinsamer Warteschlange verteilt wird. Bei allen Strategien kann IBM MQ die Sicherung suchen und RECOVER CFSTRUCT aus jedem Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange ausführen. Der Zugriff muss auf die Protokolle aller Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange möglich sein, damit die CF-Struktur wiederhergestellt werden kann.

Sicherheitsrichtlinien für Nachrichten sichern

Wenn Sie mit Advanced Message Security ein Backup Ihrer Sicherheitsrichtlinien für Nachrichten erstellen, verwenden Sie das Dienstprogramm für die Nachrichtensicherheitsrichtlinie (CSQ0UTIL), um **dspmqspl** mit dem Parameter '-export' auszuführen, und speichern Sie anschließend die Richtliniendefinitionen, die von EXPORT DD ausgegeben werden.

Sie sollten ein Backup Ihrer Nachrichtensicherheitsrichtlinien immer dann erstellen, wenn Sie Ihre Warteschlangenmanagerdaten sichern, und dabei die aktuellste Version speichern.

Archivierungsprotokolle, die Sie möglicherweise benötigen, nicht verwerfen

IBM MQ muss während des Neustarts möglicherweise Archivprotokolle verwenden. Sie müssen die Archivprotokolle ausreichend archivieren, damit das System vollständig wiederhergestellt werden kann. IBM MQ benötigt möglicherweise ein Archivprotokoll für die Wiederherstellung einer Seitengruppe aus einer wiederhergestellten Sicherungskopie. Wenn Sie das Archivprotokoll gelöscht haben, kann IBM MQ die Seitengruppe nicht in ihrem aktuellen Zustand wiederherstellen. Informationen zum Löschen von Archivierungsprotokollen finden Sie im Abschnitt Archivierungsprotokolldatensätze verwerfen .

Mit dem Befehl `/cpf DIS USAGE TYPE(ALL)` können Sie die Protokoll-RBA und die Folgenummer des Protokollsatzes (Log Range Sequence Number, LRSN) anzeigen, die für die Wiederherstellung der Seitengruppen für den Warteschlangenmanager und die Strukturen der Gruppe mit gemeinsamer Warteschlange erforderlich sind. Danach sollten Sie die Bootstrap-Dataset (BSDS)-Informationen des Warteschlangenmanagers mit dem Dienstprogramm print log map utility (CSQJU004) drucken, um die Protokolle mit der Protokoll-RBA zu finden.

Für CF-Strukturen müssen Sie das Dienstprogramm CSQJU004 auf jedem Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange ausführen, um die Protokolle mit der LRSN zu lokalisieren. Sie benötigen diese Protokolle und alle späteren Protokolle, um die Seitengruppen und Strukturen wiederherstellen zu können.

Die Zuordnung von DDname zu Seitengruppe nicht ändern

IBM MQ erstellt folgende Zuordnungen: Seitengruppe 00 zu DDname CSQP0000, Seitengruppe 01 zu DDname CSQP0001 usw. bis CSQP0099. IBM MQ schreibt die Wiederherstellungsprotokollsätze für eine Seitengruppe basierend auf dem DDname, dem die Seitengruppe zugeordnet ist. Aus diesem Grund dürfen Sie keine Seitengruppen verschieben, die bereits mit einer PSID DDname verknüpft wurden.

z/OS Seitengruppen wiederherstellen

Verwenden Sie dieses Thema, um die Faktoren zu verstehen, die beim Wiederherstellen von Seitengruppen beteiligt sind, und wie die Neustartzeiten minimiert werden.

Ein Schlüsselfaktor in der Wiederherstellungsstrategie betrifft die Zeit, für die Sie einen Ausfall des Warteschlangenmanagers tolerieren können. Die Gesamtausfallzeit kann die Zeit enthalten, die zum Wiederherstellen einer Seitengruppe aus einer Sicherung oder zum erneuten Starten des Warteschlangenmanagers nach einer abnormalen Beendigung erforderlich ist. Zu den Faktoren, die sich auf die Neustartzeit auswirken, gehört, wie oft Sie Ihre Seitengruppen sichern, und wie viele Daten in das Protokoll zwischen Prüfpunkten geschrieben werden.

Um die Neustartzeit nach einer abnormalen Beendigung zu minimieren, halten Sie die Arbeitseinheiten so kurz, dass höchstens zwei aktive Protokolle verwendet werden, wenn das System erneut gestartet wird. Wenn Sie beispielsweise eine IBM MQ-Anwendung entwerfen, sollten Sie zwischen dem ersten MQI-Aufruf am Synchronisationspunkt und dem Commitpunkt keinen MQGET-Aufruf mit langem Warteintervall platzieren, da dies zu einer Arbeitseinheit mit langer Dauer führen kann. Eine weitere häufige Ursache für lange Arbeitseinheiten sind Stapelintervalle von mehr als 5 Minuten für den Kanalinitiator.

Sie können den Befehl DISPLAY THREAD verwenden, um die RBA der Arbeitseinheiten anzuzeigen und die Auflösung der alten zu unterstützen.

Wie oft müssen Sie eine Seitengruppe sichern?

Häufiges Seitensatzes ist erforderlich, wenn eine relativ kurze Wiederherstellungszeit erforderlich ist. Dies gilt auch dann, wenn eine Seitengruppe sehr klein ist oder eine kleine Menge an Aktivitäten in Warteschlangen in dieser Seitengruppe vorhanden ist.

Wenn Sie persistente Nachrichten in einer Seitengruppe verwenden, sollte die Sicherungsfrequenz in Stunden und nicht in Tagen angegeben werden. Dies gilt auch für die Seitengruppe Null.

Um eine ungefähre Sicherungsfrequenz zu berechnen, beginnen Sie mit der Bestimmung der Gesamtwiederherstellungszeit für das Ziel. Dies setzt sich wie folgt zusammen:

1. Die Zeit, die zum Reagieren auf das Problem aufgedauert hat.
2. Die Zeit, die zum Wiederherstellen der Sicherungskopie der Seitengruppe verwendet wurde.

   Wenn Sie SnapShot backup/restore verwenden, ist die Zeit, die zur Ausführung dieser Task erforderlich ist, einige Sekunden. Weitere Informationen zu SnapShot finden Sie im Handbuch *DFSMSdss Storage Administration Guide* .
3. Der Zeitpunkt, zu dem der Warteschlangenmanager erneut gestartet werden muss, einschließlich der zusätzlichen Zeit, die zum Wiederherstellen der Seitengruppe erforderlich ist.

   Dies hängt am meisten von der Menge der Protokolldaten ab, die aus aktiven und archivierbaren Protokollen gelesen werden müssen, da diese Seitengruppe zuletzt gesichert wurde. Alle diese Protokolldaten müssen gelesen werden, zusätzlich zu den Daten, die direkt mit der beschädigten Seitengruppe verknüpft sind.

   Anmerkung: Bei Verwendung der *Fuzzy-Sicherung* (wenn eine Momentaufnahme von den Protokollen und Seitengruppen erstellt wird, während eine Arbeitseinheit aktiv ist), kann es erforderlich sein, bis zu drei zusätzliche Prüfpunkte zu lesen, und dies kann dazu führen, dass ein oder mehrere zusätzliche Protokolle gelesen werden müssen.

Bei der Entscheidung darüber, wie lange die Wiederherstellung der Seitengruppe zulässig ist, müssen die folgenden Faktoren berücksichtigt werden:

- Die Rate, mit der Daten während der normalen Verarbeitung in die aktiven Protokolle geschrieben werden, hängt davon ab, wie Nachrichten in Ihrem System eingehen, zusätzlich zu der Nachrichtenrate.

  Nachrichten, die über einen Kanal empfangen oder gesendet werden, bewirken mehr Datenprotokollierung als Nachrichten, die lokal generiert und abgerufen wurden.
- Die Rate, mit der Daten aus dem Archiv und den aktiven Protokollen gelesen werden können.

  Beim Lesen der Protokolle hängt die erreichbare Datenrate von den verwendeten Einheiten und der Gesamtbelastung für das jeweilige DASD-Subsystem ab.

  Bei den meisten Bandeinheiten ist es möglich, höhere Datenraten für archivierte Protokolle mit einer großen Blockgröße zu erzielen. Wenn jedoch ein Archivprotokoll für die Wiederherstellung erforderlich ist, müssen alle Daten in den aktiven Protokollen ebenfalls gelesen werden.

z/OS CF-Strukturen wiederherstellen

Verwenden Sie dieses Thema, um den Wiederherstellungsprozess für CF-Strukturen zu verstehen.

Mindestens ein Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange muss aktiv sein, damit ein RECOVER CFSTRUCT-Befehl verarbeitet werden kann. Die Wiederherstellung der CF-Struktur wirkt sich nicht auf die Neustartzeit des Warteschlangenmanagers aus, da die Wiederherstellung von einem bereits aktiven Warteschlangenmanager ausgeführt wird.

Der Wiederherstellungsprozess besteht aus zwei logischen Schritten, die durch den Befehl RECOVER CFSTRUCT verwaltet werden:

1. Die Sicherung lokalisieren und wiederherstellen.
2. Zusammenführen aller protokollierter Aktualisierungen in persistenten Nachrichten, die in der CF-Struktur gespeichert sind, aus den Protokollen aller Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange, die die CF-Struktur verwendet haben, und Anwenden der Änderungen im Backup.

Der zweite Schritt dauert wahrscheinlich sehr viel länger, da möglicherweise eine Menge Protokolldaten gelesen werden müssen. Sie können die Zeit verkürzen, die Sie bei häufigen Sicherungen nehmen, oder wenn Sie mehrere CF-Strukturen gleichzeitig oder beides wiederherstellen.

Der Warteschlangenmanager, der die Wiederherstellung durchführen wird, sucht alle relevanten Sicherungen in allen Protokollen der anderen Warteschlangenmanager unter Verwendung der Daten in Db2 und den Bootstrap-Datasets. Der Warteschlangenmanager führt eine Wiedergabe dieser Sicherungen in der richtigen zeitlichen Abfolge für die Gruppe mit gemeinsamer Warteschlange aus, angefangen beim Zeitpunkt kurz vor der letzten Sicherung bis zum Zeitpunkt des Ausfalls.

Die Zeit, die zum Wiederherstellen einer CF-Struktur benötigt wird, hängt von der Menge der Wiederherstellungsprotokolldaten ab, die wiedergegeben werden müssen, die wiederum von der Häufigkeit der Sicherungen abhängig sind. Im schlimmsten Fall dauert es so lange, bis das Protokoll eines Warteschlangenmanagers gelesen wurde, wie es geschrieben wurde. Wenn Sie also beispielsweise eine Gruppe mit gemeinsamer Warteschlange mit sechs Warteschlangenmanager haben, kann die Wiederholung einer Protokollaktivität mit einer Dauer von einer Stunde bis zu sechs Stunden betragen. Im Allgemeinen dauert es weniger Zeit als dies, da das Lesen von Massendaten möglich ist und weil die Protokolle des anderen Warteschlangenmanagers parallel gelesen werden können. Als Ausgangspunkt empfehlen wir Ihnen, Ihre CF-Strukturen jede Stunde zu sichern.

Alle Warteschlangenmanager können die Arbeit mit nicht gemeinsam genutzten Warteschlangen und Warteschlangen in anderen CF-Strukturen fortsetzen, während eine CF-Struktur fehlgeschlagen ist. Wenn auch die Verwaltungsstruktur fehlgeschlagen ist, muss mindestens einer der Warteschlangenmanager in der Gruppe mit gemeinsamer Warteschlange gestartet werden, bevor Sie den Befehl RECOVER CFSTRUCT ausgeben können.

Die Sicherung von CF-Strukturen kann beträchtliche Protokollschreibkapazität erfordern und kann daher dem Warteschlangenmanager, der die Sicherung ausführen wird, eine große Last aufzwingen. Wählen Sie zur Erstellung von Backups einen gering ausgelasteten Warteschlangenmanager aus. Fügen Sie auf ausgelasteten Systemen der Gruppe mit gemeinsamer Warteschlange einen zusätzlichen Warteschlangenmanager hinzu und dedizieren Sie diesen ausschließlich für die Ausführung von Backups.

z/OS Erreichen bestimmter Wiederherstellungsziele

In diesem Thema wird beschrieben, wie Sie bestimmte Wiederherstellungszielzeiten erreichen können, indem Sie die Sicherungsfrequenz anpassen.

Wenn Sie bestimmte Wiederherstellungsziele haben, z. B. die Wiederherstellung des Warteschlangenmanagers und die Neustartverarbeitung zusätzlich zu der normalen Startzeit innerhalb von *xx* Sekunden, können Sie die folgende Berechnung verwenden, um die Sicherungsfrequenz (in Stunden) zu schätzen:

```
Formula (A)
                     Required restart time * System recovery log read rate
                           (in secs)                  (in MB/sec)
Backup frequency  = ------------------------------------------------------
   (in hours)               Application log write rate (in MB/hour)
```

Anmerkung: In den folgenden Beispielen wird die Notwendigkeit hervorgehoben, die Seitengruppen häufig zu sichern. Bei den Berechnungen wird davon ausgegangen, dass die meisten Protokollaktivitäten von einer großen Anzahl persistenter Nachrichten abgeleitet werden. Es gibt jedoch Situationen, in denen

der Umfang der Protokollaktivität nicht einfach berechnet werden kann. In einer Umgebung mit einer Gruppe mit gemeinsamer Warteschlange beispielsweise kann es in einer Arbeitseinheit, in der gemeinsam genutzte Warteschlangen zusätzlich zu anderen Ressourcen aktualisiert werden, dazu kommen, dass Datensätze für die Arbeitseinheit in das IBM MQ-Protokoll geschrieben werden. Aus diesem Grund kann die Schreibgeschwindigkeit des Anwendungsprotokolls in Formel (A) nur von der beobachteten Rate, mit der die IBM MQ-Protokolle gefüllt werden, genau abgeleitet werden.

Als Beispiel wird ein System angenommen, in dem IBM MQ MQI clients eine Gesamtarbeitslast von 100 persistenten Nachrichten pro Sekunde generieren. In diesem Fall werden alle Nachrichten lokal generiert.

Wenn jede Nachricht eine Benutzerlänge von 1 KB hat, beträgt die Menge der pro Stunde protokollierten Daten ungefähr:

```
100 * (1 + 1.3) KB * 3600 = approximately 800 MB

where
      100           = the message rate a second
      (1 + 1.3) KB  = the amount of data logged for
                      each 1 KB of persistent messages
```

Betrachten Sie eine Gesamtwiederherstellungszeit von 75 Minuten. Wenn Sie 15 Minuten Zeit gelassen haben, um auf das Problem zu reagieren und die Sicherungskopie der Seitengruppe wiederherzustellen, müssen die Wiederherstellung des Warteschlangenmanagers und der Neustart innerhalb von 60 Minuten (3600 Sekunden) ausgeführt werden, wenn die Formel (A) angewendet wird. Angenommen, alle erforderlichen Protokolldaten sind auf der RVA2-T82-DASD-Einheit, die eine Wiederherstellungsrate von etwa 2,7 MB pro Sekunde hat, erfordert dies eine Seitengruppe-Sicherungsfrequenz von mindestens allen:

```
3600 seconds * 2.7 MB a second / 800 MB an hour = 12.15 hours
```

Wenn der IBM MQ-Anwendungstag ungefähr 12 Stunden dauert, ist eine Sicherung pro Tag angemessen. Wenn der Anwendungstag jedoch 24 Stunden dauert, sind zwei Sicherungen pro Tag besser geeignet.

Ein weiteres Beispiel könnte ein Produktionssystem sein, in dem alle Nachrichten für Anforderungs-/Antwortanwendungen (d.h. eine persistente Nachricht auf einem Empfängerkanal empfangen und eine persistente Antwortnachricht generiert und einen Senderkanal gesendet werden).

In diesem Beispiel ist die erreichte Stapelgröße eins, so dass für jede Nachricht ein Stapel vorhanden ist. Wenn 50 Anforderungen pro Sekunde beantwortet werden, beträgt die Gesamtlast 100 persistente Nachrichten pro Sekunde. Wenn jede Nachricht eine Länge von 1 KB hat, beträgt die Menge der pro Stunde protokollierten Daten ungefähr:

```
50((2 * (1+1.3) KB) + 1.4 KB + 2.5 KB) * 3600 = approximately 1500 MB

where:
 50                 = the message pair rate a second
 (2 * (1 + 1.3) KB) = the amount of data logged for each message pair
 1.4 KB             = the overhead for each batch of messages
                      received by each channel
 2.5 KB             = the overhead for each batch of messages sent
                      by each channel
```

Um die Wiederherstellung des Warteschlangenmanagers zu erreichen und innerhalb von 30 Minuten (1800 Sekunden) erneut zu starten, vorausgesetzt, dass alle erforderlichen Protokolldaten auf der RVA2-T82-DASD-Einheit vorhanden sind, ist es erforderlich, dass die Seitengruppe-Sicherung mindestens alle folgenden Schritte ausgeführt wird:

```
1800 seconds * 2.7 MB a second / 1500 MB an hour = 3.24 hours
```

Periodische Überprüfung der Sicherungsfrequenz

Überwachen Sie die IBM MQ-Protokollbelegung in Bezug auf MB pro Stunde. Führen Sie diese Überprüfung in regelmäßigen Abständen aus und ändern Sie gegebenenfalls die Häufigkeit der Seitengruppe.

z/OS Hinweise zur Sicherung für andere Produkte

Wenn Sie IBM MQ zusammen mit CICS oder IMS verwenden, müssen Sie auch die Auswirkungen dieser Produkte für Ihre Sicherungsstrategie berücksichtigen. Der hierarchische Speichermanager (DFHSM) verwaltet die Datenspeicherung und kann mit dem von IBM MQ verwendeten Speicher interagieren.

Sicherung und Wiederherstellung mit DFHSM

Der hierarchische Speichermanager der Dateneinrichtung (DFHSM) führt die automatische Verfügbarkeits-und Datenverfügbarkeitsverwaltung zwischen den Speichereinheiten in Ihrem System aus. Wenn Sie ihn verwenden, müssen Sie bedenken, dass er automatisch Daten in den und aus dem IBM MQ-Speicher verschiebt.

DFHSM verwaltet den DASD-Speicherbereich effizient, indem er Datensätze versetzt, die vor kurzem nicht in alternativen Speicher verwendet wurden. Außerdem werden die Daten für die Wiederherstellung zur Verfügung gestellt, indem neue oder geänderte Dateigruppen automatisch auf Band-oder DASD-Sicherungsdatenträger kopiert werden. Sie kann Datensätze löschen oder sie in eine andere Einheit verschieben. Seine Operationen werden täglich zu einem bestimmten Zeitpunkt ausgeführt und ermöglichen es, einen Datensatz für einen bestimmten Zeitraum zu halten, bevor er gelöscht oder verschoben wird.

Sie können alle DFHSM-Operationen auch manuell ausführen. Im *Data Facility Hierarchical Storage Manager Benutzerhandbuch* wird erläutert, wie die DFHSM-Befehle verwendet werden. Wenn Sie DFHSM zusammen mit IBM MQ verwenden, beachten Sie folgende Verhaltensweisen von DFHSM:

- Verwendet katalogisierte Dateigruppen.
- Operiert auf Seitengruppen und Protokollen.
- Unterstützt VSAM-Dateigruppen.

Wiederherstellung und CICS

Die Wiederherstellung von CICS-Ressourcen wird durch IBM MQ nicht beeinträchtigt. CICS erkennt IBM MQ als eine nicht zu CICS gehörende Ressource (oder als einen externen Ressourcenmanager) und schließt IBM MQ als Teilnehmer mithilfe der CICS-Ressourcenmanagerschnittstelle (RMI) in alle Anforderungen zur Synchronisationspunktkoordinierung ein. Weitere Informationen zur CICS-Wiederherstellung finden Sie im Handbuch *CICS Recovery and Restart Guide*. Weitere Informationen zur CICS-Ressourcenmanagerschnittstelle finden Sie im Handbuch *CICS Customization Guide*.

Wiederherstellung und IMS

IMS erkennt IBM MQ als externes Subsystem und als Teilnehmer an der Synchronisationspunktkoordination. Informationen zur IMS-Wiederherstellung für externe Subsystemressourcen finden Sie im Handbuch *IMS Customization Guide*.

z/OS Vorbereiten der Wiederherstellung auf einem alternativen Standort

Bei einem vollständigen Ausfall eines IBM MQ-Rechenzentrums können Sie eine Wiederherstellung auf einem anderen IBM MQ-System an einem Wiederherstellungsstandort ausführen.

Damit die Wiederherstellung eines IBM MQ-Systems an einem Wiederherstellungsstandort möglich ist, müssen Sie regelmäßig die Seitengruppen und Protokolle sichern. Wie bei allen Datenwiederherstellungsoperationen werden die Ziele der Wiederherstellung nach einem Katastrophenfall als Datenverlust, Verarbeitungsprozesse (Aktualisierungen) und Zeit wie möglich verloren gehen.

An der Wiederherstellungssite:

- Der IBM MQ-Warteschlangenmanager, der zur Wiederherstellung verwendet wird, **muss** denselben Namen haben wie der ausgefallene Warteschlangenmanager.
- Stellen Sie sicher, dass das im Wiederherstellungs-WS-Manager verwendete Systemparametermodul dieselben Parameter enthält wie der verloren gegangene Warteschlangenmanager.

Informationen zum Disaster-Recovery-Prozess finden Sie unter IBM MQ for z/OS verwalten.

z/OS Beispiel für die Sicherungsaktivität des Warteschlangenmanagers

In diesem Abschnitt wird ein Beispiel für eine Sicherungsaktivität des Warteschlangenmanagers angezeigt.

Wenn Sie die Sicherungsstrategie Ihres Warteschlangenmanagers planen, ist eine Schlüsselüberlegung die Beibehaltung der korrekten Menge an Protokolldaten. Im Abschnitt Protokolle verwalten wird beschrieben, wie Sie feststellen können, welche Protokolldatengruppen erforderlich sind, indem Sie auf die RBA des Systemwiederherstellungs-RBA des Warteschlangenmanagers verweisen. IBM MQ bestimmt die relative Byteadresse (RBA) für die Systemwiederherstellung mithilfe folgender Informationen:

- Derzeit aktive Arbeitseinheiten.
- Seitengruppe-Aktualisierungen, die noch nicht aus den Pufferpools auf die Platte gebürstet wurden.
- CF-Strukturensicherungen und unabhängig davon, ob das Protokoll dieses Warteschlangenmanagers Informationen enthält, die in einer Wiederherstellungsoperation erforderlich sind, die sie verwenden.

Sie müssen genügend Protokolldaten speichern, um die Datenträgerwiederherstellung ausführen zu können. Während sich die RBA des Systemwiederherstellungs-RBA im Laufe der Zeit erhöht, verringert sich die Menge der Protokolldaten, die aufbewahrt werden müssen, wenn nachfolgende Sicherungen ausgeführt werden. CF-Strukturensicherungen werden von IBM MQ verwaltet und deshalb bei der Berichterstellung für die Systemwiederherstellungs-RBA berücksichtigt. Dies bedeutet, dass in der Praxis die Menge der Protokolldaten, die beibehalten werden müssen, nur dann abnimmt, wenn Seitensatzes-Sicherungen ausgeführt werden.

Abbildung 43 auf Seite 215 zeigt ein Beispiel für die Sicherungsaktivität bei einem Warteschlangenmanager, der Mitglied einer Gruppe mit gemeinsamer Warteschlange ist, wie sich die Wiederherstellungs-RBA bei jeder Sicherung ändert und wie sich dies auf die Menge der Protokolldaten auswirkt, die aufbewahrt werden muss. In dem Beispiel verwendet der Warteschlangenmanager lokale und gemeinsam genutzte Ressourcen: Seitengruppen und zwei CF-Strukturen, STRUCTURE1 und STRUCTURE2.

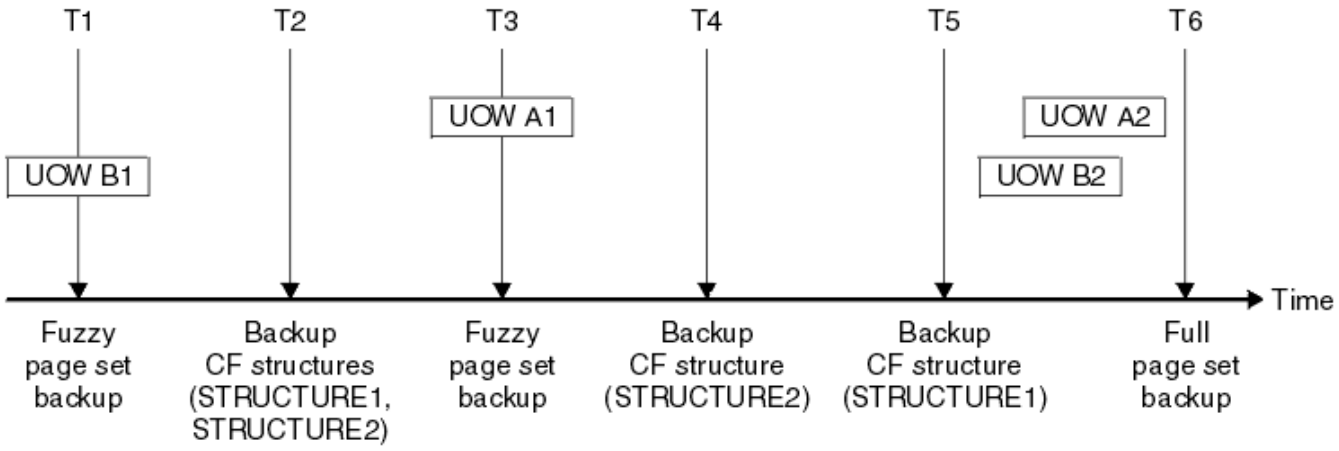


Abbildung 43. Beispiel für die Sicherungsaktivität des Warteschlangenmanagers

Dies geschieht zu jedem Zeitpunkt:

Punkt in Zeit T1

Es wird eine unscharfe Sicherung der Seitengruppen erstellt, wie im Abschnitt Seitengruppen sichern und wiederherstellen beschrieben.

Der RBA des Systemwiederherstellungs-RBA des Warteschlangenmanagers ist der niedrigste der folgenden:

- Die Wiederherstellungs-RBAs der Seitengruppen, die an diesem Punkt gesichert werden.
- Die niedrigste Recovery-RBA, die für die Wiederherstellung der CF-Anwendungsstrukturen erforderlich ist. Dies bezieht sich auf die Wiederherstellung von Sicherungen von STRUCTURE1 und STRUCTURE2, die zuvor erstellt wurden.
- Der Wiederherstellungs-RBA für die älteste derzeit aktive Arbeitseinheit im Warteschlangenmanager (UOWB1).

Der Systemwiederherstellungs-RBA für diesen Zeitpunkt wird durch Nachrichten ausgegeben, die vom Befehl DISPLAY USAGE ausgegeben werden, der Teil des Fuzzy-Sicherungsprozesses ist.

Punkt in Zeit T2

Es werden Backups der CF-Strukturen erstellt. Die CF-Struktur STRUCTURE1 wird zuerst gesichert, gefolgt von STRUCTURE2.

Die Menge der Protokolldaten, die beibehalten werden müssen, bleibt unverändert, da die gleichen Daten, die aus dem RBA für die Systemwiederherstellung bei T1 ermittelt wurden, für die Wiederherstellung nach der Seitengruppe, die bei T1 erstellt wurde, noch erforderlich sind.

Punkt in Zeit T3

Es wird eine weitere unscharfe Sicherung erstellt.

Der RBA des Systemwiederherstellungs-RBA des Warteschlangenmanagers ist der niedrigste der folgenden:

- Die Wiederherstellungs-RBAs der Seitengruppen, die an diesem Punkt gesichert werden.
- Die niedrigste RBA für Wiederherstellung, die für die Wiederherstellung der CF-Struktur STRUCTURE1 erforderlich ist, da STRUCTURE1 vor STRUCTURE2 gesichert wurde.
- Der Wiederherstellungs-RBA für die älteste derzeit aktive Arbeitseinheit im Warteschlangenmanager (UOWA1).

Der Systemwiederherstellungs-RBA für diesen Zeitpunkt wird durch Nachrichten ausgegeben, die vom Befehl DISPLAY USAGE ausgegeben werden, der Teil des Fuzzy-Sicherungsprozesses ist.

Sie können jetzt die von dieser neuen Systemwiederherstellungs-RBA festgelegten Protokolldaten reduzieren.

Zeitpunkt T4
Es wird eine Sicherung der CF-Struktur STRUCTURE2 durchgeführt. Die Wiederherstellung der RBA für die Wiederherstellung der ältesten erforderlichen CF-Struktursicherung bezieht sich auf die Sicherung der CF-Struktur STRUCTURE1, die zum Zeitpunkt T2 gesichert wurde.

Die Erstellung dieser CF-Struktursicherung hat keine Auswirkungen auf die Menge der Protokolldaten, die aufbewahrt werden müssen.

Punkt in Zeit T5
Es wird eine Sicherung der CF-Struktur STRUCTURE1 ausgeführt. Der Wiederherstellungs-RBA für die Wiederherstellung der ältesten erforderlichen CF-Struktursicherung bezieht sich nun auf die Wiederherstellung der CF-Struktur STRUCTURE2, die zum Zeitpunkt T4 gesichert wurde.

Die Erstellung dieser CF-Struktursicherung hat keine Auswirkungen auf die Menge der Protokolldaten, die aufbewahrt werden müssen.

Punkt in Uhrzeit T6
Es wird eine vollständige Sicherung Ihrer Seitengruppen übernommen, wie im Abschnitt Seitengruppen sichern und wiederherstellen beschrieben.

Der RBA des Systemwiederherstellungs-RBA des Warteschlangenmanagers ist der niedrigste der folgenden:

- Die Wiederherstellungs-RBAs der Seitengruppen, die an diesem Punkt gesichert werden.
- Die niedrigste Recovery-RBA, die zum Wiederherstellen der CF-Strukturen erforderlich ist. Dies bezieht sich auf die Wiederherstellung der CF-Struktur STRUCTURE2.
- Der Wiederherstellungs-RBA für die älteste derzeit aktive UOW im Warteschlangenmanager. In diesem Fall gibt es keine aktuellen Arbeitseinheiten.

Der Systemwiederherstellungs-RBA für diesen Zeitpunkt wird durch Nachrichten ausgegeben, die vom Befehl DISPLAY USAGE ausgegeben werden, der Teil des Gesamtsicherungsprozesses ist.

Auch hier können die gespeicherten Protokolldaten reduziert werden, da der Systemwiederherstellungs-RBA, der der Gesamtsicherung zugeordnet ist, neuerer ist.

z/OS z/OS UNIX-Umgebung planen

Bestimmte Prozesse innerhalb des IBM MQ-Warteschlangenmanagers, des Kanalinitiators und des mqweb-Servers verwenden z/OS UNIX System Services (z/OS UNIX) für ihre normale Verarbeitung.

Die Benutzer-IDs der gestarteten Tasks des Warteschlangenmanagers und Kanalinitiators benötigen ein OMVS-Segment mit einer UID, die definiert ist, damit auf z/OS UNIX zugegriffen werden kann. Die Benutzer-IDs benötigen in z/OS UNIX keine speziellen Berechtigungen.

Anmerkung: Obwohl der Warteschlangenmanager und der Kanalinitiator von z/OS UNIX-Funktionen Gebrauch machen (z. B. als Schnittstelle zu TCP/IP-Services), müssen sie auf keinen der Inhalte des IBM MQ-Installationsverzeichnisses im z/OS UNIX-Dateisystem zugreifen. Daher ist für den Warteschlangenmanager und den Kanalinitiator keine Konfiguration erforderlich, um den Pfad für das z/OS UNIX-Dateisystem anzugeben.

Der mqweb-Server, der die IBM MQ Console und REST API hostet, nutzt Dateien im IBM MQ-Installationsverzeichnis im z/OS UNIX-Dateisystem. Er benötigt außerdem Zugriff auf ein anderes Dateisystem, das zum Speichern von Daten wie Konfigurations-und Protokolldateien verwendet wird. Die JCL der gestarteten Task 'mqweb' muss so angepasst werden, dass sie auf diese z/OS UNIX-Dateisysteme verweist.

Der Inhalt des Verzeichnisses IBM MQ im z/OS UNIX Dateisystem wird auch von Anwendungen verwendet, die eine Verbindung zu IBM MQ herstellen. Zum Beispiel Anwendungen, welche die IBM MQ classes for Java- oder IBM MQ classes for JMS-Schnittstellen verwenden.

In den folgenden Abschnitten finden Sie die relevanten Konfigurationsanweisungen:

- Für IBM MQ classes for Java relevante Umgebungsvariablen
- IBM MQ classes for Java Bibliotheken

- Umgebungsvariablen festlegen
- JNI-Bibliotheken (Java Native Interface) konfigurieren

z/OS Advanced Message Security planen

TLS (oder SSL) kann zum Verschlüsseln und zum Schutz von Nachrichten verwendet werden, die in einem Netz fließen, aber dies schützt keine Nachrichten, wenn sie sich in einer Warteschlange ("in Ruhe") befinden. Advanced Message Security (AMS) schützt die Nachrichten ab dem Zeitpunkt, an dem sie zuerst in eine Warteschlange eingereiht werden, bis sie empfangen werden, so dass nur die beabsichtigten Empfänger die Nachricht lesen können. Die Nachrichten werden während der Verarbeitung verschlüsselt und signiert und während der Verarbeitung von 'get' nicht geschützt.

In AMS können unterschiedliche Schutzmaßnahmen für Nachrichten konfiguriert werden:

1. Eine Nachricht kann signiert werden. Die Nachricht ist in Klartext, aber es gibt eine Kontrollsumme, die signiert ist. Dadurch können alle Änderungen im Nachrichteninhalt erkannt werden. Aus dem signierten Inhalt können Sie angeben, wer die Daten signiert hat.
2. Eine Nachricht kann verschlüsselt werden. Der Inhalt ist für jeden ohne den Entschlüsselungsschlüssel nicht sichtbar. Der Entschlüsselungsschlüssel wird für jeden Empfänger verschlüsselt.
3. Eine Nachricht kann verschlüsselt und signiert werden. Der Entschlüsselungsschlüssel wird für jeden Empfänger verschlüsselt, und von der Signatur aus können Sie feststellen, wer die Nachricht gesendet hat.

Die Verschlüsselung und Signatur verwenden digitale Zertifikate und Schlüsselringe.

Sie können einen Client für die Verwendung von AMS konfigurieren, sodass die Daten bereits geschützt werden, bevor sie in den Clientkanal gestellt werden. Geschützte Nachrichten können an einen fernen Warteschlangenmanager gesendet werden, und Sie müssen den fernen WS-Manager so konfigurieren, dass diese Nachrichten verarbeitet werden.

einrichtenAMS

Für die AMS-Aufgaben wird ein eigener AMS-Adressraum verwendet. Dies hat zusätzliche Sicherheitsfunktion, die den Zugriff auf und den Schutz der Verwendung von Schlüsselringen und Zertifikaten bietet.

Sie konfigurieren die Warteschlangen, die geschützt werden sollen, indem Sie ein Dienstprogramm (CSQ0UTIL) verwenden, um die Sicherheitsrichtlinien für Warteschlangen zu definieren.

Nach der Konfiguration von AMS

Sie müssen ein digitales Zertifikat und einen Schlüsselring für Personen einrichten, die Nachrichten einlegen, und die Personen, die Nachrichten erhalten.

Wenn ein Benutzer, z. B. Alice, unter z/OS eine Nachricht an den Benutzer Bob senden muss, benötigt AMS eine Kopie des öffentlichen Zertifikats für Bob.

Wenn Bob eine Nachricht von Alice verarbeiten möchte, benötigt AMS das öffentliche Zertifikat für Alice oder dasselbe Zertifizierungsstellenzertifikat (CA-Zertifikat), das Alice verwendet.

Achtung: Sie müssen wie folgt vorgehen:

- Sorgfältig planen, wer die Warteschlangen in die Warteschlange stellen oder aus den Warteschlangen einholen kann
- Identifizieren Sie die Personen und deren Zertifikatsnamen.

Es ist leicht, Fehler zu machen, und Probleme können schwer zu lösen sein.

Zugehörige Konzepte

„Planung des Warteschlangenmanagers” auf Seite 157
Wenn Sie einen Warteschlangenmanager einrichten, sollte Ihre Planung die Entwicklung des WS-Managers ermöglichen, damit der Warteschlangenmanager die Anforderungen Ihres Unternehmens erfüllt.

z/OS Managed File Transfer planen

Verwenden Sie diesen Abschnitt als Anleitung, wie Sie Ihr System für die Ausführung von Managed File Transfer (MFT) unter z/OS einrichten müssen.

z/OS Planung für Managed File Transfer-Hardware-und Softwarevoraussetzungen

Verwenden Sie dieses Thema als Anleitung dazu, wie Sie Hardware-und Softwarevoraussetzungen auf Ihrem System konfigurieren müssen, damit Managed File Transfer (MFT) unter z/OSausgeführt werden kann.

Softwarevoraussetzungen

Managed File Transfer ist in Javageschrieben, mit einigen Shell-Scripts und JCL zum Konfigurieren und Ausführen des Programms.

Wichtig: Sie müssen mit z/OS UNIX System Services (z/OS UNIX) vertraut sein, um Managed File Transferkonfigurieren zu können. For example:

- Die Dateiverzeichnisstruktur mit Namen wie `/u/userID/myfile.txt`
- Mit z/OS UNIX-Befehlen, zum Beispiel:
  - `cd` (Verzeichnis ändern)
  - `ls` (Liste)
  - `chmod` (Dateiberechtigungen ändern)
  - `chown` (Dateieigentumsrecht oder Gruppen ändern, die auf die Datei oder das Verzeichnis zugreifen können)

Sie benötigen die folgenden Produkte unter z/OS UNIX, um MFT konfigurieren und ausführen zu können:

1. Java, z. B. im Verzeichnis `/java/java80_bit64_GA/J8.0_64/`
2. IBM MQ 9.2.0, z. B. im Verzeichnis `/mqm/V9R2M0`
3. Wenn Sie Db2 für den Status und den Verlauf verwenden möchten, müssen Sie Db2-JDBC-Bibliotheken installieren, z. B. im Verzeichnis `/db2/db2v10/jdbc/libs`.

Produktregistri

Beim Start überprüft Managed File Transfer die Registrierung in der `sys1.parmlib`(IFAPRDxx)-Verkettung. Der folgende Code ist ein Beispiel dafür, wie Sie MFT registrieren:

```
PRODUCT OWNER('IBM CORP')
NAME('WS MQ FILE TRANS')
ID(5655-MFT)
VERSION(*) RELEASE(*) MOD(*)
FEATURENAME('WS MQ FILE TRANS')
STATE(ENABLED)
```

Plattenspeicherplatz

V 9.2.0 Im IBM MQ for z/OS-Programmverzeichnis ist der DASD- und zFS-Speicherbedarf für Managed File Transfer angegeben. Download-Links für das Programmverzeichnis für IBM MQ for z/OSfinden Sie unter IBM MQ 9.2 PDF-Dateien für Produktdokumentation und Programmverzeichnisse.

z/OS Planung für Managed File Transfer-Topologien

Nutzen Sie dieses Thema als Anleitung für die Topologie, die Sie auf Ihrem System benötigen, um Managed File Transfer (MFT) unter z/OS auszuführen.

Managed File Transfer-Warteschlangenmanager

IBM MQ Managed File Transfer-Topologien bestehen aus:

Agenten und deren zugehörige Warteschlangenmanager
Der Agent verwendet Systemwarteschlangen, die auf dem Warteschlangenmanager des Agenten gehostet werden, um die Statusinformationen zu verwalten und Anforderungen für die Arbeit zu empfangen.

Ein Befehlswarteschlangenmanager
Dieser dient als Gateway zu einer MFT-Topologie. Er ist mit den Agenten-WS-Managern über Sender- und Empfängerkanäle oder durch Clustering verbunden. Wenn einer der aufgelisteten Befehle ausgeführt wird, stellen sie eine direkte Verbindung mit dem Befehlswarteschlangenmanager her und senden eine Nachricht an den angegebenen Agenten. Diese Nachricht wird über das IBM MQ-Netz an den Warteschlangenmanager des Agenten weitergeleitet, in dem sie vom Agenten aufgenommen und verarbeitet wird.

Ein Koordinationswarteschlangenmanager
Hierbei handelt es sich um einen zentralen Hub, der über Kenntnisse der gesamten Topologie verfügt. Der Koordinationswarteschlangenmanager ist mit allen Agenten-WS-Managern in einer Topologie über Sender- und Empfängerkanäle oder über Clustering verbunden. Agenten veröffentlichen regelmäßig Statusinformationen an den Koordinationswarteschlangenmanager und speichern dort ihre Übertragungsvorlagen.

Es ist möglich, dass ein einzelner Warteschlangenmanager mehrere Rollen innerhalb einer Topologie ausführt. Der gleiche Warteschlangenmanager kann beispielsweise als Koordinationswarteschlangenmanager, aber auch als Befehlswarteschlangenmanager für eine Topologie konfiguriert werden.

Wenn Sie mehrere WS-Manager verwenden, müssen Sie Kanäle zwischen den Warteschlangenmanagern einrichten. Sie können dies entweder durch Clustering oder durch Verwendung von Punkt-zu-Punkt-Verbindungen erreichen.

Bei der Verwendung von IBM MQ Managed File Transfer for z/OS gibt es eine Reihe von Dingen, die berücksichtigt werden müssen, wann die Warteschlangenmanager bestimmt werden, die für die verschiedenen Rollen innerhalb einer Topologie verwendet werden sollen.

Agentenwarteschlangenmanager

Der Agentenwarteschlangenmanager für einen IBM MQ Managed File Transfer for z/OS-Agenten muss unter z/OS ausgeführt werden.

Wenn:

- Der Agent mit Managed File Transfer for z/OS auf IBM MQ 9.1 oder höher ausgeführt wird
- Und der Agentenwarteschlangenmanager für IBM MQ Advanced for z/OS Value Unit Edition (Advanced VUE) lizenziert ist

kann der Agent über den CLIENT-Transport eine Verbindung mit dem Warteschlangenmanager herstellen.

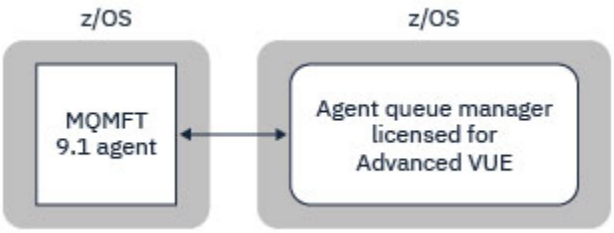


Abbildung 44. MFT 9.1-Agenten unter z/OS können mit dem CLIENT-Transport eine Verbindung zu einem Warteschlangenmanager herstellen, vorausgesetzt, der Warteschlangenmanager ist für Advanced VUE lizenziert.

Wenn:

- Der Agent mit Managed File Transfer for z/OS auf IBM MQ 9.0 oder früher ausgeführt wird
- Oder der Agentenwarteschlangenmanager mit Managed File Transfer for z/OS auf IBM MQ 9.0 oder höher ausgeführt wird, und der Agentenwarteschlangenmanager für MFT, IBM MQ Advanced for z/OS oder Advanced VUE lizenziert ist

muss der Agent mit der Transportmethode BINDINGS eine Verbindung zum Warteschlangenmanager herstellen.

Abbildung 45. MFT 9.0-Agenten unter z/OS und 9.1, die über einen Agentenwarteschlangenmanager verfügen, der für MFT oder IBM MQ Advanced lizenziert ist, müssen eine Verbindung über die Transportmethode BINDINGS herstellen.

Befehlswarteschlangenmanager

Der Artikel Welche MFT-Befehle und -Prozesse mit welchem Warteschlangenmanager verbunden sind zeigt alle Befehle an, die eine Verbindung zum Befehlswarteschlangenmanager für eine Managed File Transfer-Topologie herstellen.

Anmerkung: Wenn Sie diese Befehle unter z/OS ausführen, muss sich der Befehlswarteschlangenmanager auch unter z/OS befinden.

Wenn der Befehlswarteschlangenmanager für Advanced VUE lizenziert ist, können die Befehle mit dem CLIENT-Transport eine Verbindung zum Warteschlangenmanger herstellen. Andernfalls müssen die Befehle über den BINDINGS-Transport mit dem Befehlswarteschlangenmanager verbunden werden.

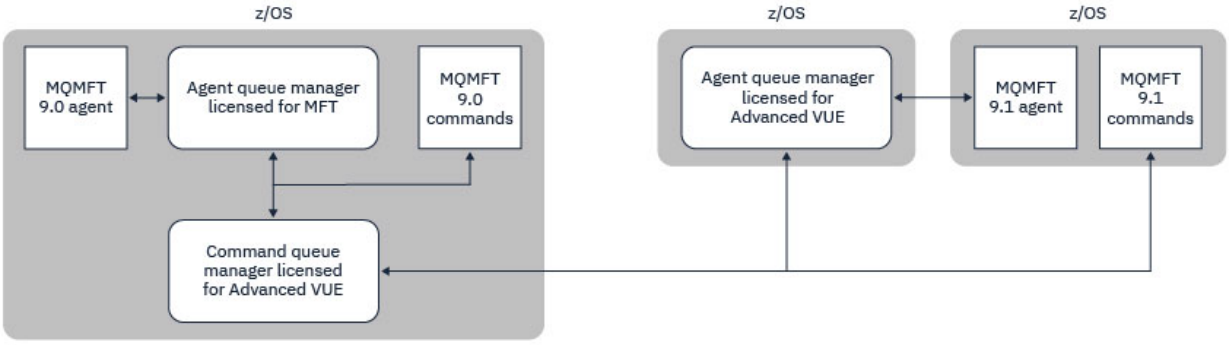


Abbildung 46. Befehle stellen eine Verbindung zum Befehlswarteschlangenmanager für eine MFT-Topologie her. Wenn Sie diese Befehle unter z/OS ausführen, muss sich der Befehlswarteschlangenmanager auch unter z/OS befinden

Koordinationswarteschlangenmanager

IBM MQ Managed File Transfer for z/OS-Agenten können Teil einer Topologie sein, bei der ein Koordinationswarteschlangenmanager entweder auf z/OS oder plattformübergreifend läuft.

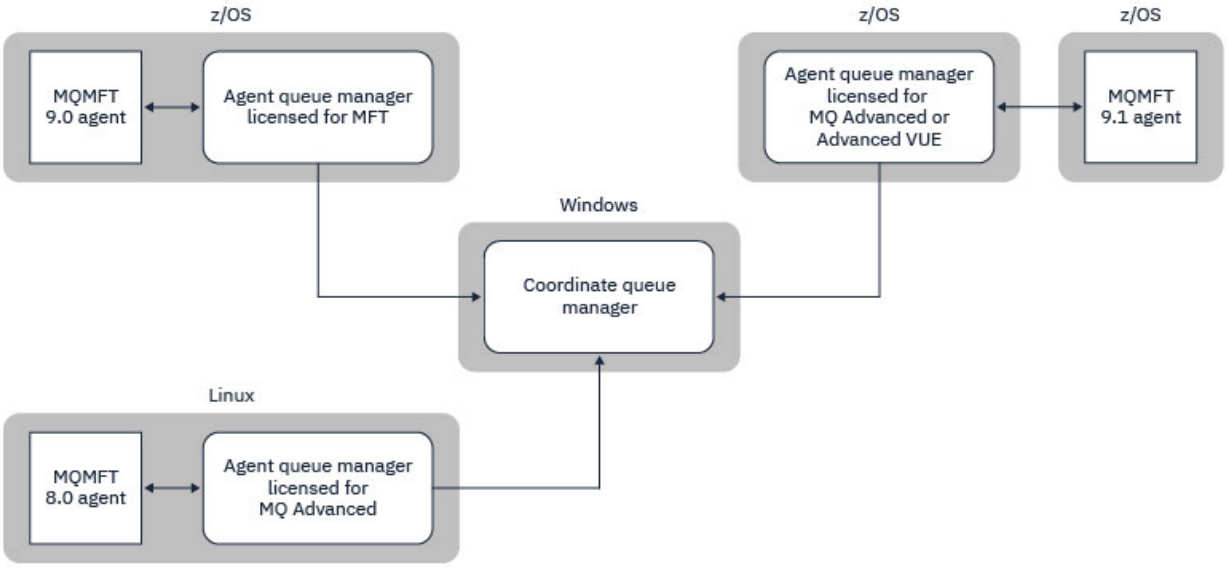


Abbildung 47. MFT-Agenten, die unter z/OS ausgeführt werden, können Teil einer MFT-Topologie sein, in der der Koordinationswarteschlangenmanager auf einer IBM MQ-Multiplattform ausgeführt wird.

Im Artikel Welche MFT-Befehle und -Prozesse mit welchem Warteschlangenmanager verbunden sind werden die Befehle angezeigt, die eine Verbindung zum Koordinationswarteschlangenmanager für eine Managed File Transfer-Topologie herstellen. Es ist möglich, diese Befehle unter z/OS auszuführen und dann eine Verbindung zum Koordinationswarteschlangenmanager herzustellen, der auf einer anderen Plattform ausgeführt wird.

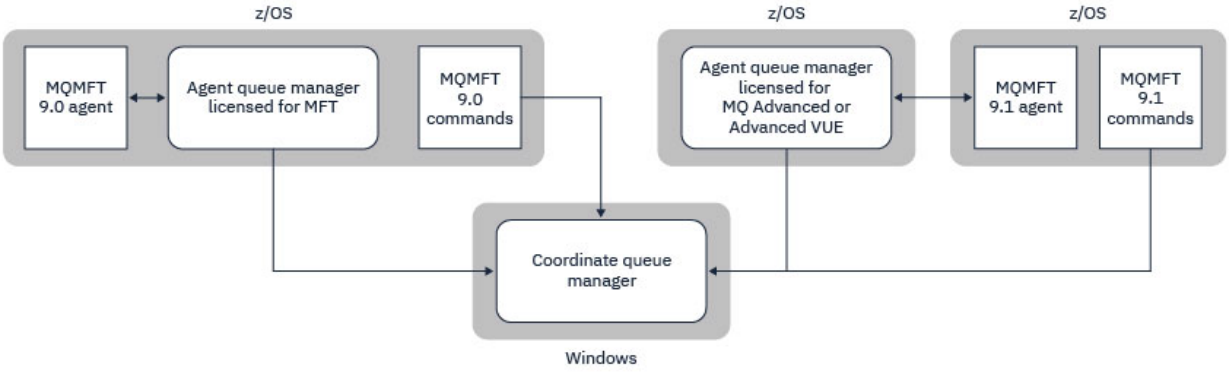


*Abbildung 48. Bestimmte Befehle, wie z. B. **fteListAgents**, stellen eine direkte Verbindung zum Koordinationswarteschlangenmanager für eine MFT-Topologie her.*

Wie viele Agenten brauche ich?

Die Agenten führen die Arbeit beim Übertragen von Daten aus, und wenn Sie eine Anforderung zum Übertragen von Daten machen, geben Sie den Namen eines Agenten an.

Standardmäßig kann ein Agent 25 Sende-und 25 Empfangsanforderungen gleichzeitig verarbeiten. Sie können diese Prozesse konfigurieren. Weitere Informationen finden Sie unter Managed File Transfer-Konfigurationsoptionen unter z/OS.

Wenn der Agent ausgelastert ist, wird die Arbeit in die Warteschlange gestellt. Die Zeit, die zum Verarbeiten einer Anforderung verwendet wird, hängt von mehreren Faktoren ab, wie z. B. dem Umfang der zu sendendem Datenvolumen, der Netzbandbreite und der Verzögerung im Netz.

Es kann erforderlich sein, mehrere Agenten parallel zu verarbeiten.

Sie können auch steuern, auf welche Ressourcen ein Agent zugreifen kann, so dass einige Agenten mit einer begrenzten Untergruppe von Daten arbeiten können.

Wenn Sie Anforderungen mit unterschiedlicher Priorität verarbeiten möchten, können Sie mehrere Agenten verwenden und den Workload-Manager verwenden, um die Priorität der Jobs festzulegen.

Agenten ausführen

In der Regel handelt es sich bei den Agenten um lange laufende Prozesse Die Prozesse können als Jobs, die im Stapelbetrieb ausgeführt werden, oder als gestartete Tasks übergeben werden.

z/OS Planung für Managed File Transfer - Sicherheitsaspekte

Verwenden Sie dieses Thema als Anleitung zu den Sicherheitsaspekten, die Sie auf Ihrem System benötigen, um Managed File Transfer (MFT) unter z/OS auszuführen.

Sicherheit

Sie müssen angeben, welche Benutzer-IDs für die MFT-Konfiguration und für MFT-Operationen verwendet werden sollen.

Sie müssen die Dateien oder Warteschlangen angeben, die Sie übertragen, und welche Benutzer-IDs die Übergabe von Übertragungsanforderungen an MFT übergeben werden.

Wenn Sie die Agenten und die Protokollfunktion anpassen, geben Sie die Gruppe der Benutzer an, die MFT-Services ausführen dürfen, oder die MFT-Verwaltung.

Sie sollten diese Gruppe konfigurieren, bevor Sie mit der Anpassung von MFT beginnen. Falls Sie die Sicherheit im Warteschlangenmanager aktiviert haben, benötigt MFT Zugriff auf folgende Ressourcen, da das Programm IBM MQ-Warteschlangen verwendet:

Tabelle 26. MQADMIN, Ressourcenklasse

Name	**Zugriff erforderlich**
QUEUE.SYSTEM.FTE.EVENT.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.COMMAND.agent_name	Aktualisieren
CONTEXT.SYSTEM.FTE.COMMAND.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.STATE.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.DATA.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.REPLY.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.AUTHAGT1.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.AUTHTRN1.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.AUTHOPS1.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.AUTHSCH1.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.AUTHMON1.agent_name	Aktualisieren
QUEUE.SYSTEM.FTE.AUTHADM1.agent_name	Aktualisieren

Tabelle 27. MQQUEUE, Ressourcenklasse

Name	**Zugriff erforderlich**
SYSTEM.FTE.AUTHAGT1.agent_name	Aktualisieren
SYSTEM.FTE.AUTHTRN1.agent_name	Aktualisieren
SYSTEM.FTE.AUTHOPS1.agent_name	Aktualisieren

Tabelle 27. MQQUEUE, Ressourcenklasse (Forts.)	
Name	**Zugriff erforderlich**
SYSTEM.FTE.AUTHSCH1.agent_name	Aktualisieren
SYSTEM.FTE.AUTHMON1.agent_name	Aktualisieren

Sie können die Benutzer-Sandboxing verwenden, um festzustellen, auf welche Teile des Dateisystems der Benutzer zugreifen kann, der die Übertragung anfordert.

Um die Benutzer-Sandboxing zu aktivieren, fügen Sie die Anweisung `userSandboxes=true` zur Datei *agent.properties* für den Agenten hinzu, den Sie einschränken möchten, und fügen Sie der Datei `MQ_DATA_PATH/mqft/config/coordination_qmgr_name/agents/agent_name/User-Sandboxes.xml` die entsprechenden Werte hinzu.

Weitere Informationen finden Sie im Abschnitt Mit Benutzer-Sandboxes arbeiten .

Diese Benutzer-ID wird in `UserSandboxes.xml`-Dateien konfiguriert.

Diese XML-Datei enthält Informationen wie Benutzer-ID oder Benutzer-ID* und eine Liste der Ressourcen, die verwendet werden können (eingeschlossen) oder nicht verwendet werden können (ausgeschlossen). Sie müssen bestimmte Benutzer-IDs definieren, die auf welche Ressourcen zugreifen können: z. B.:

Tabelle 28. Beispiel-Benutzer-ID zusammen mit Zugriff auf bestimmte Ressourcen			
Benutzer-ID	**Zugriff**	**Einschließen oder Ausschließen**	**Ressource**
Administrator *	Lesen	Anzeigeoptionen	`/home/user/**`
Administrator *	Lesen	Ausschließen	`/home/user/private/**`
Sysprog	Lesen	Anzeigeoptionen	`/home/user/**`
Administrator *	Lesen	Anzeigeoptionen	Application.reply.queue

Anmerkungen:

1. Wenn `type=queue` angegeben wird, ist die Ressource entweder ein Warteschlangenname oder `queue@qmgr`.
2. Wenn die Ressource mit `//` beginnt, handelt es sich bei der Ressource um eine Datei; andernfalls ist die Ressource eine Datei in z/OS UNIX.
3. Die Benutzer-ID ist die Benutzer-ID aus der MQMD-Struktur. Dies entspricht möglicherweise nicht der Benutzer-ID, die die Nachricht tatsächlich einreiht.
4. Für Anforderungen auf dem lokalen Warteschlangenmanager können Sie MQADMIN CONTEXT.* um zu begrenzen, welche Benutzer diesen Wert festlegen können.
5. Für Anforderungen, die über einen fernen Warteschlangenmanager ausgeführt werden, müssen Sie davon ausgehen, dass die Sicherheitsfunktion der verteilten Warteschlangenmanager die Sicherheit aktiviert hat, um eine nicht autorisierte Einstellung der Benutzer-ID in der MQMD-Struktur zu verhindern.
6. Eine Benutzer-ID von SYSPROG1 auf einer Linux-Maschine ist dieselbe Benutzer-ID SYSPROG1 für die Sicherheitsprüfung unter z/OS.

z/OS Verwendung der IBM MQ Console und der REST API unter z/OS planen

IBM MQ Console und REST API sind Anwendungen, die in einem WebSphere Liberty (Liberty)-Server ausgeführt werden, der als 'mqweb' bezeichnet wird. Der mqweb-Server wird als gestartete Task ausgeführt. Die MQ Console ermöglicht die Verwendung eines Web-Browsers zur Verwaltung von Warteschlangen-

managern. Die REST API stellte eine einfache Programmschnittstelle bereit, mit der Anwendungen die Verwaltung von Warteschlangenmanagern und Messaging-Funktionen ausführen können.

Installations-und Konfigurationsdateien

Sie müssen die IBM MQ for z/OS UNIX System Services Web Components-Funktion installieren, mit der die Dateien installiert werden, welche für die Ausführung des mqweb-Servers unter z/OS UNIX System Services (z/OS UNIX) erforderlich sind. Sie müssen mit z/OS UNIX vertraut sein, um den mqweb-Server konfigurieren und verwalten zu können.

Die IBM MQ-Dateien werden in z/OS UNIX mit verschiedenen Attributen installiert, die für den ordnungsgemäßen Betrieb des mqweb-Servers erforderlich sind. Wenn Sie die the IBM MQ z/OS UNIX-Installationsdateien ko pieren müssen, beispielsweise wenn Sie have installed IBM MQ auf dem einen System installiert haben und IBM MQ auf einem anderen System ausführen, sollten Sie die während der Installation erstellte IBM MQ-ZFS kopieren und diese schreibgeschützt an das Ziel anhängen. Wenn Sie die Dateien auf eine andere Weise kopieren, gehen unter Umständen Dateiattribute verloren.

Bei der Erstellung des mqweb-Servers müssen Sie sich für einen Speicherort für das Liberty-Benutzerverzeichnis entscheiden und dieses Verzeichnis erstellen. Dieses Verzeichnis enthält Konfigurations- und Protokolldateien, die Position kann ähnlich wie `/var/mqm/mqweb` sein.

MQ Console und REST API mit Warteschlangenmanagern auf unterschiedlichen Ebenen verwenden

Die MQ Console und die REST API können nur mit solchen Warteschlangenmanagern direkt interagieren, die hinsichtlich Version, Release und Modifikationsstufe (VRM) denselben Stand aufweisen. Beispielsweise können MQ Console und REST API, die mit IBM MQ 9.1.0 ausgeliefert werden, nur mit lokalen Warteschlangenmanagern unter IBM MQ 9.1.0 interagieren. MQ Console und REST API, die mit IBM MQ 9.0.5 ausgeliefert werden, können nur mit lokalen Warteschlangenmanagern unter IBM MQ 9.0.5 interagieren.

Mit der REST API können Sie Warteschlangenmanager einer anderen Version über den mqweb-Server verwalten, indem Sie einen Gateway-Warteschlangenmanager konfigurieren. Sie benötigen jedoch mindestens einen WS-Manager in derselben Version wie der mqweb-Server, der als Gateway-Warteschlangenmanager fungieren soll. Weitere Informationen finden Sie unter Fernverwaltung über REST API.

Migrationsinformationen

Wenn Sie nur einen Warteschlangenmanager haben, können Sie den mqweb-Server als eine einzige gestartete Task ausführen und die Bibliotheken ändern, die er bei der Migration des Warteschlangenmanagers verwendet.

Wenn Sie mehr als einen Warteschlangenmanager haben, können Sie bei der Migration die mqweb-Server in verschiedenen Versionen starten, indem Sie gestartete Tasks mit unterschiedlichen Namen verwenden. Diese Namen können ein beliebiger Name sein. Sie können z. B. einen IBM MQ 9.1.0 mqweb-Server mit einer gestarteten Task mit dem Namen MQWB0910 und einen IBM MQ 9.0.5 mqweb-Server mit einer gestarteten Task mit dem Namen MQWB0905 starten.

Wenn Sie dann die Warteschlangenmanager von einer Version auf eine neuere Version migrieren, werden die Warteschlangenmanager für die spätere Version im mqweb-Server verfügbar und sind im mqweb-Server für die frühere Version nicht mehr verfügbar.

Nachdem Sie alle WS-Manager auf die neuere Version migriert haben, können Sie den mqweb-Server für die frühere Version löschen.

HTTP-Ports

Der mqweb-Server verwendet bis zu zwei Ports für HTTP:

- Eine für HTTPS, mit einem Standardwert von 9443.
- Eine für HTTP. HTTP ist nicht standardmäßig aktiviert, aber wenn er aktiviert ist, hat er den Standardwert 9080.

Wenn die Standardportwerte im Gebrauch sind, müssen Sie andere Ports zuordnen. Wenn Sie mehrere mqweb-Server für mehrere Versionen von IBM MQ gleichzeitig ausführen, müssen Sie jeder Version separate Ports zuordnen. Weitere Informationen zum Festlegen der Ports, die vom mqweb-Server verwendet werden, finden Sie im Abschnitt HTTP-und HTTPS-Ports konfigurieren .

Sie können den folgenden TSO-Befehl verwenden, um Informationen zu einem Port anzuzeigen:

```
NETSTAT TCP tcpip (PORT portNumber)
```

Dabei steht *tcpip* für den Namen des TCP/IP-Adressraums und *portNumber* gibt die Nummer des Ports an, über den Informationen angezeigt werden sollen.

Sicherheit-Starten des mqweb-Servers

Die Benutzer-ID des mqweb-Servers benötigt bestimmte Berechtigungen. Weitere Informationen finden Sie im Abschnitt Berechtigung, die von der Benutzer-ID für die gestartete Task 'mqweb' benötigt wird .

Sicherheit für die Verwendung der MQ Console und der REST API

Für die Verwendung der MQ Console und der REST API müssen Sie sich als ein Benutzer authentifizieren, der in einer konfigurierten Registry enthalten ist. Diesen Benutzern werden bestimmte Rollen zugeordnet, die die Aktionen bestimmen, die die Benutzer ausführen können. Damit ein Benutzer beispielsweise die messaging REST API verwenden kann, muss ihm die Rolle `MQWebUser` zugewiesen sein. Weitere Informationen zu den verfügbaren Rollen für MQ Console und REST API sowie den Zugang durch diese Rollen finden Sie unter Rollen unter MQ Console und REST API.

Weitere Informationen zum Konfigurieren der Sicherheit für MQ Console und REST API finden Sie unter Sicherheit für MQ Console und REST API.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Dokumentation ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
IBM Europe, Middle East and Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Défense
U.S.A.

Bei Lizenzanforderungen zu Double-Byte-Information (DBCS) wenden Sie sich bitte an die IBM Abteilung für geistiges Eigentum in Ihrem Land oder senden Sie Anfragen schriftlich an folgende Adresse:

Lizenzierung von geistigem Eigentum

IBM Japan, Ltd.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in dieser Veröffentlichung werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekanntgegeben. IBM kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Europe, Middle East and Africa
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesen Informationen beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Die in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Um diese so realistisch wie möglich zu gestalten, enthalten sie auch Namen von Personen, Firmen, Marken und Produkten. Sämtliche dieser Namen sind fiktiv. Ähnlichkeiten mit Namen und Adressen tatsächlicher Unternehmen oder Personen sind zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musterprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos (d. h. ohne Zahlung an IBM) kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Wird dieses Buch als Softcopy (Book) angezeigt, erscheinen keine Fotografien oder Farbabbildungen.

Informationen zu Programmierschnittstellen

Die bereitgestellten Informationen zur Programmierschnittstelle sollen Sie bei der Erstellung von Anwendungssoftware für dieses Programm unterstützen.

Dieses Handbuch enthält Informationen über vorgesehene Programmierschnittstellen, die es dem Kunden ermöglichen, Programme zu schreiben, um die Services von WebSphere MQzu erhalten.

Diese Informationen können jedoch auch Angaben über Diagnose, Bearbeitung und Optimierung enthalten. Die Informationen zu Diagnose, Bearbeitung und Optimierung sollten Ihnen bei der Fehlerbehebung für die Anwendungssoftware helfen.

Wichtig: Verwenden Sie diese Diagnose-, Änderungs-und Optimierungsinformationen nicht als Programmierschnittstelle, da sie Änderungen unterliegen.

Marken

IBM, das IBM Logo, ibm.com, sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information"www.ibm.com/legal/copytrade.shtml. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Dieses Produkt enthält Software, die von Eclipse Project (https://www.eclipse.org/) entwickelt wurde.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Teilenummer:

(1P) P/N: